Sicherheitsbetrachtungen

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

Um Sicherheitssysteme richtig bewerten zu können sind eine Reihe von Daten notwendig. Eines der wichtigsten Kriterien ist die Betrachtung der Verteilung von Fehlern im Lebenszyklus eines Systems.
Grundsätzlich wird bei der Fehlerbetrachtung zwischen sicheren und gefährlichen Fehler unterschieden. Sichere Fehler werden wiederum in

- sicher entdeckbare
- sicher nicht entdeckbare

Fehler unterschieden. Um sichere Fehlern handelt es sich, wenn diese Fehler, entdeckt oder nicht entdeckt, keinen Einfluss auf die sichere Funktion des Systems darstellen. Bei gefährlichen Fehler ist dieser Umstand nicht gegeben. Diese Fehler führen bei ihrem Auftreten zu einer gefährliche Situation im System, die dann unter Umständen bis hin zur massiven Gefährdung von Menschenleben führen können. Auch diese Fehler werden in

- gefährlich entdeckbare
- gefährlich nicht entdeckbare

eingeteilt. Bei gefährlich entdeckbaren Fehler kann das Sicherheitssystem jedoch noch, sofern es entsprechend ausgelegt ist, das Gesamtsystem oder die Anlage in einen sicher Zustand bringen. Den kritischsten Zustand stellen jedoch die unentdeckbaren, gefährlichen Fehler dar. Bei ihrem Auftreten besteht bei keinem Sicherheitssystem die Möglichkeit der Aufdeckung. Sie können im System bis zu dessen Abschalten, oder im schlimmsten Fall bis zu dessen gefährlichem Ausfall vorhanden sein, ohne dass der Anwender davon Kenntnis hat.

HIMA-Systeme werden grundsätzlich nach den geltenden nationalen und internationalen Normen entwickelt, produziert und zertifiziert. Eine der wichtigsten Internationalen Normen in diesem Zusammenhang stellt die IEC/EN 61508 dar. Die IEC/EN 61508 betrachtet nicht nur reine Zahlenwerte, wie PFD und PFH die Aussagen über Fehlerwahrscheinlichkeiten der Systeme machen, sondern sie umfasst den gesamten Sicherheitslebenszyklus eines Systems.

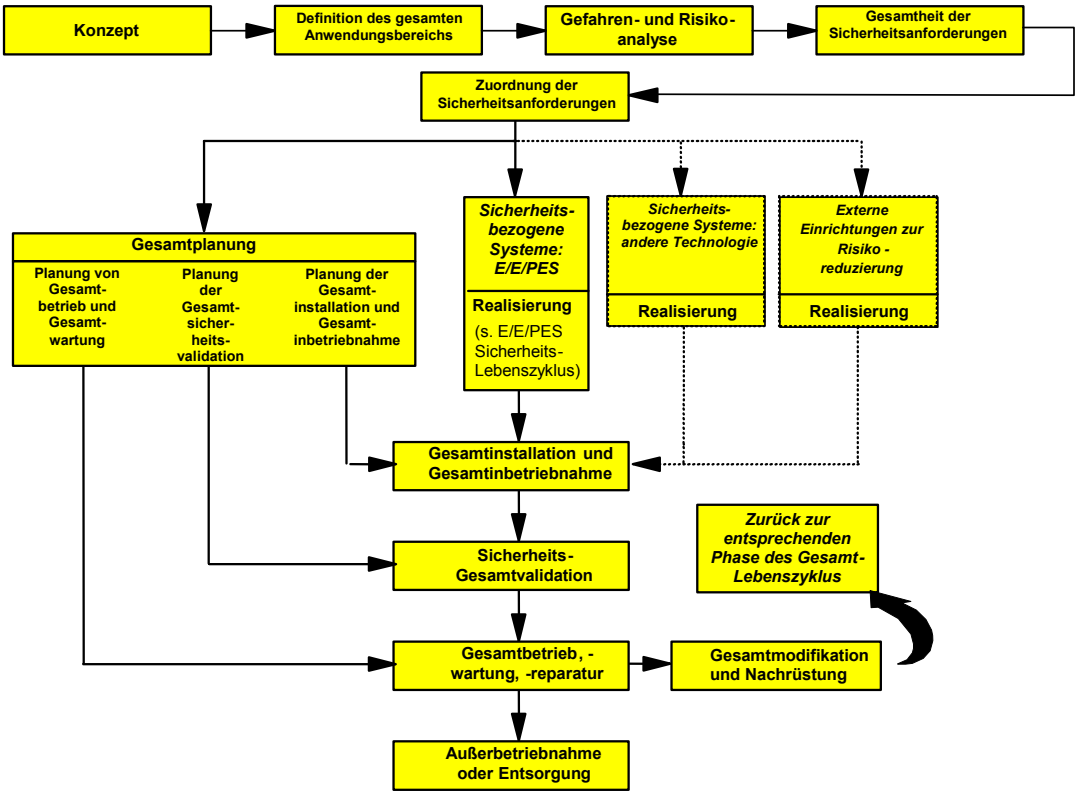


Bild 1: Darstellung des Sicherheitslebenszyklus

Die Betrachtung des Sicherheitslebenszyklus ermöglicht die systematische Herangehensweise an die Probleme der funktionalen Sicherheit. Weiter wird hier festgelegt, welchen SIL-Grad jede einzelne Sicherheitsfunktion aufweisen muss (Tabelle 1).

