

Assembly/Component Safety Data (acc. IEC 61508)

Set of Components/Component	Dampfprüfstock / Steam Test Device
Type Designator	DPS-HB-99/1
Type Approval Identification	TÜV.SV.15-1037
Variant	Overpressure Protection
Manufacturer	Waldemar Pruss Armaturenfabrik GmbH
Component Type	Type A (Ref. IEC 61508-2)
Mode of Operation	Low demand operation
Safety Function SF1: (Overpressure Protection)	The safety function is activated by activation of at least one pressure switch. The solenoid valves switch in the home position and the pressure chamber of the actuator opens with specified flow rate to the tank.
Safe State SS:	Pressure chamber of the actuator is opened to tank.

Failure Rates & FMEDA Summary [failure/10⁹ hrs = FIT]

Failure Rate Distribution	λ_{safe}	$\lambda_{dangerous\ detected}$	$\lambda_{dangerous\ undetected}$	$\lambda_{don't\ care}$	SFF [%]
SUM Channel (1oo3 architecture)	1,699.6	0	557.4	0	75


Specification of component Architecture

Architecture	1oo3	is the architecture of a single set of components/component of the analyzed type.
Hardware Fault Tolerance HFT	2	Due to HFT=2, three failures have impact on the safety function of a single set of components/component of the analyzed type.
MRT	8 h	MRT is the time required for repair of the set of components/component. MRT has marginal influence on the pfd-value. MRT is exemplary, deviating MRT must be considered in pfd-calculation.
Diagnostic Coverage (DC)	0 %	In case of missing automatic diagnosis: DC = 0 %. In case of implemented diagnostics: DC > 0% (value depends on efficiency of diagnosis). Safe Failure Fraction SFF increases by higher DC.
Diagnostic Test	-	No diagnostic tests to detect dangerous failures during operation.
Beta Factor	$\beta_{1oo3} = 2.5\%$ $\beta_{int} = 5\%$	Beta factor, which is considered in safety related parameter calculation of safety related architecture. Beta-factor is determined acc. to IEC 61508-6, appendix D to evaluate potential common cause failures for the system/sub-system.

Verification of SIL Capability

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

Proof Test Interval	1 year	2 years	3 years	4 years	5 years	6 years	7 years
PFDavg acc. IEC 61508-6, B3.2.2.6	6.12 E-05	1.22 E-04	1.84 E-04	2.46 E-04	3.09 E-04	3.72 E-04	4.37 E-04
Single component application Max. achievable SIL acc. Route 1 _H (IEC 61508-2-7.4.4.2)	SIL 4	SIL 3					

Calculated (company/name/date/signature)	INGENIEURBÜRO URBAN Anzinger Str. 24 D-85604 Pöding	Pöding, 2016-10-17	
---	--	--------------------	---



Assembly/Component Safety Data (acc. IEC 61508)

Set of Components/Component	Dampfprüfstock / Steam Test Device
Type Designator	DPS-HB-99/1
Type Approval Identification	TÜV.SV.15-1037
Variant	Over Temperature Protection
Manufacturer	Waldemar Pruss Armaturenfabrik GmbH
Component Type	Type A (Ref. IEC 61508-2)
Mode of Operation	Low demand operation
Safety Function SF2: (Over Temperature Protection)	The safety function is activated by exceeding the permitted temperatures by at least two temperature signals. The solenoid valves switch in the home position and the pressure chamber of the hydraulic actuator opens with specified flow rate to the tank.
Safe State SS:	Pressure chamber of the actuator is opened to tank.

Failure Rates & FMEDA Summary [failure/10⁹ hrs = FIT]

Failure Rate Distribution	λ_{safe}	$\lambda_{dangerous\ detected}$	$\lambda_{dangerous\ undetected}$	$\lambda_{don't\ care}$	SFF [%]
SUM Channel (2oo3 architecture)	869.5	0	393	0	69
SUM Channel (1oo3 architecture)	1,370.8	0	264.6	0	84

Remark: The temperature switches with relays are designed in a 2oo3 architecture. The solenoid valves for executing the safety function are designed in a 1oo3 architecture. This is considered in the safety related parameter calculation.


