Safety considerations

Dr. Josef Börcsök, HIMA Paul Hildebrandt GmbH + Co KG

A considerable amount of data is required in order to be able to assess safety systems properly. One of the most important criteria is consideration of the distribution of failures over a system's life cycle.

In considering such failures, a basic distinction is made between safe and dangerous failures. Safe failures are further divided into

- safe detectable, and
- safe undetectable

failures. Safe failures, whether detected or undetected, are failures that exert no influence on the safe operation of the system. This is not the case with dangerous failures. These failures, when they occur, lead to a hazardous situation in the system which may even, under certain circumstances, seriously endanger human life. These failures are also divided into

- dangerous detectable, and
- dangerous undetectable

failures. In the event of dangerous detectable failures, however, the safety system, provided it is appropriately designed, can bring the entire system or plant into a safe state. It is undetectable, dangerous failures that constitute a critical state. No safety system is able to detect such failures when they occur. They may be present in the system until it switches off or, in the worst-case scenario, until it fails dangerously without the user being aware of it.

HIMA systems are always developed, produced and certified in accordance with the prevailing national and international standards. One of the most important international standards in this regard is IEC/EN 61508. IEC/EN 61508 covers not only pure arithmetical values, such as PFD and PFH, which provide information about the probability of system failure, but also a system's entire safety life cycle.

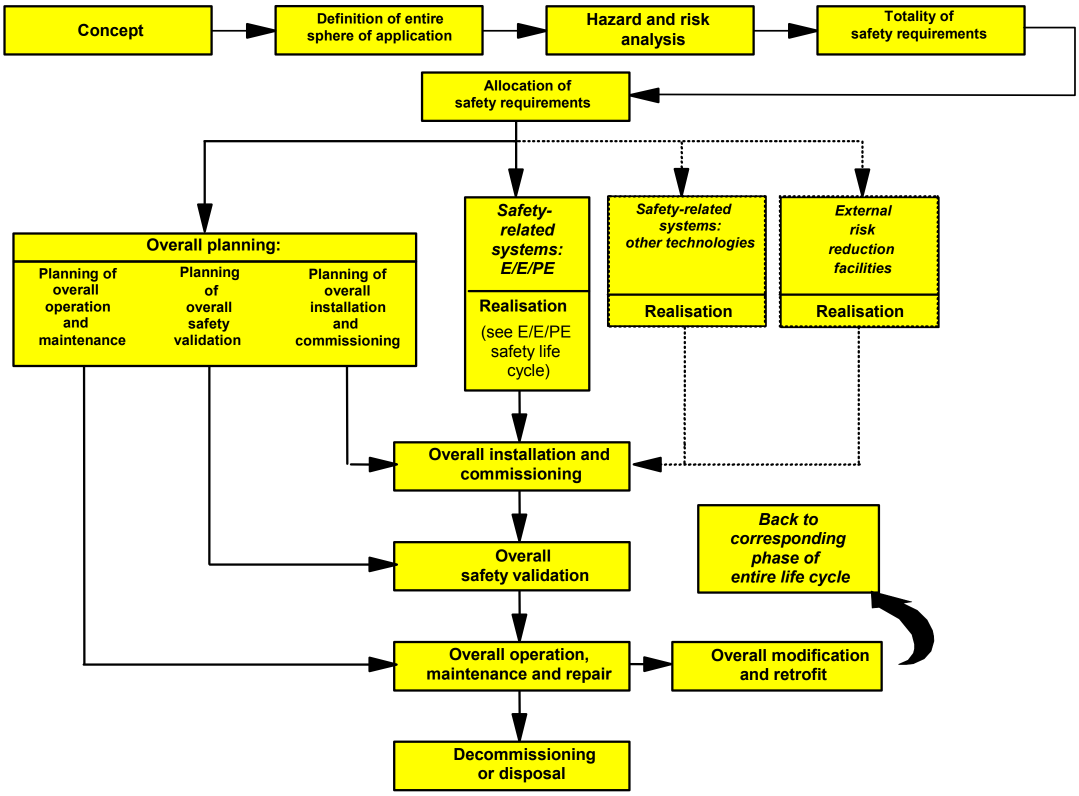


Figure 1: Representation of the safety life cycle

Consideration of the safety life cycle facilitates a systematic approach to the problems of functional safety. Moreover, the SIL capability each individual safety function must have is also laid down here (Table 1).