Tabelle 1: SIL niedrige und hohe Anforderungsrate

Sicherheits Integritätslevel (SIL)	**Betriebsart mit niedriger Anforderungsrate** (mittlere Wahrscheinlichkeit eines Ausfalls der Sicherheitsfunktion bei Anforderung)	**Betriebsart mit hoher Anforderungsrate** (Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde)
4	$\geq 10^{-5}$ bis $<10^{-4}$	$\geq 10^{-9}$ bis $<10^{-8}$
3	$\geq 10^{-4}$ bis $<10^{-3}$	$\geq 10^{-8}$ bis $<10^{-7}$
2	$\geq 10^{-3}$ bis $<10^{-2}$	$\geq 10^{-7}$ bis $<10^{-6}$
1	$\geq 10^{-2}$ bis $<10^{-1}$	$\geq 10^{-6}$ bis $<10^{-5}$

Ein wichtiger Teil der IEC/EN 61508 ist die Spezifikation der Anforderungen an die Hardware. Weiter werden hier der Sicherheitslebenszyklus der Hardware, die Architekturanforderungen sowie die Typ A (bei diesen Systemen ist das Verhalten im Fehlerfall vollständig bekannt) und Typ B Subsystemen (bei diesen Systemen ist das Verhalten im Fehlerfall nicht vollständig bekannt) und der zugehörige SFF (Safe Failure Fraction) definiert.

Um eine Spezifikation der Sicherheitsfunktion zu erstellen, sind genaue Angaben darüber notwendig, wie die benötigte Sicherheit erreicht und beibehalten werden soll.

Tabelle 2: Typ A Subsysteme und Typ B Subsysteme

	Typ A			**Typ B**		
Anteil der ungefährlichen Fehler	**Hardware Fehlertoleranz**			**Hardware Fehlertoleranz**		
	0 Fehler	**1 Fehler**	**2 Fehler**	**0 Fehler**	**1 Fehler**	**2 Fehler**
< 60 %	SIL 1	SIL 2	SIL 3	Nicht erlaubt	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

Der Entwurf eines sicherheitsgerichteten Systems muss in Übereinstimmung mit der erstellten Sicherheitsspezifikation erfolgen. Dabei muss die Hardware-Architekturanforderung dem geforderten SIL-Level angepasst sein. Diese Integritätsebene wird durch die Fehlertoleranz der Hardware und dem Anteil der ungefährlichen Fehler (Tabelle 2) begrenzt.

Beispielhaft sollen hier die Gleichungen für die PFD-/PFH-Berechnungen unterschiedlicher HIMA-Systeme angegeben werden. Diese Betrachtungen erfolgen, im Gegensatz zu vielen anderen im Moment kursierenden Darstellungen auf den gültigen Gleichungen der IEC/EN61508 und beziehen sich auf ein Zeitintervall von 10 Jahren. Häufig sind Darstellungen zu finden die sich auf ein Zeitintervall von einem halben Jahr beziehen und auf den vereinfachten Gleichungen der ISA basieren und als Zahlen der IEC/EN 61508 ausgegeben werden. Bei diesen Berechnungen fehlen die Betrachtungen der Fehler mit gemeinsamen Ursachen sowie die Betrachtung des Diagnoseabdeckungsgrades des Systems. Dadurch ergeben sich zum Teil beträchtliche Abweichungen in den PFD-Zahlen. HIMA-Systeme werden grundsätzlich immer mit all diesen Betrachtungen berechnet und zertifiziert und sind somit absolut IEC/EN61508 konform.

Für HIMA-Systeme soll in dieser Darstellung anhand realer Werte in verschiedenen Beispielen die Berechnung des Sicherheitsintegritätslevel unterschiedlicher Systeme aufgezeigt werden. Zunächst müssen jedoch, um eine klare Abgrenzung zur ISA-Norm zu erhalten, die einzelnen Gleichungen der IEC/EN 61508 für die verschiedenen Systemarchitekturen dargestellt werden.

