SIL-Fähigkeits-Analyse/SIL-Capability Analysis

Produkt/Product:
Stellantrieb Baureihe VP
Actuator Series VP

Hersteller/Manufacturer:

Autronic Reglersysteme GmbH
Grützmühlenweg 44
D-22339 Hamburg

B-Nr./Report-No. 090268
Rev. 1.0

Classification: none

Ersteller/Assessor:

INGENIEURBÜRO URBAN
Dipl.-Ing. Josef Urban
Öffentlich bestellter und vereidigter Sachverständiger für Sicherheitsfragen für programmierbare elektronische Systeme
Anerkannter Sachverständiger für die Prüfung elektrischer Anlagen

Büro Bodensee-Oberschwaben
Nelkenstr. 25, D-88239 Wangen i.A.
Tel. 07522/22662 Fax. 07522/22669

Büro München
Anzingerstr. 24, D-85604 Pöring b . München
Tel. 08106/236626 od. 236625 Fax. 08106/236624

E-Mail mail@ibu-sv.de
Mobiltel. 0171/521-3509

Inhaltsverzeichnis

Contents

0. Vorbemerkungen / Benutzungshinweise

Der vorliegende Bericht fasst die Ergebnisse einer SIL-Fähigkeitsanalyse für den Stellantrieb Baureihe VP der Fa. Autronic Reglersysteme zusammen. Der Stellantrieb Baureihe VP wird als Stellantrieb für Ventil Applikationen eingesetzt.
Mit der SIL-Fähigkeitsanalyse auf der Grundlage der IEC 61508 wurde der rechnerische Nachweis geführt, dass den Stellantrieb Baureihe VP grundsätzlich für den Einsatz in Sicherheitskreisen geeignet ist. Dabei wird von einem bestimmungsgemäßen Betrieb des Stellantriebs VP entsprechend den vom Hersteller spezifizierten Einsatzbedingungen ausgegangen.
Der Bericht liefert sicherheitstechnische Kennwerte, die für die weitergehende sicherheitstechnische Berechnung von Sicherheitskreisen in denen der Stellantrieb Baureihe VP eingesetzt wird, verwendet werden können. Die Ermittlung der sicherheitstechnischen Kenngrößen erfolgte auf der Basis allgemein anerkannter Datensammlungen (Zuverlässigkeitsdaten) und durch den Einsatz von bewährten Analysemethoden (FMEA, FMEDA, Zuverlässigkeitsanalyse).
Die verwendeten Ausfallratenmodelle basieren auf allgemeinen, dem Stand der Technik entsprechenden Ausfallratenmodellen für die Bewertung von mechanischen Komponenten und einer ingenieurmäßigen Bewertung der besonderen Belastungsanforderungen an den Stellantrieb Baureihe VP für den geplanten Einsatzzweck.
Für den Stellantrieb Baureihe VP wurden eindeutige Schnittstellen zu anderen Aggregaten/Maschinenteilen definiert.

Die Ergebnisse sind in einem Aggregate-/Komponenten-Sicherheitsdatenblatt (s. Kapitel 1) zusammengefasst.

Bei der Anwendung der Daten aus dem Sicherheitsdatenblatt ist zu beachten, dass die in den Verwenderländern geltenden zusätzlichen gesetzlichen Vorschriften und Normen bezüglich Test-/ Inspektionsintervalle und Architekturen vorrangig zu berücksichtigen sind. Daraus ergeben sich eventuell andere Anforderungen als aus den Beispielrechnungen der quantitativen SIL-Fähigkeit -Analyse.

Wangen/Pöring, den 14. November 2009

INGENIEURBÜRO URBAN

Dipl.-Ing. J. Urban

0. Remarks/Informations For Use

This report is summarizing the SIL capability analysis for the actuator series VP produced by the Co. Autronic Reglersysteme. The actuator series VP is used as Actuator for valve applications.
The SIL capability analysis based on IEC 61508 is the quantitative proof that the actuator series VP basically fits for use in safety loops. Application of the actuator series VP according the manufacturer specified conditions is assumed.
The report delivers safety relevant parameters for further safety relevant calculations of safety loops using the actuator series VP. The development of the safety relevant parameters was based on application of general accepted data bases (reliability data) and use of proven analytic methods (FMEA, FMEDA, reliability analysis).
The failure rate models used are based on state of the art failure rate models for calculation of mechanical components and engineering judgement of the special requirements/stress situation of the actuator series VP for the intended use.
Unambiguous interfaces with other assemblies/machine parts/components were defined for the actuator series VP.

The results are summarized in assembly/component safety data sheets (see chapter 1).

In case of application of data from the safety data sheet additional legal requirements and standards for test/inspection-intervals and safety loop architectures in the user countries must be followed with priority. This might result in different requirements as stated in the example calculations of the quantitative SIL-capability analysis.

Wangen/Pöring, 14th Novmeber, 2009

INGENIEURBÜRO URBAN

Dipl.-Ing. J. Urban

0.1 Revisionsindex

Index	Datum	Abschnitt	Beschreibung der Änderungen
V0.1	04.09.2009	Alle	Entwurf (Erstfassung)
V1.0	14.11.2009		Endfassung

0.1 Revision Index

Index	Date	Section	Description of the changes
V0.1	2009-09-04	All	First draft
V1.0	2009-11-14		Final version

1. Management Summary

In den nachstehenden Aggregate/Komponenten-Sicherheitsdatenblättern sind die Ergebnisse der quantitativen SIL-Fähigkeitsanalyse zusammengefasst. Die sicherheitstechnischen Kenndaten sind analytisch ermittelt worden. Die ermittelten Versagenswahrscheinlichkeiten (pfd-Werte) sind exemplarisch für gebräuchliche Proof-Test-Intervalle angegeben. Anwendungsspezifisch abweichende Werte sind anhand der in der IEC 61508-6 angegebenen Formeln gesondert zu berechnen.

Die Berechnung der Ausfallraten bzw. Ausfallratenanteile erfolgte auf der Grundlage von Ausfallratenmodellen für die Einzelkomponenten des Stellantriebs VP und einer Bewertung der Kritikalität jedes potentiellen Fehlers (Ausfall wirkt sich sicher/gefährlich/nicht aus) durch eine Failure Mode Effects and Diagnostic Analysis (FMEDA). Bei allen durchgeführten Berechnungen und Analysen wurden die besonderen Einsatzbedingungen des Stellantriebs VP berücksichtigt.

Die FMEDA-Analysen wurden in zwei Varianten durchgeführt:

Betrachtung der Fehlerauswirkungen ohne Berücksichtigung von automatischen Diagnosetests (z.B. Partial Stroke Tests bei Ventilen, Ventilantrieben, etc.)
Betrachtung der Fehlerauswirkungen mit Berücksichtigung von automatischen Diagnosetests (z.B. Partial Stroke Tests bei Ventilen, Ventilantrieben, etc.)

Da zum Stellantrieb Baureihe VP keine Diagnosetests vorlagen wurde nur die erste Variante durchgeführt. Diesbezüglich ist nur eine Datenblatt (ohne Berücksichtigung von Diagnosetests) enthalten.