Specification of component Architecture

Architecture	2oo3 (partial 1oo3)	is the architecture of a single set of components/component of the analyzed type. Temperature switches and relays are designed in 2oo3 architecture, solenoid valves in 1oo3 architecture.
Hardware Fault Tolerance HFT	1 (partial 2)	Due to HFT=1, two failures have impact on the safety function of a single set of components/component of the analyzed type.
MRT	8 h	MRT is the time required for repair of the set of components/component. MRT has marginal influence on the pfd-value. MRT is exemplary, deviating MRT must be considered in pfd-calculation.
Diagnostic Coverage (DC)	0 %	In case of missing automatic diagnosis: DC = 0 %. In case of implemented diagnostics: DC > 0% (value depends on efficiency of diagnosis). Safe Failure Fraction SFF increases by higher DC.
Diagnostic Test	-	No diagnostic tests to detect dangerous failures during operation.
Beta Factor	$\beta_{2oo3} = 7.5\%$ $\beta_{1oo3} = 2.5\%$ $\beta_{int} = 5\%$	Beta factor, which is considered in safety related parameter calculation of safety related architecture. Beta-factor is determined acc. to IEC 61508-6, appendix D to evaluate potential common cause failures for the system/sub-system.

Verification of SIL Capability

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

Proof Test Interval	1 year	2 years	3 years	4 years	5 years	6 years	7 years
PFD_{avg} acc. IEC 61508-6, B3.2.2.5 and B3.2.2.6	1.69 E-04	3.57 E-04	5.66 E-04	7.95 E-04	1.04 E-03	1.31 E-03	1.60 E-03
Single component application Max. achievable SIL acc. Route 1 _H (IEC 61508-2-7.4.4.2)	SIL 3				SIL 2		

Calculated <small>(company/name/date/signature)</small>	INGENIEURBÜRO URBAN Anzinger Str. 24 D-85604 Pöding	Pöding, 2016-10-17	
--	--	--------------------	---



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 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 and Failure Rate Distribution

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, 1oo3, etc.)
- Hardware-Fault-Tolerance (HFT) (number of failures acceptable without dispatch on the safety function of the set of components/component)
- Mean Repair Time (MRT): In case of inspection, the MRT is the mean repair time of the component/set of components. In general, the MRT is application specific. The user is responsible to define realistic MRT for the specific application. The MRT given in the datasheet is exemplary, deviating MRT must be considered in pfd-calculation.
- Mean Time to Repair (MTTR): Mean time to repair the set of components/component in case of detected dangerous failure. MTTR is the sum of MRT and diagnosis test interval.
- Diagnostic Coverage: The diagnostic coverage is resulting from the diagnostic test 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).
- Diagnostic Test: The type of installed on-line automatic diagnostic test to detected dangerous failure during operation. The diagnostic test has to fulfill requirements acc. IEC 61508-2.
- Diagnostic Test Interval: Interval between diagnostic tests to detect dangerous failures. Longer diagnostic test intervals as specified in the datasheet has to be considered separately in safety parameter calculations, see IEC 61508-2, 7.4.9.4.
- Beta Factor: If the components/component is used in safety relevant architecture with a HFT ≥ 1 a beta factor has to be considered in safety loop calculations. The beta factor for the component is initial (β_{int}). To estimate the final beta factor for a specific application the effects of the architecture have to be considered. Thus the beta factor has to be calculated individual according IEC 61508-6, table D.5.
- Beta Factor Diagnostics: β_D is the fraction of dangerous common cause failures if the components/component is used in safety relevant architectures, which can be detected by diagnostic tests. see IEC 61508-6, table B1.

Verification of SIL-capability (examples)

The SIL verification consists of two steps:

- Step (1) = quantitative verification by calculation of the pfd-value / pfh-value depending from the defined Proof Test Interval and used architecture. The max. reachable SIL for the calculated safety loop within the component is used can be estimated according IEC 61508-1 table 2 (for low demand operation) or table 3 (for high demand operation)
- Step (2) = qualitative verification based on the architectural information of the set of components/component according route 1H, the qualitative max. SIL is defined in IEC 61508-2, 7.4.4.2.

The final achievable SIL is the minimum resulting SIL-value of step (1) and step (2): $\min \{(1); (2)\}$. The final achievable SIL is only relevant for the final safety loop not for a single component used in the safety loop.

IEC 61508-2 permits SIL 3 applications with an architecture with HFT = 0 according to route 1H in case of SFF > 90% for type A components. From technical safety point of view, this can only be accepted if the overall system risk is higher using a redundant safety related architecture in comparison using a single channel architecture. Using non-redundant safety related architectures for SIL 3 application is in general evaluated as insufficient. For SIL 3 application a safety related architecture with HFT ≥ 1 is highly recommended.

Further remarks using safety relevant parameters

- If operating medium is required (oil, air, etc.), failure rate of operating medium is not considered in the safety related parameter shown in this datasheet.
- Failure Rates considering diagnostic measures with DC > 0 may only be used if diagnosis with sufficient quality is installed in the application.
- Common cause failures, which can occur using the analyzed component in architectures, have to be considered by the user in safety loop calculations.
- If the subsystem is used in application with architectures, e.g. in a 1oo2 architecture, a beta-factor for the subsystem derived from β_{int} acc. IEC 61508-6, table D.5 has to be considered in the safety loop calculation of the application.