PFD-Bestimmungsgleichung für ein 1oo1-System:

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

mit

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

PFH-Bestimmungsgleichung für ein 1oo1-System:

$$\mathrm{PFH}_{\mathrm{G,1oo1}} = \lambda_{\mathrm{DU}} \qquad (3)$$

PFD-Bestimmungsgleichung für ein 1oo2-System:

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

mit

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

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

PFH-Bestimmungsgleichung für ein 1oo2-System:

$$\mathrm{PFH}_{\mathrm{G,1oo2}} = 2\cdot\left(\left(1-\beta_{\mathrm{D}}\right)\cdot\lambda_{\mathrm{DD}}+\left(1-\beta\right)\cdot\lambda_{\mathrm{DU}}\right)^{2}\cdot \mathrm{t}_{\mathrm{CE}} + \beta_{\mathrm{D}}\cdot\lambda_{\mathrm{DD}}+\beta\cdot\lambda_{\mathrm{DU}} \qquad (7)$$

mit

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

PFD-Bestimmungsgleichung für ein 2oo3-System:

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

mit

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

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

PFH-Bestimmungsgleichung für ein 2oo3-System:

$$\mathrm{PFH}_{\mathrm{G,2oo3}} = 6\cdot\left(\left(1-\beta_{\mathrm{D}}\right)\cdot\lambda_{\mathrm{DD}}+\left(1-\beta\right)\cdot\lambda_{\mathrm{DU}}\right)^{2}\cdot \mathrm{t}_{\mathrm{CE}} + \beta_{\mathrm{D}}\cdot\lambda_{\mathrm{DD}}+\beta\cdot\lambda_{\mathrm{DU}} \qquad (12)$$

mit

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

Zwei weitere wichtige Indikatoren für sicherheitsrelevante Systemen stellen der Faktor SFF (Safe Failure Fraction) und der Faktor DC (Diagnostic Coverage Factor) dar. Die Berechnung des SFF kann über die Gleichung

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

erfolgen.

Der DC-Faktor lässt sich mit der Gleichung

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

bestimmen. Hierbei stellt der SFF den Anteil der sicherheitsrelevanten Fehler und der DC-Faktor den Diagnoseaufdeckungsgrad dar. Die einzelnen Faktoren in diesen Gleichungen haben die Bedeutung:

β	Gewichtungsfaktor für gefährliche, nicht entdeckte common-cause-Fehler
β_D	Gewichtungsfaktor für gefährliche, entdeckte common-cause-Fehler
λ_D	Ausfallrate des Systems durch gefährliche Fehler
λ_{DD}	Ausfallrate des Systems durch gefährliche, entdeckte Fehler
λ_{DU}	Ausfallrate des Systems durch gefährliche, nicht entdeckte Fehler
MTTR	Mittlere Reparatur-Ausfallzeit
PFD_G	Mittlere Ausfallswahrscheinlichkeit bei niedriger Anforderung
PFH_G	Mittlere Ausfallswahrscheinlichkeit bei hoher Anforderung
T_1	Zeit-Intervall eines Prüf-Tests
t_{CE}	Kanalbezogene mittlere Ausfallzeit
t_{GE}	Systembezogene mittlere Ausfallzeit

Um die Sicherheitsintegrität von sicherheitsgerichteten Systemen bestehend aus mehreren Einzelsystemen zu bestimmen, benötigt man die mittlere Wahrscheinlichkeit eines Ausfalls PFD_{sys} bzw. PFH_{sys} für das Gesamtsystem. PFD_{sys} bzw. PFH_{sys} wird bestimmt, indem man die mittleren Wahrscheinlichkeiten der Einzelsysteme ermittelt und addiert.

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

bzw.

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

Um die mittlere Ausfallwahrscheinlichkeit für jedes Teilsystem zu bestimmen, müssen folgende Angaben vorhanden sein:

- die zugrunde liegende Architektur
- die Diagnoseabdeckung eines jeden Kanals
- die Ausfallrate pro Stunde für jeden Kanal
- die Faktoren β und β_D für die Ausfälle mit gemeinsamer Ursache

In der letzten Aufzählung ist der Begriff „Ausfälle mit gemeinsamer Ursache“ eingeführt worden. Ziel ist es hierbei, Ausfälle mit gemeinsamer Ursache so früh als möglich zu erkennen und das System in einen sicheren Zustand zu bringen. Der β-Faktor wird als Verhältnis der Wahrscheinlichkeit von Ausfällen mit gemeinsamer Ursache zu der Wahrscheinlichkeit zufälliger Ausfälle eingeführt.

Im folgenden werden verschiedene Systemarchitekturen vorgestellt und der PFD-/PFH-Wert für die einzelnen Systeme ermittelt. Folgende Parameter sollen bei allen Systemen identisch sein

β_D	=	common cause-Faktor für entdeckbare Fehler
β	=	common cause-Faktor für nicht entdeckbare Fehler
T_1	=	Wartungsintervall
MTTR	=	Mittlere Reparatur-Ausfallzeit

und folgende Werte besitzen:

β_D	=	1 %
β	=	2 %
T_1	=	10 Jahre
MTTR	=	8 Stunden

Folgende Einzelsysteme werden bei den Beispielberechnungen in unterschiedlichen Konfigurationen verwendet:

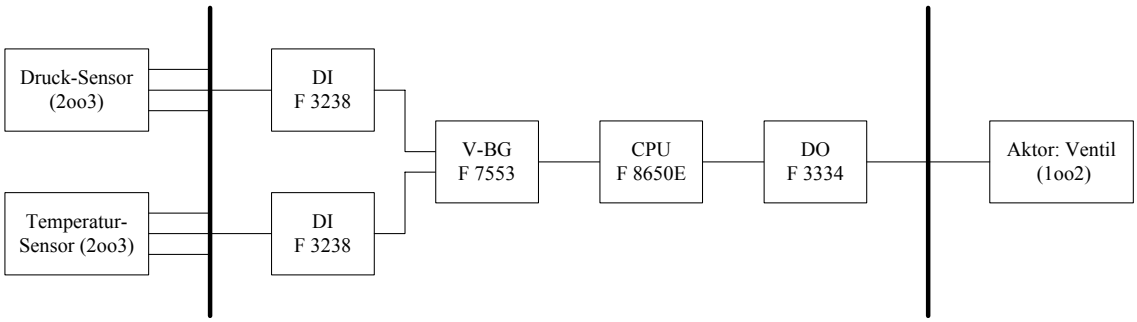
Baugruppe	Druck-Sensor	Temp.-Sensor	DI: F 3236	DI: F 3238	AI: F 6214	AI: F6217	V-BG: F 7553	CPU: F 8650E	DO: F 3330	DO: F 3334	AO: F 6705	Aktor: Ventil
lambda_b in [1/h]			7,43E-07	1,09E-06	1,11E-06	1,11E-06	5,60E-07	2,08E-06	8,17E-07	6,21E-07	9,45E-07	
MTTF in [Jahre]			153,66	104,60	102,80	103,17	203,99	54,79	139,78	183,91	120,79	
Proof-check-Intervall T_1 in [Jahre]	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	

Für alle folgenden Architekturen sollen die beiden folgenden Punkte immer gelten:

- Sensoren in 2oo3-Architektur
- Aktoren in 1oo2-Architekt

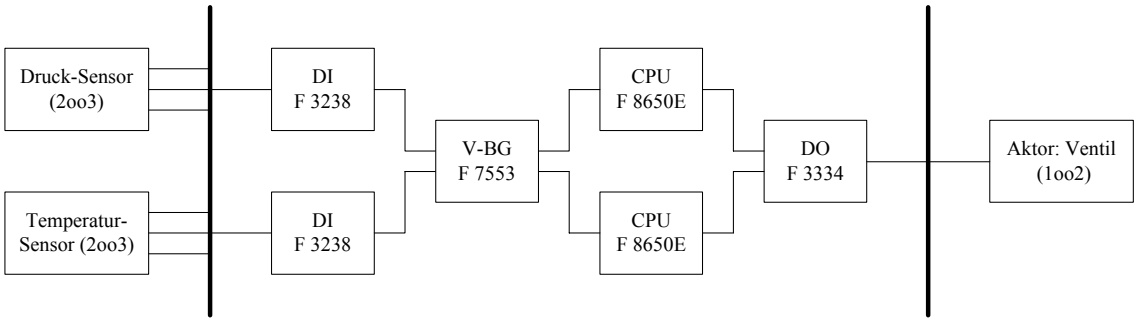
Folgende Systeme sollen untersucht werden:

System 1 (Digital Loop 1)



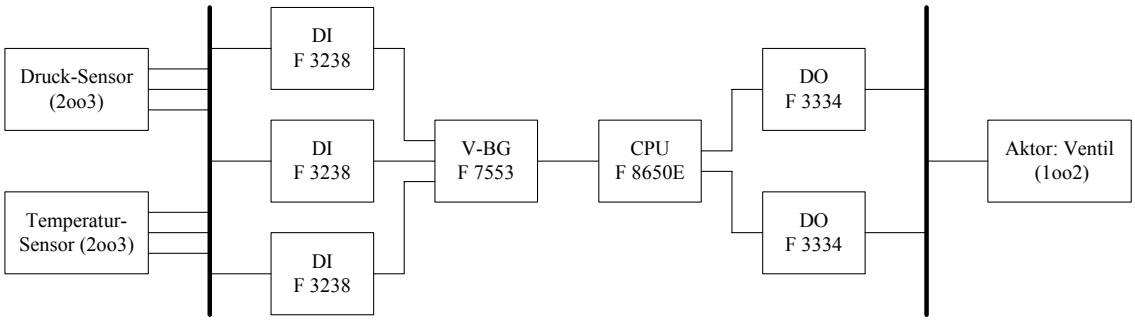
	Architektur	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Druck-Sensor	2oo3	1,00E-04	2,22E-08	3	3
Temperatur-Sensor	2oo3	1,56E-04	3,47E-08	3	3
DI: F 3238	1oo2	4,63E-07	1,55E-09	4	3
V-BG: F 7553	1oo1	9,78E-06	5,76E-10	4	4
CPU: F 8650E	1oo1	2,94E-05	4,08E-09	3	3
DO: F 3334	1oo1	1,40E-05	6,87E-10	4	4
Aktor: Ventil	1oo2	3,33E-05	7,40E-09	4	3
System ohne Sensor und Aktor		5,36E-05	6,90E-09	4	4
System mit Sensor u. Aktor		3,43E-04	7,12E-08	3	3
TÜV claimed SIL für System ohne Sensor und Aktor				3	3

