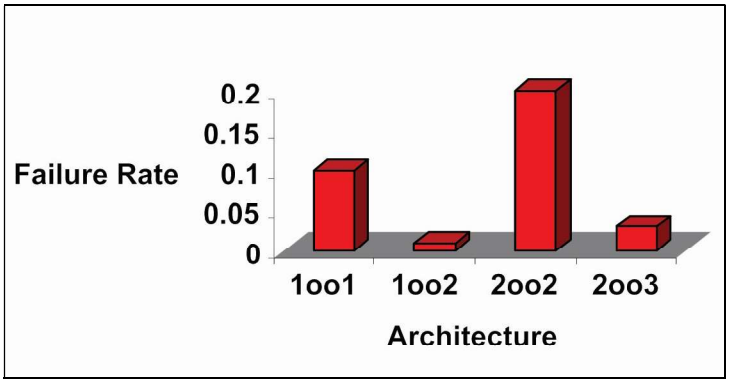
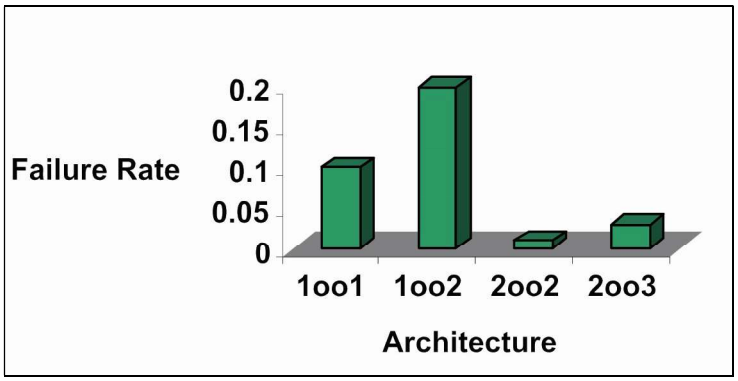
The following graphs show λd and λs versus the sensor architecture used.




-Figure 15 λd vs. circuit



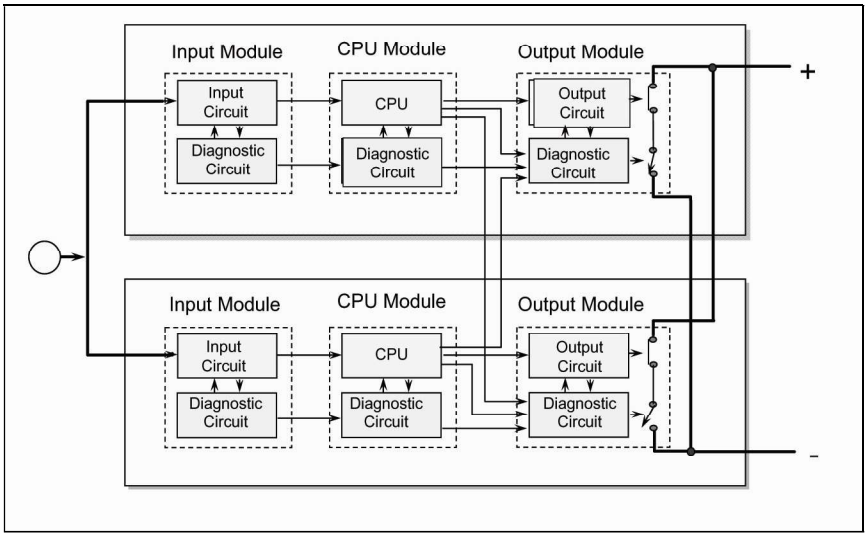

-Figure 16 λs vs. circuit

A 1oo1 can be a simple emergency stop or a single sensor. By increasing the redundancy from 1oo1 to 1oo2, λd is reduced but λs is increased. With a 2oo2 circuit, the redundancy is also increased but λd is doubled because if 1 system fails, the parallel system always remains on standby and therefore a dangerous trip is not signaled. Increasing the redundancy does not necessarily increase safety. The 2oo3 is therefore the most optimal redundant configuration in which both λd and λs are reduced and therefore also the PFD.

Applications:

Safety PLC:

The structure of a PLC system can be found in Fig.11.
Fail safe PLCs are used because of the increased safety and availability of the hardware. The HFT as described in figure 13 is considerably higher than with normal PLCs. To achieve this increased HFT, redundant power supplies and redundant internal communication buses are used. Simple safety PLCs have a 1oo1D version, i.e. the I/O is single and the CPU is redundant. The I/O and CPU are checked for correct operation by means of special diagnostic hardware. The D therefore stands for Diagnostic hardware. Safety PLCs can also be designed as 1oo2D, in which case the I/O is also redundant. This means that these PLCs can be used in SISs up to SIL3. To achieve an even higher HFT, even more I/O and CPUs can be connected in parallel. A 1oo2D system is shown in the following figure:




-Figure 17 1oo2D PLC structure

A burner management system (BMS) is usually equipped with a fail safe PLC due to the high SIL classification for burner and boiler.