Table 1: SILs for low and high demand modes of operation

Safety integrity level (SIL)	**Low demand mode of operation** (mean probability of failure to perform design function on demand)	**High demand mode of operation** (probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-4}$ to $<10^{-3}$	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-3}$ to $<10^{-2}$	$\geq 10^{-7}$ to 10^{-6}
1	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$

Specification of the demands on hardware is an important part of IEC/EN 61508. The safety life cycle of the hardware, the architecture requirements as well as type A (whose behaviour in the event of failure is fully known) and type B (whose behaviour in the event of failure is not fully known) subsystems and the corresponding SFF (safe failure fraction) are also defined here.

In order to draw up a specification of the safety function, precise information is required on how the required safety is to be achieved and maintained.

Table 2: Type A subsystems and Type B subsystems

	Type A			**Type B**		
Safe failure fraction	**Hardware failure tolerance**			**Hardware failure tolerance**		
	0 failures	**1 failure**	**2 failures**	**0 failures**	**1 failure**	**2 failures**
< 60 %	SIL 1	SIL 2	SIL 3	Not allowed	SIL 1	SIL 2
60 % - < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90 % - < 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

A safety-related system must be designed in accordance with the safety specification drawn up for it. The hardware architecture requirement has to be matched to the required SIL capability. This safety integrity level is limited by the hardware failure tolerance and the share of non-dangerous errors (Table 2).

For example, the equations for the PFD/PFH calculations of different HIMA systems should be given here. In contrast to many other reports currently circulating, these observations are based on the applicable equations in IEC/EN 61508 and relate to a 10-year time period. Many reports are to be found that relate to a time period of half a year and are based on the simplified ISA equations but passed off as the IEC/EN 61508 figures. These calculations do not include common-cause failures or the system's diagnostic coverage capability. This gives rise to sometimes considerable discrepancies in the PFD figures. These consequences are always taken into account in all calculations and certification processes relating to HIMA systems, which consequently conform fully to IEC/EN61508.

This report uses various examples of actual values to illustrate the calculation of the safety integrity level of various HIMA systems. First, however, the individual IEC/EN 61508 equations for the various system architectures must be presented in order to make a clear distinction between them and the ISA norm.

Equation for determining PFD of a 1oo1 system:

$$
\begin{aligned}
PFD_{G,1oo1} &= (\lambda_{DU} + \lambda_{DD}) \cdot t_{CE} \\
&= \lambda_D \cdot t_{CE} \qquad\qquad\qquad (1)\\
&= \lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR\right) + \lambda_{DD} \cdot MTTR
\end{aligned}
$$

with

$$
t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \qquad (2)
$$

Equation for determining PFH of a 1oo1 system:

$$
PFH_{G,1oo1} = \lambda_{DU} \qquad (3)
$$

Equation for determining PFD of a 1oo2 system:

$$
\begin{aligned}
PFD_{G,1oo2} = {} & 2 \cdot ((1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU})^2 \cdot t_{CE} \cdot t_{GE} \\
& + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR\right)
\end{aligned} \qquad (4)
$$

with

$$
t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \qquad (5)
$$

$$
t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \qquad (6)
$$

Equation for determining the PFH of a 1oo2 system:

$$
\begin{aligned}
PFH_{G,1oo2} = {} & 2 \cdot ((1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU})^2 \cdot t_{CE} \\
& + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU}
\end{aligned} \qquad (7)
$$

with

$$
t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \qquad (8)
$$

Equation for determining the PFD of a 2oo3 system:

$$
\begin{aligned}
PFD_{G,2oo3} = {} & 6 \cdot \left((1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU} \right)^2 \cdot t_{CE} \cdot t_{GE} \\
& + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR \right)
\end{aligned}
\qquad (9)
$$

with

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \qquad (10)$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{3} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \qquad (11)$$

Equation for determining the PFH of a 2oo3 system:

$$
\begin{aligned}
PFH_{G,2oo3} = {} & 6 \cdot \left((1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU} \right)^2 \cdot t_{CE} \\
& + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU}
\end{aligned}
\qquad (12)
$$

with

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \qquad (13)$$

Two further important indicators for safety-related systems are the SFF (safe failure fraction) and the DC (diagnostic coverage) factor. The SFF can be calculated by means of the following equation:

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}} \qquad (14)$$

The DC factor can be determined by means of the following equation:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} \qquad (15)$$

The SFF represents the share of safety-relevant failures and the DC factor the level of diagnostic coverage. The meaning of the individual factors in these equations is as follows:

β	weighting factor for dangerous, undetected, common-cause failures
β_D	weighting factor for dangerous, detected, common-cause failures
λ_D	system failure rate due to dangerous failures
λ_{DD}	system failure rate due to dangerous, detected failures
λ_{DU}	system failure rate due to dangerous, undetected failures
MTTR	mean time to repair
PFD_G	average probability of failure on low demand
PFH_G	average probability of failure on high demand
T_1	proof test time
t_{CE}	average channel-related failure time
t_{GE}	average system-related failure time