Die Bewertung der SIL-Fähigkeit erfolgt anhand der in der IEC 61508 vorgegebenen quantitativen und qualitativen Kriterien (IEC 61508-1, Tabelle 2 bzw. 3 und IEC 61508-2, Tabelle 2 und 3). Die Bewertung der SIL-Fähigkeit im vorliegenden Bericht beschränkt sich auf diese Kriterien. Weitere erforderliche Kriterien der IEC 61508 (z.B. Anwendung von Methoden und Verfahren während des gesamten Safety-Life-Cycle des Produktes) werden in diesem Zusammenhang nicht betrachtet.

Die FMEDA des Stellantriebs VP wurde auf Grundlage der Annahme des in den Datenblättern angegebenen sicheren Zustandes bzw. der Sicherheitsfunktion durchgeführt.

Das Ergebnis der in diesem Bericht zusammengefassten Untersuchungen zeigt, dass den Stellantrieb Baureihe VP für Anwendungen in Sicherheitskreisen geeignet ist. Es wird jedoch ausdrücklich darauf hingewiesen, dass die in den Datenblättern angegebenen SIL-Angaben exemplarisch sind. Die Beurteilung der Eignung des Stellantriebs VP für die jeweilige Anwendung bzw. die eventuell zu erstellende, anwendungsspezifische Architektur und eventueller automatischer Diagnosetests liegt im Verantwortungsbereich des Anwenders (z.B.

1. Management Summary

In the assembly/component safety data sheets the results of the quantitative SIL capability analysis are summarized. The safety relevant parameters were developed by analysis. The developed probabilities to fail (pfd-values) are example values for widely used proof-test intervals. Deviating application specific values should be calculated separately by using the appropriate formula given in IEC 61508-6.

The calculation of failure rates and failure rate partitions was based on failure rate models for single components of the actuator series VP and an evaluation of the criticality of each potential failure (failure is safe/dangerous/not relevant) by a Failure Mode Effects and Diagnostic Analysis (FMEDA). For all calculations and analysis the specific conditions of the application of the actuator series VP were considered.

The FMEDA-analysis was done in two variants:

- Analysis of failure effects without consideration of automatic diagnosis (e.g. partial stroke tests for valves, valve drives, etc.)
- Analysis of failure effects with consideration of automatic diagnosis (e.g. partial stroke tests for valves, valve drives, etc.

Because of no existing diagnostic measures for the actuator series VP only the first variant is realized. Due to this reason the actuator series VP data sheet (without consideration of diagnosis) is documented below.

The evaluation of the SIL capability follows the quantitative and qualitative criteria of IEC 61508 (IEC 61508-1, table 2 resp. table 3 and IEC 61508-2, table 2 and 3). The evaluation of the SIL capability in the scope of this report is restricted to these criteria. Further required criteria of IEC 61508 (e.g. application of methods and techniques during overall safety life cycle of the product) are not considered in this context.

The FMEDA of the actuator series VP was based on the safe state/safety function documented in the data sheets.

The result of the examinations, summarized in this report, indicates the suitability/capability of the actuator series VP for application in safety loops. It is explicitly advised that the SIL-figures given in the data sheet are examples. The suitability for specific intended applications respectively the designing applications specific architectures and of eventual automatic diagnosis is user's responsibility (e.g. plant designer).

The safety relevant parameters documented in the data sheets could be used as base for further calculations of application specific architectures.
It is also user's responsibility to define adequate proof test intervals for detection of undetected dangerous

Anlagenbauer).

Die in den Datenblättern angegebenen sicherheitstechnischen Kenndaten können dabei als Bewertungsgrundlagen bzw. als Ausgangswerte für die weitergehende Berechnung anwendungsspezifischer Architekturen verwendet werden.
Ebenfalls ist der Anwender dafür verantwortlich, adäquate Proof Test Intervalle zur Aufdeckung unentdeckter gefährlicher Ausfälle (die z.B. auch durch regelmäßige Diagnosetests wie partial stroke tests nicht entdeckt werden können) festzulegen. Dabei kann sich der Anwender an den Herstellervorgaben für die in der Benutzerdokumentation angegebenen Zeitintervalle gemäß dem Wartungsplan orientieren.
Dem Anwender obliegt es auch, die Einhaltung der Herstellerspezifikation sicher zu stellen. Bei eventuellen Abweichungen von den spezifizierten Einsatzbedingungen des Stellantriebs VP ist der Hersteller zu kontaktieren. Der Hersteller bewertet in diesem Falle, ob die ermittelten sicherheitstechnischen Kenngrößen auch für die veränderten Einsatzbedingungen weiterhin anwendbar sind, oder ob Korrekturen erforderlich sind.

failures (e.g. which could not be detected by regular diagnosis). The user‘s could take into account the manufacturer information on inspection intervals in the user documentation defined for maintenance.
Also it’s user responsibility to take care of the specified conditions. In case of deviation of the specified conditions for the actuator series VP the manufacturer must be consulted. In that case the manufacturer estimates the validity of the calculated safety relevant parameters under changed conditions or if corrections are required

Die Analyse umfasst folgende elektrohydraulische Stellantriebe Type VP:

The Analysis contains following electro hydraulics actuators Type VP:

Typenschlüssel alle Typenschilder : *** / * /ST * / * / * / ***

a / b / c / d / e / f

	Beschreibung *	***Werte***	***Alternativwerte***
a	Zündschutzart elektrisches Stellsignal	Ohne = kein Ex-Schutz	i= eigensicher
b	Max. Betriebsstrom	93 mA	keine
c	Pumpenfördermenge in cm³/sek.	Vp40 = 15,0	Vp50=19,5 / Vp250 = 120,0
d	Stellhub	10 bis 100 mm	bis 200mm
e	Stellkraft	5 bis 150 kN	Sondergrößen
f	Sonderausführung	Ohne = keine Sonderausführung	Ex = Explosionsgeschützt

Type codes : *** / * /ST * / * / * / ***

a / b / c / d / e / f

	Description *	***Data***	***Alternative data***
a	Type of protection of electrical input signal	without = non flame proof	i= intrinsic safety
b	Max. operational current	50 mA	none
c	Hydraulic pump capacity in cm³/sek.	Vp40 = 15,0	Vp50=19,5 / Vp250 = 120,0
d	Adjustment stroke	10 to 100 mm	Up to 200mm
e	Adjustment power	5 to 150 kN	Special size
f	Special design	without = no Special design	Ex = flame proof

In der weitern Betrachtung wird zwischen zwei Varianten unterschieden:

- Eine Variante des Stellantriebs VP mit einem Druckspeicher
- Eine Variante des Stellantriebs VP mit zwei Druckspeicher

Die Unterschiede gehen aus der Fehlerbaumanalyse hervor. Sie sind im Datenblatt dokumentiert.
Jeweils zu diesen zwei Varianten gibt es drei Möglichkeiten den Schnellschluss auszulösen:

- Mit Magnetventil und Motorabschaltung
- Nur mit Motorabschaltung
- Nur mit Magnetventil

In der folgenden Tabelle sind diese Versionen ebenfalls berücksichtigt

In the further consideration it is differed in two variants:

- First variant is the actuator series VP with one reservoir
- Second variant is the actuator series VP with two reservoirs

The differences result from a Fault Tree Analysis and are documented in the Datasheet below.
In addition to these two variants three possibilities exist to activate the emergency shutdown:

- With solenoid valve and motor shutoff
- Only with motor shutoff
  Only with solenoid valves

In the table below these versions are considered.