System 2 (Digital Loop 2)



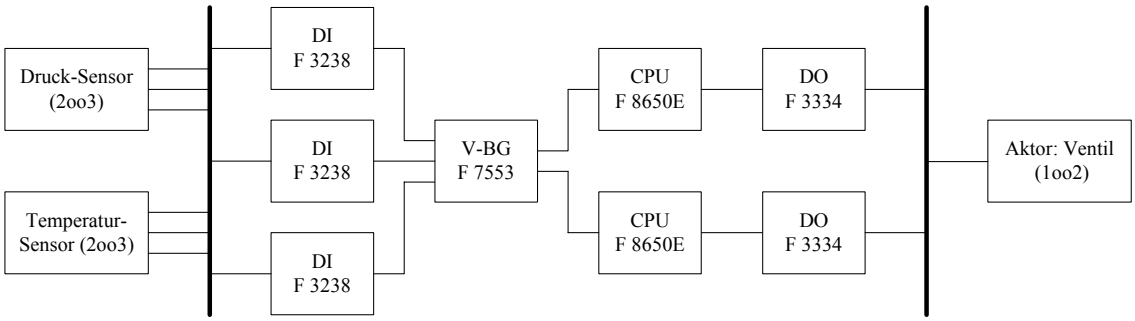
	Architektur	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Druck-Sensor	2oo3	1,00E-04	2,22E-08	3	3
Temperatur-Sensor	2oo3	1,56E-04	3,47E-08	3	3
DI: F 3238	1oo2	4,63E-07	1,55E-09	4	3
V-BG: F 7553	1oo1	9,78E-06	5,76E-10	4	4
CPU: F 8650E	1oo2	3,08E-06	7,24E-09	4	3
DO: F 3334	1oo1	1,40E-05	6,87E-10	4	4
Aktor: Ventil	1oo2	3,33E-05	7,40E-09	4	3
System ohne Sensor und Aktor		2,73E-05	1,01E-08	4	3
System mit Sensor u. Aktor		3,17E-04	7,43E-08	3	3
TÜV claimed SIL für System ohne Sensor und Aktor				3	3

System 3 (Digital Loop 3)



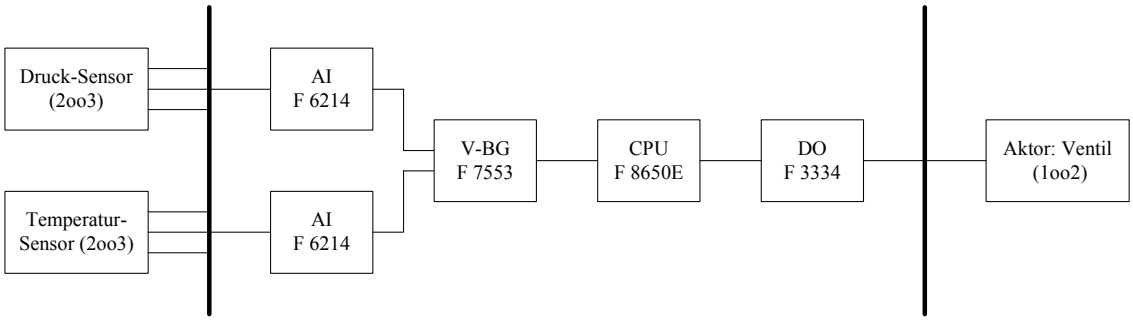
	Architektur	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Druck-Sensor	2oo3	1,00E-04	2,22E-08	3	3
Temperatur-Sensor	2oo3	1,56E-04	3,47E-08	3	3
DI: F 3238	2oo3	4,65E-07	1,57E-09	4	3
V-BG: F 7553	1oo1	9,78E-06	5,76E-10	4	4
CPU: F 8650E	1oo1	2,94E-05	4,08E-09	3	3
DO: F 3334	1oo2	6,09E-07	1,29E-09	4	4
Aktor: Ventil	1oo2	3,33E-05	7,40E-09	4	3
System ohne Sensor und Aktor		4,03E-05	7,52E-09	4	4
System mit Sensor u. Aktor		3,30E-04	7,18E-08	3	3
TÜV claimed SIL für System ohne Sensor und Aktor				3	3

System 4 (Digital Loop 4)