In order to determine the safety integrity of safety-related systems consisting of several individual systems, the mean probability of failure PFD_{sys} or PFH_{sys} is required for the whole system. PFD_{sys} or PFH_{sys} is determined by obtaining and summing the mean probabilities for the individual systems.

$$PFD_{sys} = PFD_S + PFD_L + PFD_{FE} \qquad (16)$$

or

$$\mathrm{PFH}_{\mathrm{sys}} = \mathrm{PFH}_{\mathrm{S}} + \mathrm{PFH}_{\mathrm{L}} + \mathrm{PFH}_{\mathrm{FE}} \qquad (17)$$

In order to determine the mean probability for each part of the system, the following information must be available:

- the basic architecture
- the diagnosis coverage of each channel
- the failure rate per hour for each channel
- the factors β and β_D for common-cause failures

This last list introduces the notion of ‘common-cause failures’. The aim here is to detect common-cause failures as early as possible and to bring the system into a safe state. The β-factor is introduced as the fraction of common-cause failures to normal (single) failures.

In the following, various system architectures are presented and the PFD/PFH values for the individual systems established. The following parameters should be identical for all systems

β_D = common-cause factor for detectable failures
β = common-cause factor for undetectable failures
T_1 = maintenance interval
$MTTR$ = mean time to repair

And have the following values

β_D = 1%
β = 2%
T_1 = 10 years
$MTTR$ = 8 hours

The following individual systems are used in various configurations in the example calculations:

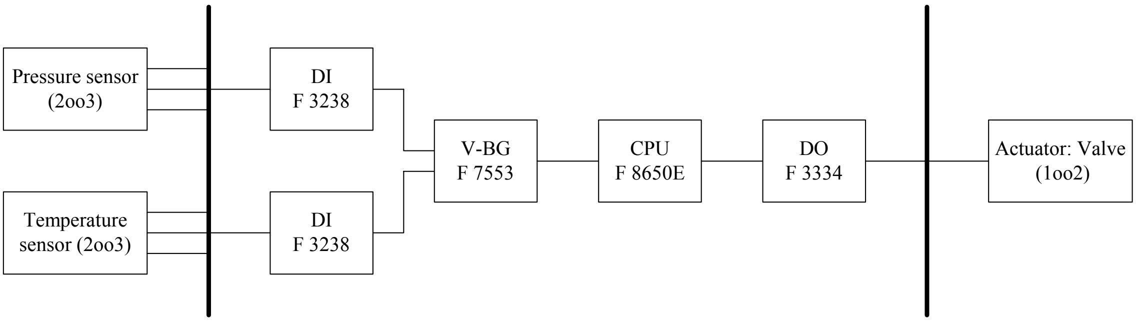
Module	Pressure sensor	Temp. sensor	DI: F 3236	DI: F 3238	AI: F 6214	AI: F6217	V-BG: F 7553	CPU: F 8650E	DO: F 3330	DO: F 3334	AO: F 6705	Actuator: valve
lambda_b in [1/h]			7,43E-07	1,09E-06	1,11E-06	1,11E-06	5,60E-07	2,08E-06	8,17E-07	6,21E-07	9,45E-07	
MTTF in [years]			153,66	104,60	102,80	103,17	203,99	54,79	139,78	183,91	120,79	
Proof-check interval T_1 in [years]	10	10	10	10	10	10	10	10	10	10	10	10
MTTR in [h]	8	8	8	8	8	8	8	8	8	8	8	8
β_D	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01
β	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02	0,02
PFD_{1oo1} in [1]			9,79E-06	2,38E-05	5,12E-05	2,87E-05	9,78E-06	2,94E-05	8,18E-06	1,40E-05	1,86E-05	
PFH_{1oo1} in [1/h]			2,05E-10	5,14E-10	1,11E-09	9,64E-10	5,76E-10	4,08E-09	6,58E-10	6,87E-10	6,17E-10	
$PFD_{1oo2/2oo3}$ in [1] *)	1,00E-04	1,56E-04										3,33E-05
$PFH_{1oo2/2oo3}$ in [1/h] *)	2,22E-08	3,47E-08										7,40E-09
TÜV claimed SIL			3	3	3	3	3	3	3	3	3	

For all the following architectures, the following two points should always apply:

- sensors in 2oo3 architecture
- actuators in 1oo2 architecture

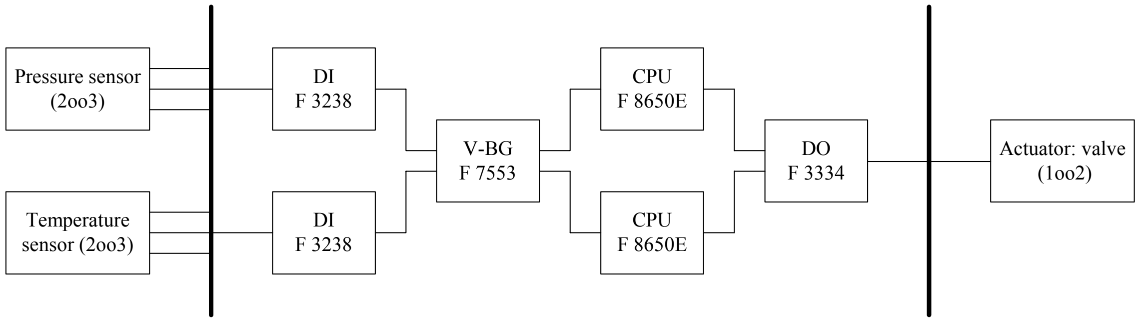
The following systems are to be investigated:

System 1 (Digital Loop 1)



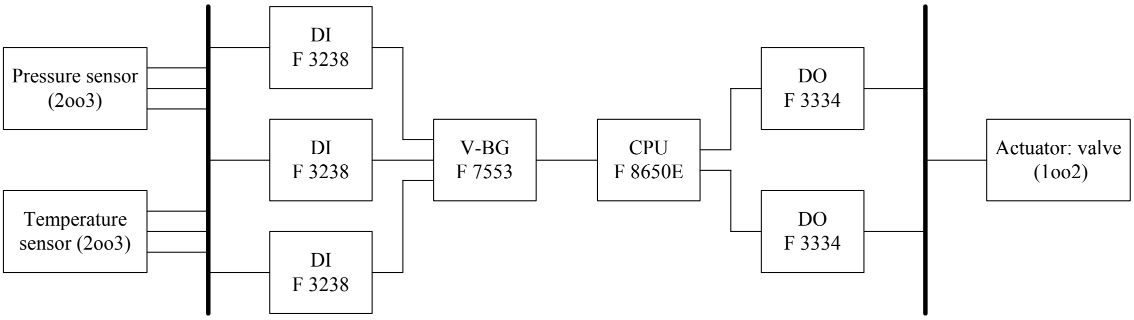
	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1.00E-04	2.22E-08	3	3
Temp. sensor	2oo3	1.56E-04	3.47E-08	3	3
DI: F 3238	1oo2	4.63E-07	1.55E-09	4	3
V-BG: F 7553	1oo1	9.78E-06	5.76E-10	4	4
CPU: F 8650E	1oo1	2.94E-05	4.08E-09	3	3
DO: F 3334	1oo1	1.40E-05	6.87E-10	4	4
Actuator: valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor or actuator		5.36E-05	6.90E-09	4	4
System with sensor and actuator		3.43E-04	7.12E-08	3	3
TÜV claimed SIL for system without sensor and actuator				3	3

System 2 (Digital Loop 2)



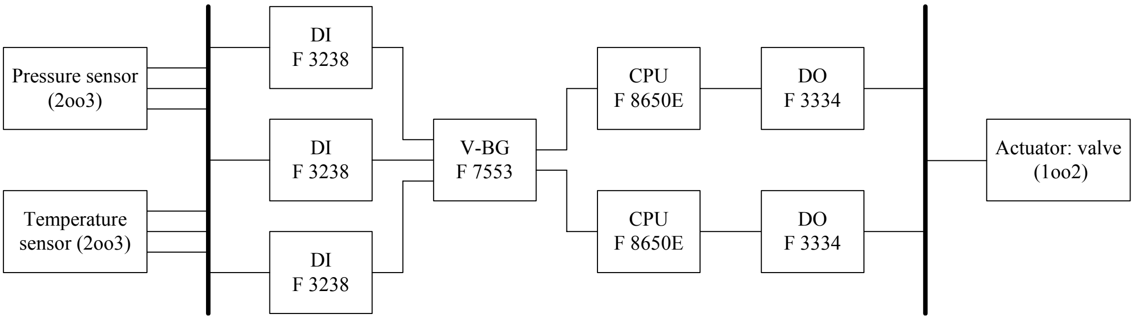
	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1.00E-04	2.22E-08	3	3
Temp. sensor	2oo3	1.56E-04	3.47E-08	3	3
DI: F 3238	1oo2	4.63E-07	1.55E-09	4	3
V-BG: F 7553	1oo1	9.78E-06	5.76E-10	4	4
CPU: F 8650E	1oo2	3.08E-06	7.24E-09	4	3
DO: F 3334	1oo1	1.40E-05	6.87E-10	4	4
Actuator: valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor or actuator		2.73E-05	1.01E-08	4	3
System with sensor and actuator		3.17E-04	7.43E-08	3	3
TÜV claimed SIL for system without sensor or actuator				3	3