Set of Components/Component Safety Data (acc. IEC 61508 et al.)		
Set of Components/Component	Actuator	
Type	Electro Hydraulic Actuaor for Valve Applications	
Product Designator	VP-Series	
Manufacturer	Autronic Reglersysteme GmbH, Hamburg	
Component Type	Type A	Ref. IEC 61508-2
Mode of Operation	Low demand operation	
Safety Function	Drive go in Fail Safe Position	
Safe State	Drive in Fail Safe Position	

Failure Rates [failure/10^9 hrs = FIT]

Failure Rate Distribution		λ_{totale}	λ_{safe}	$\lambda_{dangerous\ undetected}$	$\lambda_{don't\ care}$	SFF [%]
With **2** Reservoirs (results from FTA / FMEDA)	Solenoid valves and motor shutoff	10,200.052	9,544.861	**655.191**	1,787.698	92.577
	Only motor shutoff	8,476.058	7,782.080	**693.978**	1,787.698	91.812
	Only Solenoid valves	10,029.661	9,222.470	**807.191**	1,787.698	91.952
With **1** reservoir (results from FTA / FMEDA)	Solenoid valves and motor shutoff	9,900.052	9004.861	**895.191**	1,787.698	90.958
	Only motor shutoff	8,176.058	7,242.380	**933.978**	1,787.698	88.580
	Only Solenoid valves	9,729.661	8,682.471	**1,047.190**	1,787.698	89.237

Specification of component Architecture		
Architecture	**1oo1**	1oo1 is the architecture of a single set of components/component of the analysed type. The system contains subsystems which have different architectures. In sum the system is 1oo1.
Hardware Fault Tolerance HFT	**0**	Due to HFT=0 a single set of components/component of the analysed type is not sufficient for SIL3-Safety Loops. For these applications an architecture built from several set of components/components of the analysed type is required (e.g. one shut down valve and one control valve in serial configuration). The influence of HFT on SIL capability is respected in (2) below.
MTTR [h]	**8**	MTTR ist he time required for repair of the set of components/component in case of failure. MTTR has influence on the pfd-value.
Diagnostic Coverage DC [%]	**0**	In case of missing automatic diagnosis (e.g. partial stroke test): DC = 0 %. In case of implemented partial stroke test: DC > 0% (value depends on efficiency of partial stroke test). Safe Failure Fraction SFF increased by higher DC. Influence of DC on SIL capability of the set of components/component is respected in (2) below (via SFF).

Calculated (company/name/date/signature)	INGENIEURBÜRO URBAN Anzinger Str. 24 D-85604 Pöring	Pöring, 2009-11-14	

Verification of SIL Capability (examples) (see comments on next page/backside of this page)		
Set of Components/Component	Actuator	
Type	Electro Hydraulic Actuator for Valve Applications	
Product Designator	VP-Series	
Manufacturer	Autronic Reglersysteme GmbH, Hamburg	

(1) quantitative achievable SIL (IEC 61508-1, Tab. 2)	**SIL**(HFT 0; Typ A)	**(2)** qualitative achievable SIL (IEC 61508-2, Tab. 2)
$\geq 10^{-4}$ SFF < 10^{-3}	**3**	90% ≤ SFF <99%
$\geq 10^{-3}$ SFF < 10^{-2}	**2**	60% ≤ SFF <90%
$\geq 10^{-2}$ SFF < 10^{-1}	**1**	0% ≤ SFF <60%

2 Reservoir, ESD-Solenoid Valve and Motor Shutdown					
Proof Test Intervall	**1 year**	**2 years**	**3 years**	**4 years**	**5 years**
PFD (FTA- Analysis) B090267_Appendix_A	2.87 E-03	5.75 E-03	8.62 E-03	1.15 E-02	1.44 E-02
Achievable SIL = Min {(1); (2)}	**SIL 2**	**SIL 2**	**SIL 2**	**SIL 1**	**SIL 1**

2 Reservoir, Only Motor Shutdown					
Proof Test Intervall	**1 year**	**2 years**	**3 years**	**4 years**	**5 years**
PFD (FTA- Analysis) B090267_Appendix_B	3.04 E-03	6.09 E-03	9.13 E-03	1.22 E-02	1.52 E-02
Achievable SIL = Min {(1); (2)}	**SIL 2**	**SIL 2**	**SIL 2**	**SIL 1**	**SIL 1**

2 Reservoir, Only ESD-Solenoid Valve					
Proof Test Intervall	**1 year**	**2 years**	**3 years**	**4 years**	**5 years**
PFD (FTA- Analysis) B090267_Appendix_C	3.54 E-03	7.08 E-03	1.06 E-02	1.42 E-02	1.77 E-02
Achievable SIL = Min {(1); (2)}	**SIL 2**	**SIL 2**	**SIL 1**	**SIL 1**	**SIL 1**

1 Reservoir, ESD-Solenoid Valve and Motor Shutdown					
Proof Test Intervall	**1 year**	**2 years**	**3 years**	**4 years**	**5 years**
PFD (FTA- Analysis) B090267_Appendix_D	3.92 E-03	7.84 E-03	1.18 E-02	1.57 E-02	1.96 E-02
Achievable SIL = Min {(1); (2)}	**SIL 2**	**SIL 2**	**SIL 1**	**SIL 1**	**SIL 1**

1 Reservoir, Only Motor Shutdown					
Proof Test Intervall	**1 year**	**2 years**	**3 years**	**4 years**	**5 years**
PFD (FTA- Analysis) B090267_Appendix_E	4.09 E-03	8.18 E-03	1.23 E-02	1.64 E-02	2.04 E-02
Achievable SIL = Min {(1); (2)}	**SIL 2**	**SIL 2**	**SIL 1**	**SIL 1**	**SIL 1**

1 Reservoir, Only ESD-Solenoid Valve					
Proof Test Intervall	**1 year**	**2 years**	**3 years**	**4 years**	**5 years**
PFD (FTA- Analysis) B090267_Appendix_F	4.59 E-03	9.17 E-03	1.38 E-02	1.83 E-02	2.29 E-02
Achievable SIL = Min {(1); (2)}	**SIL 2**	**SIL 2**	**SIL 1**	**SIL 1**	**SIL 1**

Calculated (company/name/date/signature)	INGENIEURBÜRO URBAN Anzinger Str. 24 D-85604 Pöring	Pöring, 2009-11-14	

Explanations to the Data Sheet

The data sheet is divided in 4 areas:

- Common technical description of the set of components/component (blue)
- Failure rates (light green)
- Specification of architecture of the set of components/component (light orange)
- Verification of SIL capability (examples) (grey)

General technical Description of the System / Component

- Information on the set of components/component, type of component and component designator
- Manufacturer information
- Component type (Typ A or Typ B) acc. IEC 61508-2/7.4.3.1.2 und 7.4.3.1.3)
- Mode of operation of the set of components/component (acc. IEC 61508-1)
- Description of the safety function of the set of components/component
- Description of the safe state of the set of components/component

Failure Rates

The failure rates and failure rate distribution are the results of the reliability calculation of the set of components/component and the Failure Modes Effects and Diagnostic Analysis (FMEDA). The failure rates can be used for further quantitative analysis of the set of components/component as pfd/pfh-calculation, Markov-Analysis, Fault Tree Analysis, and due to this for a quantitative evaluation of SIL-capability of the set of components/component. Based on the failure rate distribution the Safe Failure Fraction (SFF) is calculated according the formula SFF [%] = $(\lambda_S + \lambda_{DD}) / (\lambda_S + \lambda_{DD} + \lambda_{DU})$

Specification of Component Architecture

The architecture of the set of components/component is described by following parameters:

- Structure/architecture (single-channel, multi-channel expressed by 1oo1, 1oo2, 2oo3, etc.)
- Hardware-Fault-Tolerance (HFT) (number of failures acceptable without dispatch on the safety function of the set of components/component)
- Mean Time to Repair (MTTR): time to repair the set of components/component in case of failure
- Diagnostic Coverage: The diagnostic coverage is resulting from the diagnostic structure/diagnostic measures for the set of components/component ind case of application of automatic diagnosis (e.g. partial stroke test). The diagnostic coverage is considered in the FMEDA and the quantitative results of the analysis (see failure rates)

Verification of SIL-capability (examples)

The SIL capability of the set of components/component is of major interest for the user. Therefore with respect to default values and basic qualitative and quantitative preconditions for the set of components/component a verification of the product capability for use in safety loops is calculated for some examples of proof test intervals. In case of deviation of the application specific values from the used default values an application specific evaluation is required.

The verification consists of two steps:

- Step (1) = f{pfd; proof test interval}: quantitative verification by calculation of the pfd-value depending from the defined Proof Test Interval (1 year, 2 years, 3 years, 4 years, 5 years)
- Step (2) = f{HFT; component type; SFF}: qualitative verification based on the architectural information of the set of components/component

The final achievable SIL is the minimum resulting SIL-value of step (1) and step (2): MIN{ (1);(2)}.

Caution: For a complete SIL-verification of a set of components/component additional measure to this quantitative analysis are required (methods and techniques used fort he overall life cycle of the set of components/component). For proven-in use components a proven-in-use-assessment is possible.

Aggregate/Komponenten-Sicherheitsdaten (gem. IEC 61508 et al.)

Aggregat/Komponente	Stellantrieb	
Typ	ST-Antrieb für Ventil Anwendungen	
Bezeichnung	VP	
Hersteller	Autronic Reglersysteme GmbH, Hamburg	
Komponententyp	Typ A	Ref. IEC 61508-2
Betriebsart	Niedrige Anforderungsrate	
Sicherheitsfunktion	Antrieb fährt in Grund Position	
Sicherer Zustand	Antrieb in Grund Position	

Ausfallraten [Fehler/10^9 hrs = FIT]

Ausfallratenverteilung		λ_{gesamt}	λ_{sicher}	$\lambda_{gefährlich\ unentdeckt}$	$\lambda_{don't\ care}$	SFF [%]
Mit **2** Druckspeicher (Ergebnisse aus FTA / FMEDA)	Magnetventil und Motorabschaltung	10.200,052	9.544,861	**655,191**	1.787,698	92,577
	Nur Motorabschaltung	8.476,058	7.782,080	**693,978**	1.787,698	91,812
	Nur Magnetventile	10.029,661	9.222,470	**807,191**	1.787,698	91,952
Mit **1** Druckspeicher (Ergebnisse aus FTA / FMEDA))	Magnetventil und Motorabschaltung	9.900,052	9.004,861	**895,191**	1.787,698	90,958
	Nur Motorabschaltung	8.176,058	7.242,380	**933,978**	1.787,698	88,580
	Nur Magnetventile	9.729,661	8.682,471	**1.047,190**	1.787,698	89,237

Specification of component Architecture		
Architecture	**1oo1**	1oo1 ist die Architektur eines(r) einzigen Aggregates/Komponente vom untersuchten Typ Das System besteht auch aus aus Teilsystemen die eine andere Architektur haben. Diese sind in der Fehlerbaumanalyse berücksichtigt worden.
Hardware Fault Tolerance HFT	**0**	Wegen HFT=0 ist für SIL3-Safety Loops ein(e) einziges Aggregat/Komponente des untersuchten Typs nicht empfehlenswert. Für diese Anwendungen ist eine Architektur bestehend aus mehreren Aggregaten/Komponenten von Vorteil (z.B. ein Stellventil und ein Regelventil in Reihe geschaltet). Einfluss der HFT auf die SIL-Fähigkeit ist unter Punkt (2) unten berücksichtigt.
MTTR [h]	**8**	MTTR ist die erforderliche Zeit für die Reparatur des(r) Aggregates/Komponente im Fehlerfall. Durch die MTTR wird der pfd-Wert beeinflusst.
Diagnostic Coverage DC [%]	**0**	Bei fehlender automatischer Diagnose (z.B. Teilhubprüfung): DC = 0 %. Mit laufender Teilhubprüfung DC > 0% (tatsächlicher Wert abhängig von der Qualität der Teilhubprüfung). Erhöhung der Safe Failure Fraction SFF durch besseren DC. Der Einfluss des DC auf die SIL-Fähigkeit des Aggregats/der Komponente ist unter Punkt (2) berücksichtigt (via SFF).

Calculated (company/name/date/signature)	INGENIEURBÜRO URBAN Anzinger Str. 24 D-85604 Pöring	Pöring, 2009-11-14	

Exemplarische Verifizierung der SIL-Fähigkeit (Erläuterung auf der Rückseite beachten)

Aggregat/Komponente	Stellantrieb	
Typ	ST-Antrieb für Ventil Anwendungen	
Bezeichnung	VP	
Hersteller	Autronic Reglersysteme GmbH, Hamburg	

(1) quantitativ erreichbares SIL (IEC 61508-1, Tab. 2)	**SIL**(HFT 0; Typ A)	**(2)** qualitativ erreichbares SIL (IEC 61508-2, Tab. 2)
$\geq 10^{-4}$ SFF < 10^{-3}	**3**	90% ≤ SFF <99%
$\geq 10^{-3}$ SFF < 10^{-2}	**2**	60% ≤ SFF <90%
$\geq 10^{-2}$ SFF < 10^{-1}	**1**	0% ≤ SFF <60%