Comparison of relay/PLC systems:

The following table provides a comparison between the performance of relay and PLC systems

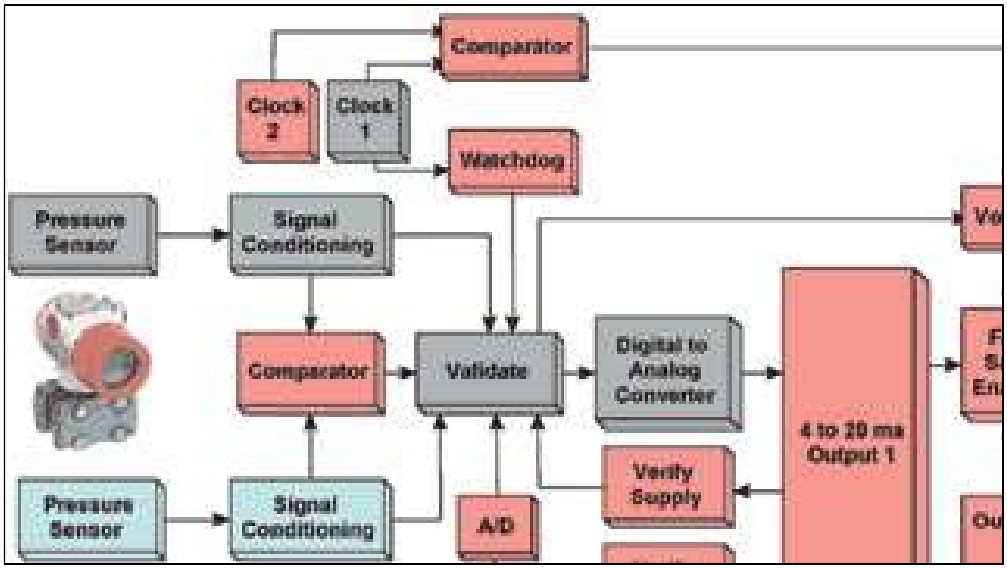
| Type: | Advantage: | Disadvantage | MTBF (year) | RRF |
|---|---|---|---|---|
| Relay system | Low cost, high used, none software, high speed | Reprogramming (new hardware), none diagnosis | 31 | 10000 (SIL3) |
| Normal PLC | Flexible, modular, testing possibilities | Software dependent , common cause failure possible, duration | 32 (with hot backup CPU*) | 240 (SIL2) |
| Safety PLC | High error tolerance, self diagnosis, redundant CPU I/O possible | Duration | > 50,000 | > 100000 (SIL4) |

For MTBF and RRF max. possible values are given.
SIL calculation depends on entire SIF; so sensor, logic solver and final element.
* = a hot backup CPU can directly take over the operation of the original CPU, so there are two CPUs.

Nowadays there are also relays available with a reduced PFD that can therefore be used in a SIF.

## Fail safe transmitter:

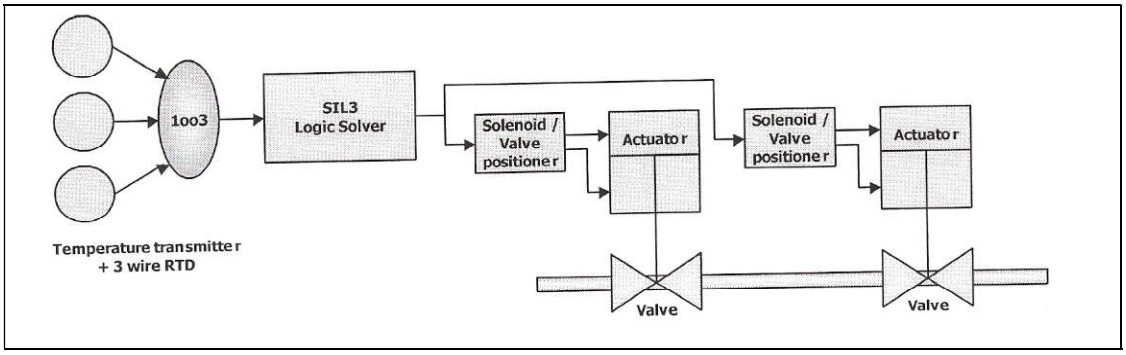
In order to function in a SIF with SIL2, the transmitter sensor must be redundant, the hardware architecture must be redundant, there must be a diagnostic circuit and the output must be fail safe. There are two sensor circuits that generate independent signals that are validated by the microprocessor by comparing them with each other. If the comparison deviates too much, the output is 'up- or downscaled' depending on the fail safe condition that the process requires. An internal diagnostic circuit checks the internal digital variables and the correct operation of the memory. The outgoing 4-20mA is also checked with the expected calculated value. A single SIL2 transmitter can replace two redundantly connected conventional transmitters in a SIL2 SIF. Two redundantly connected SIL2 transmitters can be used in a SIL3 SIF. For this, of course, the total PFD of the SIF must always be calculated. The transmitter architecture is shown in fig.18. Today's smart transmitters have enhanced diagnostic capabilities and digital communication capabilities, but they are not necessarily suitable for failsafe applications.