System 3 (Digital Loop 3)



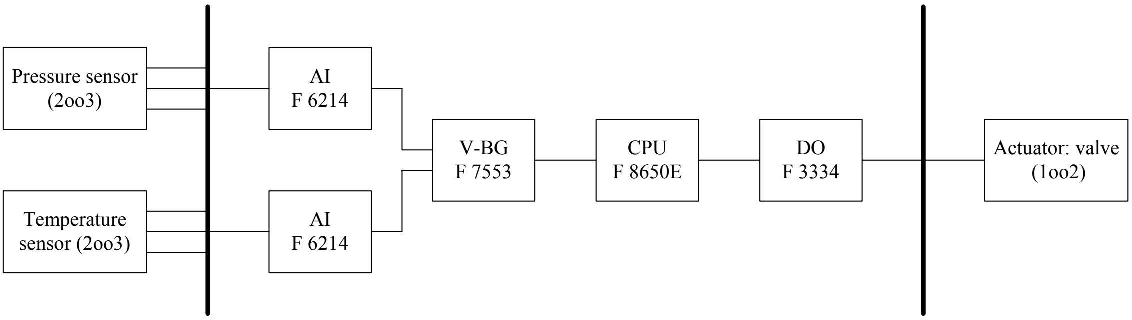
	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1.00E-04	2.22E-08	3	3
Temp. sensor	2oo3	1.56E-04	3.47E-08	3	3
DI: F 3238	2oo3	4.65E-07	1.57E-09	4	3
V-BG: F 7553	1oo1	9.78E-06	5.76E-10	4	4
CPU: F 8650E	1oo1	2.94E-05	4.08E-09	3	3
DO: F 3334	1oo2	6.09E-07	1.29E-09	4	4
Actuator: valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor or actuator		4.03E-05	7.52E-09	4	4
System with sensor and actuator		3.30E-04	7.18E-08	3	3
TÜV claimed SIL for system without sensor or actuator				3	3

System 4 (Digital Loop 4)



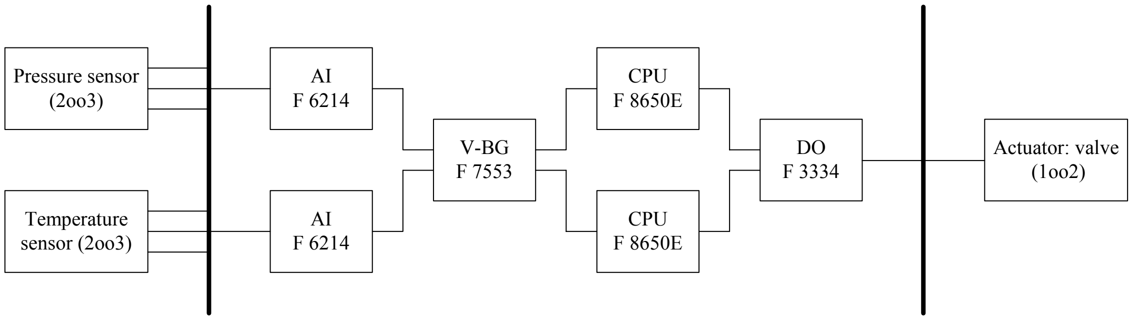
	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1.00E-04	2.22E-08	3	3
Temp. sensor	2oo3	1.56E-04	3.47E-08	3	3
DI: F 3238	2oo3	4.65E-07	1.57E-09	4	3
V-BG: F 7553	1oo1	9.78E-06	5.76E-10	4	4
CPU: F 8650E	1oo2	3.08E-06	7.24E-09	4	3
DO: F 3334	1oo2	6.09E-07	1.29E-09	4	4
Actuator: valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor or actuator		1.39E-05	1.07E-08	4	3
System with sensor and actuator		3.03E-04	7.50E-08	3	3
TÜV claimed SIL for system without sensor or actuator				3	3

System 5 (Analog-Digital Loop 1)