2 Druckspeicher, SS-Magnetventil und Motorabschaltung

Proof Test Intervall	**1 year**	**2 years**	**3 years**	**4 years**	**5 years**
PFD (FB- Analyse) B090267_Appendix_A	2,87 E-03	5,75 E-03	8,62 E-03	1,15 E-02	1,44 E-02
Erreichbares SIL = Min {(1); (2)}	**SIL 2**	**SIL 2**	**SIL 2**	**SIL 1**	**SIL 1**

2 Druckspeicher, nur Motorabschaltung

Proof Test Intervall	**1 year**	**2 years**	**3 years**	**4 years**	**5 years**
PFD (FB- Analyse) B090267_Appendix_B	3,04 E-03	6,09 E-03	9,13 E-03	1,22 E-02	1,52 E-02
Erreichbares SIL = Min {(1); (2)}	**SIL 2**	**SIL 2**	**SIL 2**	**SIL 1**	**SIL 1**

2 Druckspeicher, nur SS-Magnetventil

Proof Test Intervall	**1 year**	**2 years**	**3 years**	**4 years**	**5 years**
PFD (FB- Analyse) B090267_Appendix_C	3,54 E-03	7,08 E-03	1,06 E-02	1,42 E-02	1,77 E-02
Erreichbares SIL = Min {(1); (2)}	**SIL 2**	**SIL 2**	**SIL 1**	**SIL 1**	**SIL 1**

1 Druckspeicher, SS-Magnetventil und Motorabschaltung

Proof Test Intervall	**1 year**	**2 years**	**3 years**	**4 years**	**5 years**
PFD (FB- Analyse) B090267_Appendix_D	3,92 E-03	7,84 E-03	1,18 E-02	1,57 E-02	1,96 E-02
Erreichbares SIL = Min {(1); (2)}	**SIL 2**	**SIL 2**	**SIL 1**	**SIL 1**	**SIL 1**

1 Druckspeicher, nur Motorabschaltung

Proof Test Intervall	**1 year**	**2 years**	**3 years**	**4 years**	**5 years**
PFD (FB- Analyse) B090267_Appendix_E	4,09 E-03	8,18 E-03	1,23 E-02	1,64 E-02	2,04 E-02
Erreichbares SIL = Min {(1); (2)}	**SIL 2**	**SIL 2**	**SIL 1**	**SIL 1**	**SIL 1**

1 Druckspeicher, nur SS-Magnetventil

Proof Test Intervall	**1 year**	**2 years**	**3 years**	**4 years**	**5 years**
PFD (FB- Analyse) B090267_Appendix_F	4,59 E-03	9,17 E-03	1,38 E-02	1,83 E-02	2,29 E-02
Achievable SIL = Min {(1); (2)}	**SIL 2**	**SIL 2**	**SIL 1**	**SIL 1**	**SIL 1**

Calculated (company/name/date/signature)	INGENIEURBÜRO URBAN Anzinger Str. 24 D-85604 Pöring	Pöring, 2009-11-14	

Erläuterung zum Datenblatt

Das Datenblatt gliedert sich in 4 Bereiche:

- Allgemeine technische Beschreibung des Aggregates/ der Komponente (blau)
- Ausfallraten (hellgrün)
- Architekturspezifikation des Aggregates/ der Komponente (hellorange)
- Exemplarische Verifizierung der SIL-Fähigkeit

Allgemeine technische Beschreibung des Aggregates/der Komponente:

- Angabe und Bezeichnung des Aggregates/der Komponente, Typ und Herstellerbezeichnung
- Herstellerinformation,
- Angabe des Komponententyps (Typ A oder Typ B) gemäß IEC 61508-2/7.4.3.1.2 und 7.4.3.1.3)
- Betriebsart des Aggregates/der Komponente (gemäß IEC 61508-1)
- Beschreibung der Sicherheitsfunktion des Aggregates/der Komponente
- Beschreibung des Sicheren Zustandes des Aggregates/der Komponente

Ausfallraten

Die Ausfallraten, bzw. Ausfallratenanteile stellen die Ergebnisse der für das Aggregat/die Komponente durchgeführten Zuverlässigkeitsberechnung und Failure Modes Effects and Diagnostics Analysis (FMEDA) dar. Die Ausfallratenwerte können für weitere quantitative Analysen des Aggregates/der Komponente wie pfd/pfh-Berechnung, Markoff-Analysen, Fehlerbaumanalysen, und somit für eine quantitative Bewertung der SIL-Fähigkeit des Aggregates/der Komponente etc. weiter verwendet werden.
Aus den Ausfallratenanteilen wird die ebenfalls in diesem Block angegebene Safe Failure Fraction (SFF) gemäß der Formel SFF [%] = $(\lambda_S + \lambda_{DD}) / (\lambda_S + \lambda_{DD} + \lambda_{DU})$ errechnet.

Architekturspezifikation

Die Architektur des Aggregates/der Komponente wird durch die Kenngrößen

- Struktur (einkanalig, mehrkanalig, ausgedrückt durch 1oo1, 1oo2, 2oo3, etc.)
- Hardware-Fehler-Toleranz (HFT) (welche Anzahl von Fehlern ist zulässig, ohne dass die Sicherheitsfunktion des Aggregates/der Komponente beeinträchtigt ist)
- Mean Time to Repair (MTTR): mittlere Reparaturdauer die erforderlich ist um einen Fehler des Aggregates/der Komponente zu beheben.
- Diagnosedeckungsgrad: Der Diagnosedeckungsgrad ergibt sich aus der Diagnosestruktur des Aggregates/der Komponente, d.h. der Anwendung von automatischen Diagnosetest (z.B. Teilhubprüfung). Der Diagnosedeckungsgrad ist in der FMEDA und den daraus resultierenden quantitativen Ergebnissen (s. Ausfallraten) berücksichtigt.

Exemplarische Verifizierung der SIL-Fähigkeit

Die SIL-Fähigkeit des Aggregates/der Komponente ist für den Anwender von großem Interesse. Daher ist auf dem Datenblatt unter Berücksichtigung von Default-Werten und unter Berücksichtigung von grundlegenden qualitativen und quantitativen Vorgaben des Aggregates/der Komponente eine Verifizierung für die Anwendbarkeit des Produktes in Sicherheitskreisen für einige Beispiele von Proof Test Intervallen durchgeführt. Bei Abweichungen der anwendungsspezifischen Parameter von den verwendeten Default Werten muß eine anwendungsspezifische Verifizierung durchgeführt werden.
Die Verifizierung erfolgt in zwei Teilschritten:

- Schritt (1) = f{pfd; Proof Test Intervall}: quantitative Verifizierung durch Ermittlung eines pfd-Wertes in Abhängigkeit von festgelegten Proof Test-Intervallen (1 Jahr, 2 Jahre, 3 Jahre, 4 Jahre, 5 Jahre)
- Schritt (2:) = f{HFT; component type; SFF): qualitative Verifizierung aufgrund der Architektur des Aggregates/der Komponente:

Das daraus resultierende SIL ergibt sich als minimales SIL von Schritt (1) und Schritt 2): MIN{(1);(2)}
Achtung! Für eine vollständige Verifizierung der SIL-Fähigkeit eines Aggregats/einer Komponenten sind zusätzliche Maßnahmen erforderlich (angewendete Methoden und Verfahren über den gesamten Life Cycle). Ein Betriebsbewährtheitsnachweis für betriebsbewährte Komponenten ist möglich.

