Set of Components/Component Safety Data (acc. IEC 61508 and IEC 61511)

Set of Components/Component	**Pneumatischer Mehrfedermembranantrieb** **Diaphragm Multi-Spring Pneumatic Actuator**	
Variants	Type P/R Single + Tandem (without handwheel) Type P1/R1 Single + Tandem (without handwheel) Spring Range 1...7	
Manufacturer	PRE-VENT GmbH	
Component Type	Type A	Ref. IEC 61508-2
Mode of Operation	Low demand operation	
Safety Function	Actuator moves in safe position by spring force	
Safe State	Actuator in safe position and hold in safe position by spring force	

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

Failure Rate Distribution	λ_{total}	λ_{safe}	$\lambda_{dangerous\ detected}$	$\lambda_{dangerous\ undetected}$	$\lambda_{don't\ care}$	**SFF [%]**
Diaphragm Actuator (P/R & P1/R1) (SINGLE)	1,573	1,479	29	**65***	1	96
Diaphragm Actuator (P/R & P1/R1) (TANDEM)	3,135	2,950	57	**128***	1	96

* Design of actuator tolerates min. one spring failure without affecting safety function

Specification of component Architecture

Architecture	**1oo1**	1oo1 is the architecture of a single set of components/component of the analysed type.
Hardware Fault Tolerance HFT	**0**	Due to HFT=0, one failure has impact on the safety function. The influence of HFT on SIL capability is respected in (2) below.
MTTR [h]	**32**	MTTR is the time required for repair of the set of components/component in case of failure. MTTR has marginal influence on the pfd-value.
Diagnostic Coverage DC [%]	**31 %**	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).

Verification of SIL Capability (examples Diaphragm Actuator SINGLE with diagnosis)

(see comments on next page/backside of this page)

Proof Test Interval	**6 months**	**1 year**	**2 years**	**3 years**	**5 years**
PFD (avg.) (IEC 61508-6, B3.2.2; λ_{du} from FMEDA)	1.45 E-04	2.88 E-04	5.72 E-04	8.57 E-04	1.43 E-03
(1) quantitative achievable SIL (IEC 61508-1, Tab. 2)	**SIL 3**	**SIL 3**	**SIL 3**	**SIL 3**	**SIL 2**
(2) qualitative achievable SIL (IEC 61508-2, Tab. 2)	**SIL. 3 (**for HFT 0; Type A; 90% ≤ SFF <99%)				
Achievable SIL = Min {(1); (2)}	**SIL 3**	**SIL 3**	**SIL 3**	**SIL 3**	**SIL 2**

Calculated (company/name/date/signature)	INGENIEURBÜRO URBAN Anzinger Str. 24 D-85604 Pöring	Pöring, 2013-12-13	

Explanations to the Data Sheet

The data sheet is divided in 4 areas:

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

General description of the Part / Component:

- Information on the set of components/component, type of component and component designator
- Manufacturer information
- Component type (Type A or Type B) acc. IEC 61508-2/7.4.4.1.2 und 7.4.4.1.3)
- 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 [%] = $(\lambda_S + \lambda_{DD}) / (\lambda_S + \lambda_{DD} + \lambda_{DU})$

Failure rates are calculated in acc. with NSWC-06 LE10.

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 in 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 (6 months, 1 year, 2 years, 3 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 for the overall life cycle of the set of components/component). For proven-in use components a proven-in-use-assessment is possible.

Remark: For λ_{du} in pfd calculations results of the FMEDA are used. According IEC 61508 -6 for architecture 1oo1 λ_{du} is defined as $\lambda_{total} / 2$ for use in pfd-calculation.