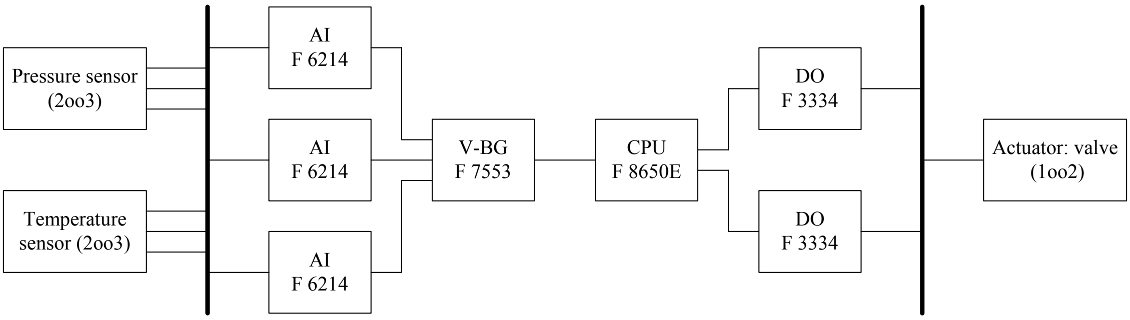
	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1.00E-04	2.22E-08	3	3
Temp. sensor	2oo3	1.56E-04	3.47E-08	3	3
AI: F 6214	1oo2	1.00E-06	3.44E-09	4	3
V-BG: F 7553	1oo1	9.78E-06	5.76E-10	4	4
CPU: F 8650E	1oo1	2.94E-05	4.08E-09	3	3
DO: F 3334	1oo1	1.40E-05	6.87E-10	4	4
Actuator: valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor or actuator		5.42E-05	8.78E-09	4	4
System with sensor and actuator		3.43E-04	7.31E-08	3	3
TÜV claimed SIL for system without sensor or actuator				3	3

System 6 (Analog-Digital Loop 2)



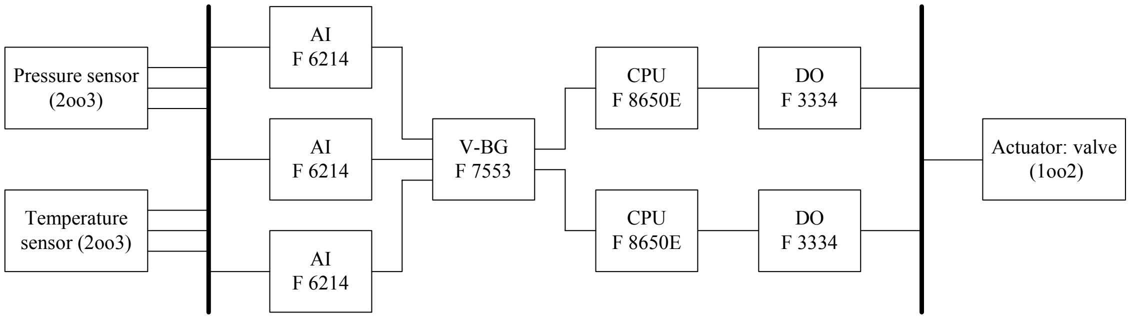
	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1.00E-04	2.22E-08	3	3
Temp. sensor	2oo3	1.56E-04	3.47E-08	3	3
AI: F 6214	1oo2	1.00E-06	3.44E-09	4	3
V-BG: F 7553	1oo1	9.78E-06	5.76E-10	4	4
CPU: F 8650E	1oo2	3.08E-06	7.24E-09	4	3
DO: F 3334	1oo1	1.40E-05	6.87E-10	4	4
Actuator: valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor or actuator		2.79E-05	1.19E-08	4	3
System with sensor and actuator		3.17E-04	7.62E-08	3	3
TÜV claimed SIL for system without sensor or actuator				3	3

System 7 (Analog-Digital Loop 3)



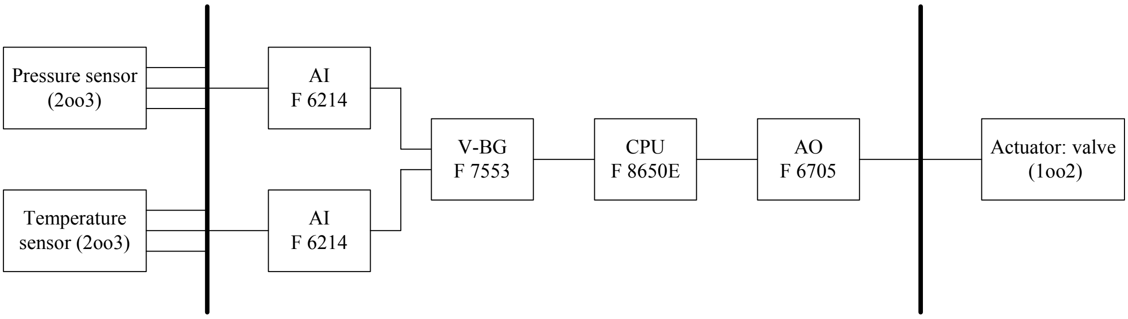
	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1.00E-04	2.22E-08	3	3
Temp. sensor	2oo3	1.56E-04	3.47E-08	3	3
AI: F 6214	2oo3	1.01E-06	3.50E-09	4	3
V-BG: F 7553	1oo1	9.78E-06	5.76E-10	4	4
CPU: F 8650E	1oo1	2.94E-05	4.08E-09	3	3
DO: F 3334	1oo2	6.09E-07	1.29E-09	4	4
Actuator: valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor or actuator		4.08E-05	9.45E-09	4	4
System with sensor and actuator		3.30E-04	7.37E-08	3	3
TÜV claimed SIL for system without sensor or actuator				3	3