2. Beschreibung des Produktes

2.1 Allgemeiner Aufbau und Typisierung

Der allgemeine Aufbau und die Funktionsweise des VP sind in [16] beschrieben.
Das VP hat aus sicherheits-technischer Sicht eine 1oo1 Architektur in fail-safe-Technik.

Schnittstellen:
Das VP hat folgende Schnittstellen:

- Anschluss an Rohrleitungen (verschraubt) (mech.)
- Anschluss an Ventil (Kupplung) (mech.)
- Anschluss an Messtechnik (el.)
- Anschluss an Hydraulikversorgung (hydr.)
- Anschluss an die Steuerung (el.)

Der Betrachtungsumfang vorl. Analyse endet jeweils an den Schnittstellen; Flanschschrauben, Kupplungen, Zuleitungen (el./hydr./pneu.) etc. gehören nicht zum Betrachtungsumfang

2.2 Definition des sicheren Zustandes und Fehlerdefinition

Zur einheitlichen Bewertung von Fehlern werden folgende Definitionen festgelegt:

Tabelle 1: Definition von Sicherheitsbegriffen

Sicherer Zustand	Zustand/Position die als sicher für das System definiert worden sind.
Sicherheitsfunktion	Funktion, die verantwortlich dafür ist, dass von der aktuellen Position/ vom aktuellen Betriebszustand zum Zeitpunkt der Anforderung der Sicherheitsfunktion ausgehend, der sichere Zustand erreicht wird
Gefährlicher Fehler	Fehler, der verhindert, dass der sichere Zustand erreicht wird.
Gefährlicher, erkannter Fehler	Fehler, der erkannt wird und zum sicheren Zustand führt
Gefährlicher, unerkannter Fehler	Fehler, der nicht erkannt wird und zu einem gefährlichen Zustand führen könnte bzw. verhindert, dass der sichere Zustand erreicht wird.
Ungefährlicher Fehler (Fail Safe)	Fehler, der dazu führt, dass der sichere Zustand erreicht wird oder dies zumindest nicht verhindert.
Fehler ohne Auswirkung	Fehler, die die Sicherheitsfunktion nicht betreffen

2. Product Description

2.1 General Structure and Type

The general structure and the functionality of the VP are described in [16].
The VP from safety point of view is a 1oo1 fail safe architecture.

Interfaces:
The VP has following interfaces:

- interface to pipes (flange) (mechanical)
- interface to valve (clutch) (mechanical)
- interface to I&C (electrical)
- interface to hydraulic supply (hydr.)
- interface to control (el.)

The scope of this analysis is limited at the interfaces; flange fasteners, clutches, supply (el./hydr./pneu.) etc. are not within the scope.

2.2 Definition of Safe State and Failure Definition

For common understanding of failures following items are defined:

Table 1: Definition of Safety Items

Safe State	Status/position which is defined as safe for the system.
Safety Function	Function responsible for reaching the safe state starting from the actual position/mode of operation after request of the safety function.
Dangerous failure	Failure which inhibits, that the safe state will be reached.
Dangerous detected failure	Failure which is detected and will lead to the safe state.
Dangerous undetected failure	Failure which is not detected and could result in a dangerous state or will prevent reaching the safe state
Safe failure (Fail Safe)	Failure leading to the safe state or not preventing to reach the safe state.
No effect failure (not relevant failure)	Failure not effecting the safety function

2.3 Weitere Definitionen und Abkürzungen

2.3 Further Definitions and Acronyms

Tabelle 2: Definitionen und Abkürzungen

Table 2: Definitions and Acronyms

HFT	Hardware-Fehler-Toleranz N/Hardware Fault Tolerance N	bedeutet, daß N +1 Fehler einer Betrachtungseinheit zu einem Verlust der Sicherheitsfunktion führt (z.B. HFT N=0 bedeutet, dass 1 Fehler zum Verlust der Sicherheitsfunktion führt)	Means, that N + 1 failure of a system or subsystem could result in loss of the safety function (e.g. HFT N=0 means, that 1 failure could result as loss of the safety function).
Proof Test		Proof Test dienen der Aufdeckung von gefährlichen Fehlern, die sonst bis zu einer Anforderung der Sicherheitsfunktion unentdeckt bleiben würden. Proof Tests finden statt, wenn das Sicherheitssystem nicht in Betrieb ist.	Proof Tests are useful to detect dangerous failures which could be undetected as long until the safety function is required. Proof tests will be executed when the safety system is out of operation.
Proof Test Intervall		Das Proof-Test Intervall definiert den zeitlichen Abstand zwischen zwei periodischen Prüfungen bzw. Wartungen an einem Sicherheitssystem, durch die unentdeckte, gefährliche Fehler bemerkt bzw. beseitigt werden. Das Sicherheitssystem oder die Sicherheitskomponente wird nach dem Proof-Test als „quasi neu“ betrachtet, bzw. in den Berechnungen als „quasi neu“ angenommen.	The Proof-Test Interval defines the time between two periodic test or maintenance activities to recognize undetected dangerous faults of a safety system. The safety system or the safety component after proof test is as a new system or component (also in the calculation the component or system is defined as new.
SFF	Safe Failure Fraction [%]	Anteil der ungefährlichen Fehler in einer Sicherheitsfunktion SFF [%] = $(\lambda_S + \lambda_{DD}) / (\lambda_S + \lambda_{DD} + \lambda_{DU})$	Fraction of safe failures in a safety function SFF [%] = $(\lambda_S + \lambda_{DD}) / (\lambda_S + \lambda_{DD} + \lambda_{DU})$
PFD	Probability of failure on demand	Ausfallwahrscheinlichkeit für eine Sicherheitsfunktion im Anforderungsfall (für Betriebsart low demand)	Probability that a safety function will fail in case of demand (for low demand operation).
DC	Diagnostic Coverage	= $\Sigma\lambda_{DD} / \Sigma\lambda_D$	= $\Sigma\lambda_{DD} / \Sigma\lambda_D$
MTTR	Mean Time to Repair	Zeit die im Fehlerfall benötigt wird, um die Funktion wieder herzustellen.	Time needed to restore the function in case of failure.
FMEA	Failure Mode and Effects Analysis	Analytische Methode zur Betrachtung der Auswirkungen von Einfachfehlern	Analytic method to consider the effects of single failures
FMEDA	Failure Mode Effects and Diagnostic Analysis	Erweiterte Version der FMEA, die auch Fehlererkennungsmechanismen berücksichtigt.	Extended version of FMEA, which also takes into account failure detection mechanisms.
λ	Ausfallrate/Failure Rate	Einheit: FIT [Fehler/10^9 Stunden]	FIT [failure/10^9 hours]
QM	Qualitätsmanagement/ Quality Management		
Weitere Abkürzungen und Definitionen siehe IEC 61508-4 und IEC 61508-7		Further acronyms and definitions see IEC 61508-4 and IEC 61508-7	