-Figure 18 Fail safe transmitter construction

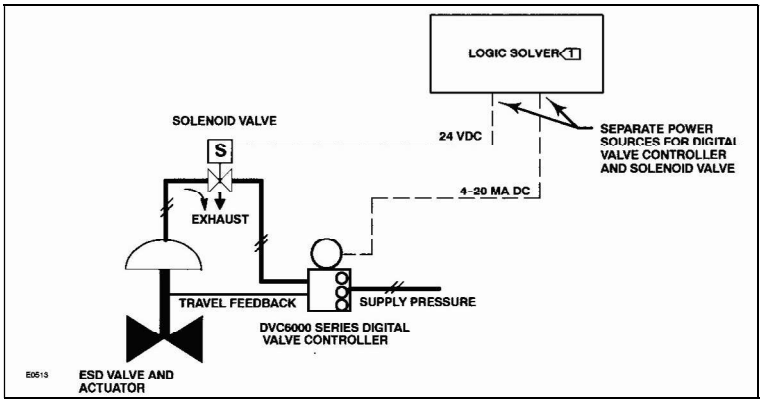
Partial stroke testing:

Shut/off valves usually remain in the open position in a process. Often these valves 'get stuck' just at the moment they should be controlled closed. This causes an unsafe situation. It is therefore necessary to regularly test whether the valves can be controlled open-closed. If these valves are part of a SIF they can be checked during the periodic test. However, this is often done once a year. Tests have shown that the PFD of this SIF is mainly determined by the on/off valve. By testing the valve more often the PFD can be reduced. In the loop below in fig. 19 the PFD calculation showed that it is unsuitable for use in a SIL3 SIF because the valves greatly increase the PFD. A third valve should therefore be used to achieve SIL3 level because this results in a 1oo3 valve control which has a favourable effect on the PFD. By testing the valves more often the PFD can also be improved because the TI is then reduced, so that no third valve is needed. This can be done by means of so-called Partial stroke testing; in this way the valve is closed slightly without going into a full closing stroke. This verifies that the valve is functioning properly without affecting the process that reduces the PFD.




-Figure 19 Partial stroke test configuration

This partial stroke testing can be integrated into an intelligent positioner that is currently available on the market. The entire partial stroke test procedure is thus handled by the positioner, so that the overarching automation system does not have to be loaded. A four-wire SIS positioner system now looks like this:




-Figure 20 Partial stroke test configuration

The SIF for controlling the on/off valve now also consists of a solenoid valve that shuts off the air and a positioner that sends the output signal to 0. This results in a 1oo2 system that reduces the PFD again.

Nowadays, intelligent valve positioners are also available for direct analogue control of a control valve with an increased SIL classification. Shut-off valves are also available that have such a low PFD that they can be used in a SIF (up to SIL3).

PFD/SIL calculation (using software):

Nowadays, software is available for calculating complete SIS systems, whereby a PFD/SIL calculation can be made for multiple SIFs. Well-known programs include: SIFpro, SILver and SILence. The American institute Exida has developed a lot of software. An agency that has a lot of reliability and PFD data available is OREDA, i.e. Offshore Reliability Data. In the following figures 21-23, some calculations are shown.