System 8 (Analog-Digital Loop 4)



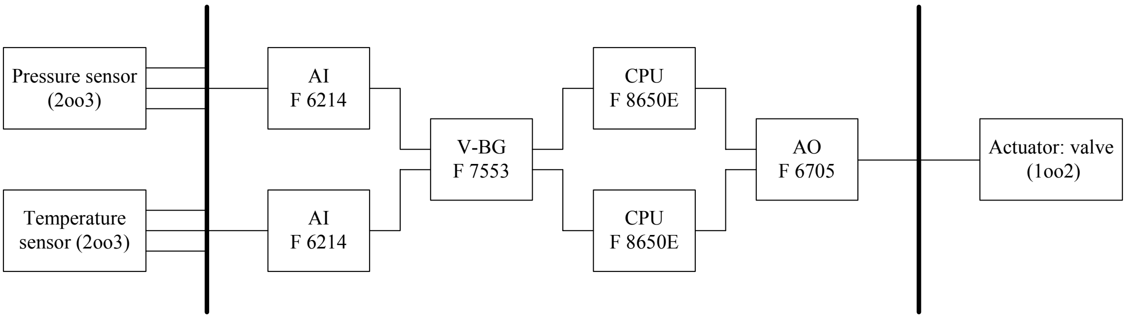
	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1.00E-04	2.22E-08	3	3
Temp. sensor	2oo3	1.56E-04	3.47E-08	3	3
AI: F 6214	2oo3	1.01E-06	3.50E-09	4	3
V-BG: F 7553	1oo1	9.78E-06	5.76E-10	4	4
CPU: F 8650E	1oo2	3.08E-06	7.24E-09	4	3
DO: F 3334	1oo2	6.09E-07	1.29E-09	4	4
Actuator: valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor or actuator		1.45E-05	1.26E-08	4	3
System with sensor and actuator		3.04E-04	7.69E-08	3	3
TÜV claimed SIL for system without sensor or actuator				3	3

System 9 (Analog Loop 1)



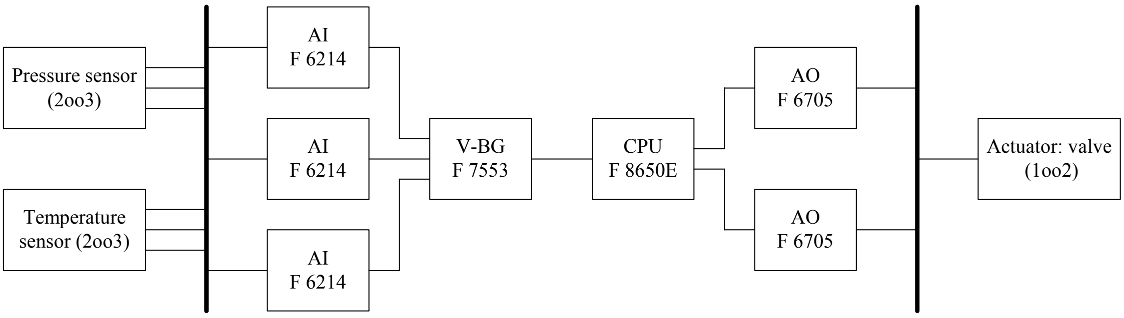
	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1.00E-04	2.22E-08	3	3
Temp. sensor	2oo3	1.56E-04	3.47E-08	3	3
AI: F 6214	1oo2	1.00E-06	3.44E-09	4	3
V-BG: F 7553	1oo1	9.78E-06	5.76E-10	4	4
CPU: F 8650E	1oo1	2.94E-05	4.08E-09	3	3
AO: F 6705	1oo1	1.86E-05	6.17E-10	3	4
Actuator: valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor or actuator		5.88E-05	8.71E-09	4	4
System with sensor and actuator		3.48E-04	7.30E-08	3	3
TÜV claimed SIL for system without sensor or actuator				3	3