3. Referenzunterlagen

3.1 Normen und sonstige Literatur

Tabelle 3: Referenzunterlagen Normen und sonstige Literatur

3. Reference Documents

3.1 Standards and Other Literature

Table 3: Referenced standards and other literature

No.	Title	remarks	
[1]	IEC 61508-1/12.1998: Functional safety of electrical/electronic/programmable electronic safety-related systems: Part 1- General requirements		
[2]	IEC 61508-2/05.2000: Functional safety of electrical/electronic/programmable electronic safety-related systems: Requirements for electrical/electronic/programmable electronic safety-related systems		
[3]	IEC 61508-3/12.1998: Functional safety of electrical/electronic/programmable electronic safety-related systems: Software Requirements		
[4]	IEC 61508-4/12.1998: Functional safety of electrical/electronic/programmable electronic safety-related systems: Definitions and abbreviations		
[5]	IEC 61508-5/11.1998: Functional safety of electrical/electronic/programmable electronic safety-related systems: Examples of methods for the determination of safety integrity levels		
[6]	IEC 61508-6/04.2000: Functional safety of electrical/electronic/programmable electronic safety-related systems: Guidelines on the application of IEC 61508-2 and IEC 61508-3		
[7]	IEC 61508-7/03.2000: Functional safety of electrical/electronic/programmable electronic safety-related systems: Overview of techniques and measures		
[8]	IEC 61511-1/02.2004 (Draft): Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie : Teil 1 – Allgemeines, Begriffe, Anforderungen an System, Hardware und Software		
[9]	IEC 61511-2/02.2004 (Draft): Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie: Teil 2 – Anleitung zur Anwendung von 61511-1		
[10]	IEC 61511-3/02.2004 (Draft): Funktionale Sicherheit – Sicherheitstechnische Systeme für die Prozessindustrie : Anleitung für die Bestimmung der erforderlichen Sicherheitsintegritätslevel		
[11]	DIN EN ISO 13849-1/07.2007: Sicherheit von Maschinen –Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze		
[12]	DIN EN ISO 13849-2/12.2003: Sicherheit von Maschinen –Sicherheitsbezogene Teile von Steuerungen – Teil 2: Validierung		
[13]	NSWC-06/LE1: Handbook of Reliability Prediction Procedures for Mechanical Equipment; Naval Service Warfare Center, West Bethesda,		
[14]	NPRD-1: Non Electronic Parts Reliability Data Handbook		
[15]	OREDA-HDBK		

3.2 Herstellerunterlagen

Tabelle 4: Referenzunterlagen – Herstellerunterlagen

3.2 Manufacturer Documentation

Table 4: Reference Documents – Manufacturer Documentation

No.	Title	remarks	
[16]	BAVP07d		
[17]	B090268_Appendix_A_Reference_Documents		

3.3 Ergebnisberichte im Rahmen der SIL-Fähigkeits-Analyse

Tabelle 5: Referenzunterlagen – Ergebnisberichte

3.3 Result Reports within the SIL Capability Analysis

Table 5: Reference documents – Result Reports

No.	Title	remarks	
[18]	B090267_V10_FTA-Report_Autronic_Hamburg_VP		
[19]	B090266_V10_FMEDA-Report_Autronic_Hamburg_VP		
[20]	B090264_V10_R-Report_ Autronic_Hamburg_VP		

4. SIL-Fähigkeits-Analyse

4.1 Methodik der SIL-Fähigkeits-Analyse

Bei dem Analysegegenstand von SIL-Fähigkeits-Analysen handelt es sich immer um Komponenten von Sicherheitskreisen, d.h. nicht um den gesamten Sicherheitskreis. Das Analyseergebnis ist daher stets nur ein Nachweis, dass die jeweilige Komponente für den Einsatz in Sicherheitskreisen, die einem bestimmten Safety Integrity Level (SIL) genügen müssen, geeignet ist.

Die SIL-Fähigkeitsanalyse besteht aus folgenden Teilschritten:

- Nachweis der probabilistischen Sicherheitsintegrität (rechnerischer Nachweis, quantitative Verifizierung)
- Nachweis der systematischen Sicherheitsintegrität (qualitative Verifizierung)

Die SIL-Fähigkeits-Analyse im vorliegenden Bericht beruht wesentlich auf dem rechnerischen Nachweis und einer ingenieurmäßigen Bewertung der speziellen Einsatzbedingungen des VP in der vorgesehenen Anwendung. Grundlage hierfür ist eine FMEDA (Failure Mode Effects and Diagnostics Analysis), sowie eine Zuverlässigkeitsanalyse (Ermittlung der Ausfallraten unter Berücksichtigung der spezifizierten Belastungen). Diese Analysen sind in gesonderten, firmenvertraulichen Berichten dokumentiert.

4.2 Grundlegende Annahmen bei der Durchführung der SIL-Fähigkeits-Analyse

Für die Durchführung der SIL-Fähigkeits-Analyse basierend auf einer FMEDA, sowie der Berechnung von Ausfallraten wurden folgende Annahmen auf Grundlage der IEC 61508 getroffen:

- Es werden nur zufällige Einzelfehler betrachtet (keine Fehlerkombinationen)
- Ein einziger Fehler einer Komponente bedeutet einen Fehler des Produktes (d.h. für sicherheitsrelevante Komponenten bedeutet dies im ungünstigsten Fall den Verlust der Sicherheitsfunktion)
- Diagnosetests (z.B. Teilhubprüfungen) werden mit einer Häufigkeit von mindestens der 10-fachen, zu erwartenden Anforderungsrate durchgeführt
- Ausfallraten sind konstant (d.h. Frühausfälle und Langzeitausfälle am Ende der festgelegten Lebensdauer werden durch entsprechende herstellerseitige/anwendungsseitige Maßnahmen ausgeschlossen)
- Verschleißmechanismen werden bei der Berechnung nicht berücksichtigt, da die

4. SIL Capability Analysis

4.1 Method of SIL Capability Analysis

Scope of SIL capability analysis are always components of safety loops and mostly not the overall safety loop. The result of the analysis therefore is only the proof that the analyzed component will fit for use in safety loops which must fulfill the requirements of a certain Safety Integrity Level (SIL).

The SIL capability analysis consists of following Steps:

- Proof of the probabilistic safety integrity (proof by calculation, quantitative verification)
- Proof of the systematic safety integrity (qualitative verification)

The SIL capability in this report is focused on the probabilistic proof and engineering judgement of the special conditions for the VP in the planned application. FMEDA (Failure Mode Effects and Diagnostic Analysis) as well as Reliability Analysis (failure rate calculation considering the specific conditions of use) are the essential activities. These analyses are documented in separate, company confidential reports.