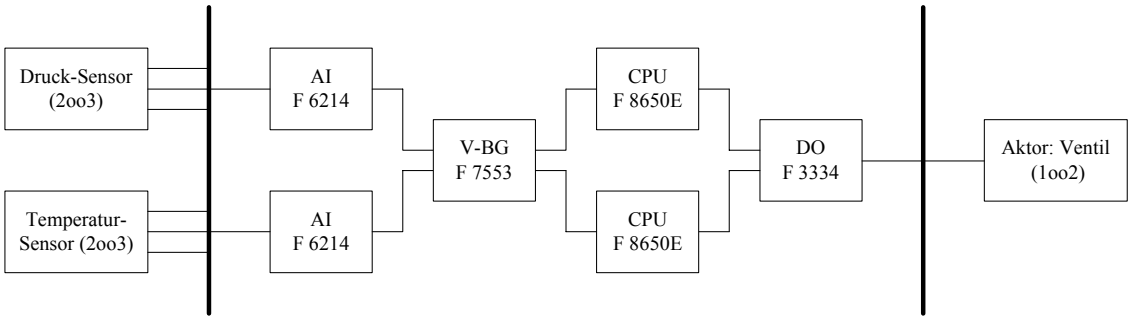
	Architektur	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Druck-Sensor	2oo3	1,00E-04	2,22E-08	3	3
Temperatur-Sensor	2oo3	1,56E-04	3,47E-08	3	3
DI: F 3238	2oo3	4,65E-07	1,57E-09	4	3
V-BG: F 7553	1oo1	9,78E-06	5,76E-10	4	4
CPU: F 8650E	1oo2	3,08E-06	7,24E-09	4	3
DO: F 3334	1oo2	6,09E-07	1,29E-09	4	4
Aktor: Ventil	1oo2	3,33E-05	7,40E-09	4	3
System ohne Sensor und Aktor		1,39E-05	1,07E-08	4	3
System mit Sensor u. Aktor		3,03E-04	7,50E-08	3	3
TÜV claimed SIL für System ohne Sensor und Aktor				3	3

System 5 (Analog-Digital Loop 1)



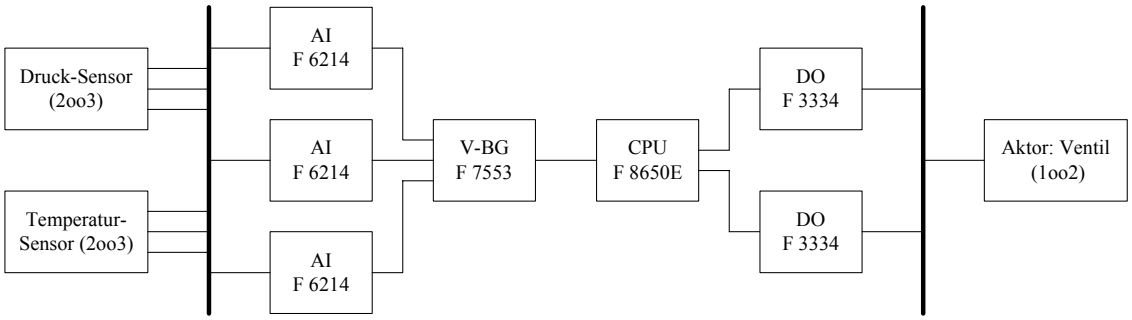
	Architektur	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Druck-Sensor	2oo3	1,00E-04	2,22E-08	3	3
Temperatur-Sensor	2oo3	1,56E-04	3,47E-08	3	3
AI: F 6214	1oo2	1,00E-06	3,44E-09	4	3
V-BG: F 7553	1oo1	9,78E-06	5,76E-10	4	4
CPU: F 8650E	1oo1	2,94E-05	4,08E-09	3	3
DO: F 3334	1oo1	1,40E-05	6,87E-10	4	4
Aktor: Ventil	1oo2	3,33E-05	7,40E-09	4	3
System ohne Sensor und Aktor		5,42E-05	8,78E-09	4	4
System mit Sensor u. Aktor		3,43E-04	7,31E-08	3	3
TÜV claimed SIL für System ohne Sensor und Aktor				3	3

System 6 (Analog-Digital Loop 2)



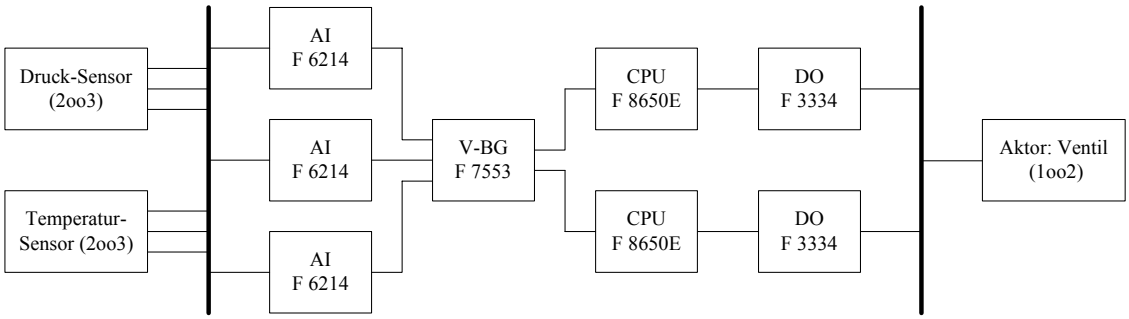
	Architektur	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Druck-Sensor	2oo3	1,00E-04	2,22E-08	3	3
Temperatur-Sensor	2oo3	1,56E-04	3,47E-08	3	3
AI: F 6214	1oo2	1,00E-06	3,44E-09	4	3
V-BG: F 7553	1oo1	9,78E-06	5,76E-10	4	4
CPU: F 8650E	1oo2	3,08E-06	7,24E-09	4	3
DO: F 3334	1oo1	1,40E-05	6,87E-10	4	4
Aktor: Ventil	1oo2	3,33E-05	7,40E-09	4	3
System ohne Sensor und Aktor		2,79E-05	1,19E-08	4	3
System mit Sensor u. Aktor		3,17E-04	7,62E-08	3	3
TÜV claimed SIL für System ohne Sensor und Aktor				3	3