System 10 (Analog Loop 2)



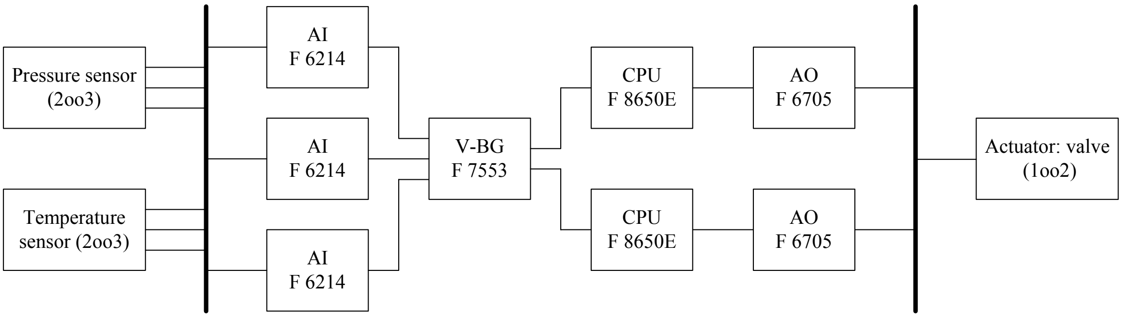
	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1.00E-04	2.22E-08	3	3
Temp. sensor	2oo3	1.56E-04	3.47E-08	3	3
AI: F 6214	1oo2	1.00E-06	3.44E-09	4	3
V-BG: F 7553	1oo1	9.78E-06	5.76E-10	4	4
CPU: F 8650E	1oo2	3.08E-06	7.24E-09	4	3
AO: F 6705	1oo1	1.86E-05	6.17E-10	3	4
Actuator: valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor or actuator		3.25E-05	1.19E-08	4	3
System with sensor and actuator		3.22E-04	7.62E-08	3	3
TÜV claimed SIL for system without system or actuator				3	3

System 11 (Analog Loop 3)



	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1.00E-04	2.22E-08	3	3
Temp. sensor	2oo3	1.56E-04	3.47E-08	3	3
AI: F 6214	2oo3	1.01E-06	3.50E-09	4	3
V-BG: F 7553	1oo1	9.78E-06	5.76E-10	4	4
CPU: F 8650E	1oo1	2.94E-05	4.08E-09	3	3
AO: F 6705	1oo2	3.78E-07	2.26E-09	4	3
Actuator: valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor or actuator		4.06E-05	1.04E-08	4	3
System with sensor and actuator		3.30E-04	7.47E-08	3	3
TÜV claimed SIL for system without sensor or actuator				3	3

System 12 (Analog Loop 4)



	Architecture	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Pressure sensor	2oo3	1.00E-04	2.22E-08	3	3
Temp. sensor	2oo3	1.56E-04	3.47E-08	3	3
AI: F 6214	2oo3	1.01E-06	3.50E-09	4	3
V-BG: F 7553	1oo1	9.78E-06	5.76E-10	4	4
CPU: F 8650E	1oo2	3.08E-06	7.24E-09	4	3
AO: F 6705	1oo2	3.78E-07	2.26E-09	4	3
Actuator: valve	1oo2	3.33E-05	7.40E-09	4	3
System without sensor or actuator		1.43E-05	1.36E-08	4	3
System with sensor and actuator		3.04E-04	7.79E-08	3	3
TÜV claimed SIL for system without sensor or actuator				3	3

Bibliography

[1] IEC/EN 61508: International Standard 61508 Functional Safety: Safety-Related System. Geneva, International Electrotechnical Commission

[2] *Börcsök, J.*: IEC/EN 61508- eine Norm für viele Fälle, atp 44, 2002 Oldenbourg-Verlag

[3] *Börcsök, J.*: Konzepte zur methodischen Untersuchung von Hardwarearchitekturen in sicherheitsgerichteten Anwendungen, erscheint im VDE–Verlag 2003

[4] *Börcsök, J.*: Sicherheits-Rechnerarchitekturen Teil 1 und 2, Vorlesung Universität Kassel 2000/2001

[6] DIN VDE 0801: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme (E/E/PES), (IEC 65A/255/CDV:1998), S. 27f, August 1998.

[7] DIN V 19250: Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen. Beuth Verlag Berlin 1998

[8] DIN VDE 0801/A1: Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben. Beuth Verlag

[9] IEC 60880-2: Software für Rechner mit sicherheitskritischer Bedeutung. 12/2001