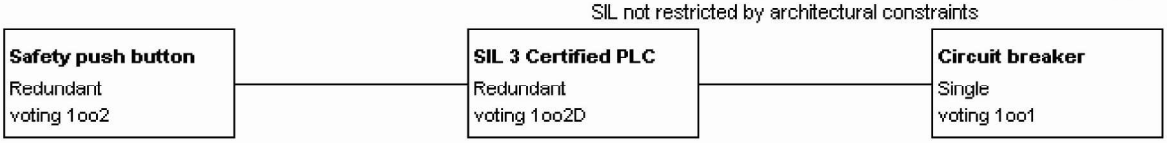
| Component | Source | lambda(d) | lambda(s) | TI (yr) | Voting | Bèta | MTTR | PFD | STR |
|---|---|---|---|---|---|---|---|---|---|
| TE + TT | OREDA 97 | 3.8650 | 3.8650 | 1 | 1oo1 | 2% | 72h | 1.7207E-02 | 3.3857E-02 |
| | OREDA 97 | | | 5 | 1oo3 | 2% | 72h | 2.2748E-03 | 1.0157E-01 |
| dP FE + FT | OREDA 97 | 1.3800 | 1.3800 | 1 | 1oo1 | 2% | 72h | 6.1439E-03 | 1.2080E-02 |
| Generic LT | OREDA 97 | 3.0450 | 3.0450 | 1 | 1oo1 | 2% | 72h | 1.3556E-02 | 2.6670E-02 |
| | OREDA 97 | | | 1 | 1oo2D | 2% | 72h | 6.5737E-05 | 5.3348E-02 |
| Safety PLC | - | | | - (D) | 1oo2D | 2% | 72h | 5.0000E-04 | 5.0000E-03 |
| XEV (DTT) | OREDA 97 | 1.9030 | 7.6110 | | 1oo1 | 2% | 72h | | |
| | OREDA 97 | | | 1 | 2oo2 | 2% | 72h | 1.6944E-02 | 8.8898E-03 |
| | OREDA 97 | | | 1 | 1oo2(2oo2) | 2% | 72h | 2.8710E-04 | 1.7780E-02 |
| XV ESD Ball 5.1-10" | OREDA 97 | 5.3100 | 5.3100 | 0.25 | 1oo1 | 2% | 72h | 6.1968E-02 | 4.6516E-01 |
| | OREDA 97 | | | 0.5 | 1oo1 | 2% | 72h | 1.2011E-01 | 4.6516E-01 |
| | OREDA 97 | | | 1 | 1oo1 | 2% | 72h | 2.3640E-01 | 4.6516E-01 |
| | | | | | | | | | |
| | | | | | | | | | |
| note 1 : lambda : failures / 10E6 hours | | | | | | | | | |
| note 2 : low demand rates, systems not in continuous mode | | | | | | | | | |
| note 3 : D = internal diagnostic | | | | | | | | | |
| note 4 : failure rates are assumed to be constant and indepent of time (no burn-in or wear-out is taken into account) | | | | | | | | | |

-Figure 21 PFD/SIL calculation

| Group name | Voting | Group type | β [%] | Component name | Type A/B | λ [1/h] | [% ]λ Safe | DC Safe | DC Dang. | MTTR [hour] | TI [Months] | PFDavg Part |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Safety push button | 1oo2 | Redundant | 1 | ESW-1 | A | 1.0E-6 | 60 | 0 | 0 | 4 | 12 | 3.90E-05 |
| SIL 3 Certified PLC | 1oo2D | Redundant | 1 | GA-I | B | 2.5E-6 | 80 | 60 | 50 | 4 | 12 | 2.35E-05 |
| Circuit breaker | 1oo1 | Single | - | LV-CB1 | A | 1.5E-6 | 92 | 0 | 0 | 4 | 12 | 5.25E-04 |

Fractional Process Deadtime
Spurious Trip Rate per year

Average Probability of Failure on Demand **5.88E-04**
Safety Integrity Level **3**
Risk Reduction Factor **1.70E+03**
SIL not restricted by architectural constraints




-Figure 22 PFD/SIL calculation

## Sensor Part Information

| Sensor Group(s) | Edit |
|---|---|
| (1) Pressure group | Details |
| PFDavg Sensor Part: | 3.25E-05 |
| MTTFS Sensor Part (years): | 123.23 |
| Maximum SIL allowed (Architectural Constraints): | 2 |

## Logic Solver Part Information

| Logic Solver | Edit |
|---|---|
| (1) Safety PLC | Details |
| PFDavg Logic Solver Part | 2.00E-03 |
| MTTFS Logic Solver Part (years) | 3.27 |
| Maximum SIL allowed (Architectural Constraints): | 2 |

## Final Element Part Information

| Final Element Group(s) | Edit |
|---|---|
| (1) Shutoff valves | Details |
| PFDavg Final Element Part: | 1.84E-03 |
| MTTFS Final Element Part (years): | 12.39 |
| Maximum SIL allowed (Architectural Constraints): | 2 |

## SIF Performance Metrics

| Safety Instrumented Function | Preview |
|---|---|
| Average Probability of Failure on Demand (PFDavg) | 3.86E-03 |
| Safety Integrity Level | 2 |
| Safety Integrity Level (Architectural Constraints) | 2 |
| Risk Reduction Factor | 259 |
| MTTFS (years) | 2.53 |

-Figure 23 PFD/SIL calculation