System 7 (Analog-Digital Loop 3)



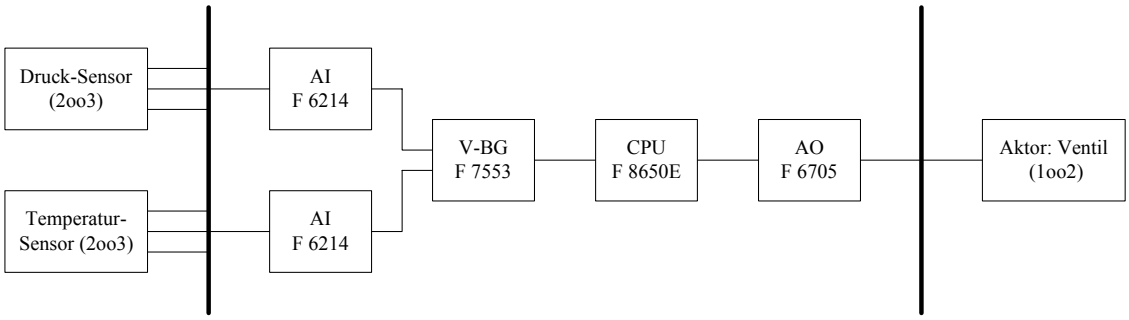
	Architektur	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Druck-Sensor	2oo3	1,00E-04	2,22E-08	3	3
Temperatur-Sensor	2oo3	1,56E-04	3,47E-08	3	3
AI: F 6214	2oo3	1,01E-06	3,50E-09	4	3
V-BG: F 7553	1oo1	9,78E-06	5,76E-10	4	4
CPU: F 8650E	1oo1	2,94E-05	4,08E-09	3	3
DO: F 3334	1oo2	6,09E-07	1,29E-09	4	4
Aktor: Ventil	1oo2	3,33E-05	7,40E-09	4	3
System ohne Sensor und Aktor		4,08E-05	9,45E-09	4	4
System mit Sensor u. Aktor		3,30E-04	7,37E-08	3	3
TÜV claimed SIL für System ohne Sensor und Aktor				3	3

System 8 (Analog-Digital Loop 4)



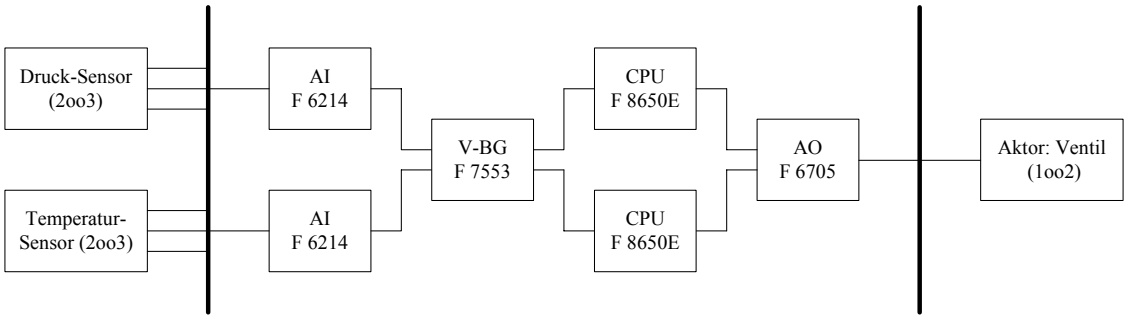
	Architektur	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Druck-Sensor	2oo3	1,00E-04	2,22E-08	3	3
Temperatur-Sensor	2oo3	1,56E-04	3,47E-08	3	3
AI: F 6214	2oo3	1,01E-06	3,50E-09	4	3
V-BG: F 7553	1oo1	9,78E-06	5,76E-10	4	4
CPU: F 8650E	1oo2	3,08E-06	7,24E-09	4	3
DO: F 3334	1oo2	6,09E-07	1,29E-09	4	4
Aktor: Ventil	1oo2	3,33E-05	7,40E-09	4	3
System ohne Sensor und Aktor		1,45E-05	1,26E-08	4	3
System mit Sensor u. Aktor		3,04E-04	7,69E-08	3	3
TÜV claimed SIL für System ohne Sensor und Aktor				3	3

System 9 (Analog Loop 1)



