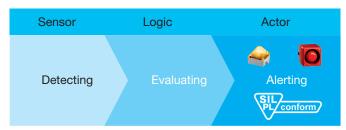
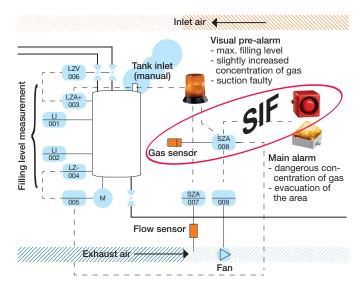
Functional safety IEC 61508 / IEC 61511 (SIL)

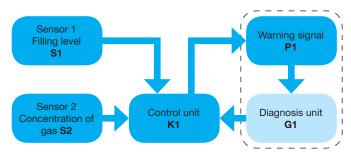
Safety Instrumented System SIS (Safety Loop)



Process safety e.g. gas alarm



Safety block diagram filling level / gas

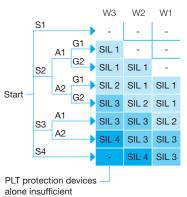


- S1 Sensor 1 (filling level in the tank)
- S2 Sensor 1 (concentration of gas in plant room)
- K1 Control unit
- P1 Visual and audible warning signal
- G1 Diagnosis unit for signaling devices

| 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 | е |
| 99% up to > 99% | SIL 3 | SIL 4 | SIL 4 | 4 | - |

Requirement according to IEC 61508, type B (partially unknown failure conduct) Compare SIL/PL (IEC 61508 / DIN EN ISO 13849)

Hazard graph according to IEC 61508



- S = Extent of damage S1 minor injury of a person
- S2 serious, irreversible injury of one or more people or
- death of one person death of several people S3 <u>S</u>4 disastrous effects with several dead
- A = Likelihood of people being
- in the area rarely to slightly more often frequently to continuously A1 A2
- G = Danger prevention G1 possible under certain
- conditions
- G2 barely possible
- W = Likelihood of occurrence W1 very small W2 small
- W3 relatively high

Evaluation of the safety function

| Required safety related parameters | | | | | |
|---|--|-------------------------------|---|--|--|
| IEC | IEC 61508 Device type | | | | |
| PFH/PFD SIL T1 | - | Units with internal diagnosis | | safety control safety switch gears | |
| $\begin{array}{c} MTTF_{d} \\ \lambda_{d} \\ \lambda_{s} \end{array}$ | DC, CCF, subsystem type | Units without internal | Without omponents that are subject to wear and tear | sensors, signaling devices | |
| B10 _d λ _d λ _s | DC, CCF, subsystem type, n _{op} | diagnosis | With omponents that are subject to wear and tear | emergency shut- down, relay, switch | |
| CCF: failure due to common cause | | | | | |

DC: Diagnostic coverage

Calculation of an SIS with a SIL 2-actor

Given values:

| PFD Sensor A | 1.5 * 10-3 | (suitable for SIL 2) |
|--------------|------------------------|----------------------|
| PFD Control | 1.3 * 10-4 | (suitable for SIL 3) |
| PFD Actor | 1.1 * 10 ⁻³ | (suitable for SIL 2) |

Example for a 1001 Actor

(1 unit required for the functioning of 1 available unit)

| Sensor A SIL 2 | | • | Control SIL 3 | (e.g. | SPS) | ٠ | Actor SIL 3 |
|--------------------|---|------|-------------------------|--------|------------|---|------------------|
| PFD _{Sys} | = | PFD |) _s | + | PFD | + | PFD _A |
| PFD _{Sys} | = | 1.5 | * 10 ⁻³ | + | 1.3 * 10-4 | + | 1.1 * 10-3 |
| PFD_{Sys} | = | 2.73 | 3 * 10 ⁻³ (S | SIL 2) | | | |

By using this component, the SIS reaches the PFD for SIL 2.

Failure probability

| SIL | Operating mode with low requirement rate – PFD (average failure probability of the function in case of demand) | Operating mode with continual requirement rate – PFH (probability of a failure that brings dangerous risk per hour) | PL |
|-------|---|--|----|
| SIL 4 | $\geq 10^{-5} \text{ up to} < 10^{-4}$ | $\ge 10^{-9}$ up to < 10^{-8} | - |
| SIL 3 | $\geq 10^{-4}$ up to < 10^{-3} | $\geq 10^{-8}$ up to < 10^{-7} | е |
| SIL 2 | $\geq 10^{-3}$ up to < 10^{-2} | $\geq 10^{-7}$ up to < 10^{-6} | d |
| SIL 1 | > 10 ² up to 1 101 | $\geq 10^{-6}$ up to 3 x 10 ⁻⁶ | С |
| | $\geq 10^{-2}$ up to < 10^{-1} | $\ge 3 \times 10^{-6} \text{ up to} < 10^{-5}$ | b |