4.2 Basic Assumptions for the SIL Capability Analysis

Following assumptions for the SIL capability analysis based on a FMEDA as well as failure rate calculations are stated in accordance with IEC 61508:

- Only statistic single faults will be considered (no failure combination)
- A single fault of a component results in a product failure (this means for safety relevant components in worst case conditions loss of the safety function)
- Automatic diagnostic tests (e.g. partial stroke tests) will be executed 10x the assumed demand rate
- Failure rates are constant (premature failures and long time failures at the end of the life time will be excluded by measures in the responsibility of the manufacturer/user)
- Wear out mechanisms are not considered for the calculation, because wear out parts will be changed after defined intervals (only random failures will be considered, but possible failure modes are also wear out and aging)
- All failure modes of the used components are well known (type A subsystem acc. IEC

Verschleißteile nach definierten Intervallen erneuert werden (d.h. es werden nur Zufallsausfälle betrachtet, deren Ursache natürlich eine Bauteilalterung oder Verschleiß sein können)
- Alle Ausfallarten der verwendeten Bauteile sind bekannt (Typ A-Teilsystem gem. IEC 61508)
- Alle Komponenten, die nicht Teil der Sicherheitsfunktion sind und diese nicht unmittelbar beeinflussen (Rückwirkungsfreiheit gewährleistet), werden nicht in die Berechnungen mit einbezogen. Die Ermittlung der für die Sicherheitsfunktion relevanten Komponenten erfolgt im Rahmen einer Failure Mode Effect and Diagnostic Analysis (FMEDA)
- Die Belastungsgrößen entsprechen dem industriellen Einsatz und werden entsprechend den durch den Hersteller spezifizierten Bedingungen bei der Berechnung berücksichtigt. Es wird nur die spezifikationsgemäße Verwendung berücksichtigt. Vernünftigerweise vorhersehbare Fehlanwendungen sind in den maximal spezifizierten Grenzen anzunehmen.
- Die konstruktive Auslegung erfolgte nach dem anerkannten Stand der Technik und allgemein anerkannten sicherheitstechnischen Konstruktionsprinzipien
- Die in der FMEA bzw. FMEDA benutzten Fehlermodelle und Berechnungsmodelle entsprechen dem Stand der Technik.

4.3 Rechnerischer Nachweis für die Sicherheitsintegrität

Der rechnerische Nachweis für die Sicherheitsintegrität des VP erfolgte anhand einer Zuverlässigkeitsanalyse (Ausfallratenberechnungen) und einer FMEDA

Zunächst wurde die Gesamtausfallrate für das VP auf der Grundlage von Zuverlässigkeitswerten ermittelt. Diese wurden mittels Zuverlässigkeitsmodellen für jede Einzelkomponente bzw. für jeden Komponententyp berechnet.
Die Basis bilden dabei die in [13] angegebenen Ausfallratenmodelle.
Des Weiteren bildet die Bewertung der Bauteilausfälle auf der Grundlage einer detaillierten FMEDA den Ausgangspunkt für die Ermittlung der Safe Failure Fraction.

Die für das VP im Rahmen der SIL-Fähigkeits-Analyse ermittelten sicherheitstechnischen Grenzwerte sind in Zusammenhang mit den Erfahrungen des Herstellers des VP verifiziert worden. Darüber hinaus sind die analytisch ermittelten Werte in Zukunft möglichst durch die kontinuierliche Erfassung von Betriebsdaten/Einsatzdaten zu plausibilisieren. Dies soll eine möglichst zuverlässige und anwendungsnahe Bewertung unter Berücksichtigung der speziellen Einsatzerfordernisse ermöglichen.
Entsprechende Möglichkeiten zur Datenerfassung sind

61508)
- All components which are not part of the safety function and are not directly influencing the safety function are not part of the calculation. The definition of the safety relevant components is part of the Failure Mode Effect and Diagnostic Analysis (FMEDA)
- Stress factors are in the range of industrial practice and are considered due to the manufacturer specified conditions. Only operation under specified conditions and maximum specified limits are considered.
- The design is in accordance with acknowledged design rules and state of the art.
- The used component failure models for FMEA and FMEDA are state of the art and manufacturer's experience.

4.3 Calculatoric Proof for Safety Integrity

The calculatoric proof for Safety Integrity of the VP was based on the reliability analysis (failure rate calculations) and FMEDA.

As a first step the total failure rate for the VP was calculated based on reliability figures. The reliability figures were calculated for each part or type of part with reliability models.
Base were the failure rate models stated in [13]
Furthermore the evaluation of the component failures based on a detailed FMEDA was the starting point for the Safe Failure Fraction (SFF) calculation.

The safety relevant parameters calculated as result of the SIL-capability analysis for the VP were verified with the manufacturers experience on the VP. Furthermore the values calculated by analysis must be evaluated in future activities of continuous collection of operating data. This should result in a maximum reliable and application specific evaluation considering the special conditions of use.
Data collection measures must be planned for future plants.

künftig in die Anlagenplanung mit einzubeziehen.

4.4 Nachweis der systematischen Sicherheitsintegrität

Der nach IEC 61508 geforderte Nachweis der systematischen Sicherheitsintegrität war nicht Gegenstand der vorliegenden Untersuchung. Es ist zu berücksichtigen, dass der Entwicklungs- und Fertigungsprozess des VP nicht nach den Anforderungen der IEC 61508, sondern anhand der firmeninternen QM-Vorgaben durchgeführt wurde.
Das VP ist seit Jahren in einschlägigen Sicherheitsanwendungen eingesetzt und darf als betriebsbewährt angenommen werden.
Bei der Bewertung der systematischen Sicherheitsintegrität ist auch zu berücksichtigen, dass es sich bei dem Betrachtungsgegenstand nicht primär um ein elektrisches/elektronisches/elektromechanisches System handelt. Die speziell für elektronische Bauteile und Software erforderlichen Prozeduren sind daher nicht zu berücksichtigen.

4.4 Proof of Systematic Safety Integrity

The proof of systematic safety integrity acc. IEC 61508 was not part of this analysis. It must be considered, that the design and manufacturing process for the VP was not based on IEC 61508 requirements, but on company specific QM-requirements.
The VP is used since many years in safety applications and is mentioned proven-in-use.
For systematic safety evaluation also it must be considered, that product is not primarily an electric/electronic/electromechanical system. Therefore the required procedures for electronic components and software must not be respected.

5. Ergebnisse

Alle für die weitere Berechnung von Sicherheitskreisen erforderlichen Daten des VP sind in den Datenblättern in Kapitel 1 wiedergegeben.

Es ist zu beachten, dass diese Ergebnisse erst in Kombination mit den sicherheitstechnischen Kennwerten (z.B. PFD-Werten) der anderen Komponenten, die eine Sicherheitsfunktion bilden, eine abschließende Bewertung der SIL-Fähigkeit einer Sicherheitsfunktion erlauben.

5. Results

All relevant safety data of the VP for further calculations of safety loops are documented in the data sheets in chapter 1.

Consider, that data of the data sheets will allow a definite evaluation of SIL capability only in combination with the safety relevant parameters (e.g. pfd-values) of the other components building the safety loop.