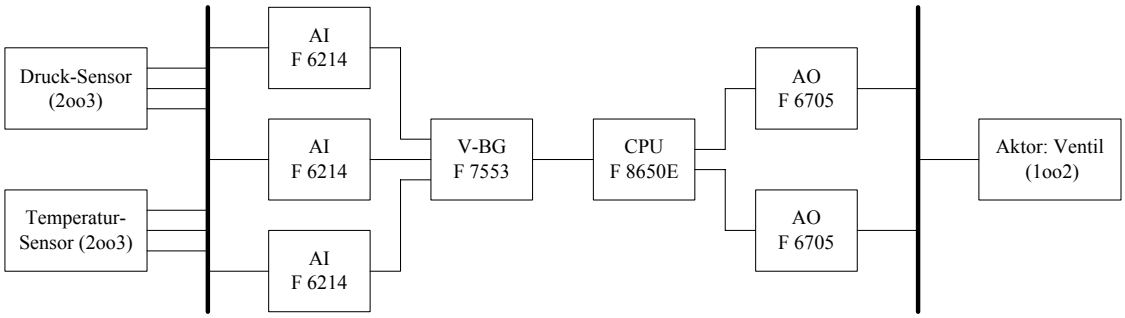
	Architektur	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Druck-Sensor	2oo3	1,00E-04	2,22E-08	3	3
Temperatur-Sensor	2oo3	1,56E-04	3,47E-08	3	3
AI: F 6214	1oo2	1,00E-06	3,44E-09	4	3
V-BG: F 7553	1oo1	9,78E-06	5,76E-10	4	4
CPU: F 8650E	1oo1	2,94E-05	4,08E-09	3	3
AO: F 6705	1oo1	1,86E-05	6,17E-10	3	4
Aktor: Ventil	1oo2	3,33E-05	7,40E-09	4	3
System ohne Sensor und Aktor		5,88E-05	8,71E-09	4	4
System mit Sensor u. Aktor		3,48E-04	7,30E-08	3	3
TÜV claimed SIL für System ohne Sensor und Aktor				3	3

System 10 (Analog Loop 2)



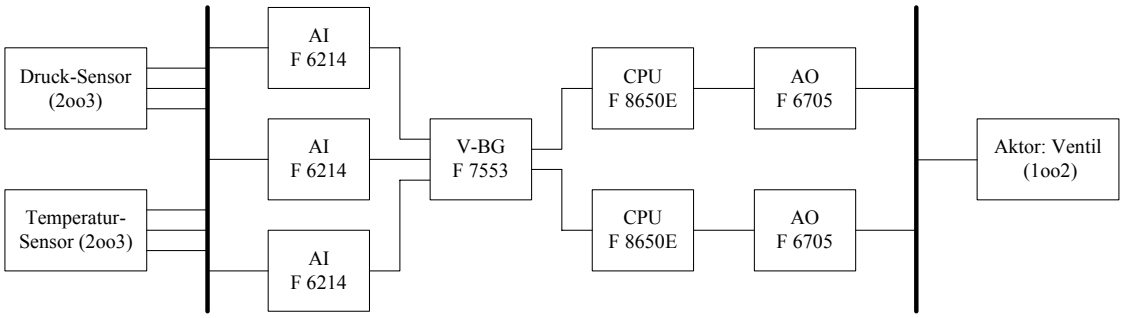
	Architektur	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Druck-Sensor	2oo3	1,00E-04	2,22E-08	3	3
Temperatur-Sensor	2oo3	1,56E-04	3,47E-08	3	3
AI: F 6214	1oo2	1,00E-06	3,44E-09	4	3
V-BG: F 7553	1oo1	9,78E-06	5,76E-10	4	4
CPU: F 8650E	1oo2	3,08E-06	7,24E-09	4	3
AO: F 6705	1oo1	1,86E-05	6,17E-10	3	4
Aktor: Ventil	1oo2	3,33E-05	7,40E-09	4	3
System ohne Sensor und Aktor		3,25E-05	1,19E-08	4	3
System mit Sensor u. Aktor		3,22E-04	7,62E-08	3	3
TÜV claimed SIL für System ohne Sensor und Aktor				3	3

System 11 (Analog Loop 3)



	Architektur	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Druck-Sensor	2oo3	1,00E-04	2,22E-08	3	3
Temperatur-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
Aktor: Ventil	1oo2	3,33E-05	7,40E-09	4	3
System ohne Sensor und Aktor		4,06E-05	1,04E-08	4	3
System mit Sensor u. Aktor		3,30E-04	7,47E-08	3	3
TÜV claimed SIL für System ohne Sensor und Aktor				3	3

System 12 (Analog Loop 4)



	Architektur	PFD-IEC in [1]	PFH-IEC in [1/h]	SIL, PFD-IEC	SIL, PFH-IEC
Druck-Sensor	2oo3	1,00E-04	2,22E-08	3	3
Temperatur-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
Aktor: Ventil	1oo2	3,33E-05	7,40E-09	4	3
System ohne Sensor und Aktor		1,43E-05	1,36E-08	4	3
System mit Sensor u. Aktor		3,04E-04	7,79E-08	3	3
TÜV claimed SIL für System ohne Sensor und Aktor				3	3

Literatur

[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