



FMEDA including SFF determination and PFD calculation

Project:

HART multiplexer KFD2-HMM-16 together with KFD0-HMS-16
and 2700 HART Signal Multiplexer

Customer:

Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 02/4-11

Report No.: P+F 02/4-11 R006

Version V1, Revision R1.2, July 2002

Stephan Aschenbrenner

CONFIDENTIAL INFORMATION

Management summary

This report summarizes the results of the analysis carried out on the HART multiplexer KFD2-HMM-16 together with KFD0-HMS-16 and the 2700 HART Signal Multiplexer.

The assessment does not contain an evaluation of the correct functioning of the HART multiplexer but a statement about the interference freeness on the safety related 4..20mA loop when used for HART communication with regard to the suitability in part for Safety Instrumented System (SIS) usage in a particular Safety Integrity Level (SIL).

The failure rates are based on the Siemens standard SN 29500.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-4}$ to $< 10^{-3}$ for SIL 3 safety functions and $\geq 10^{-3}$ to $< 10^{-2}$ for SIL 2 safety functions. However, as the modules under consideration are only one part of an entire safety function they should not claim more than 10% of this range, i.e. they should be better than or equal to 10^{-4} for SIL 3 and better than or equal to 10^{-3} for SIL 2.

The modules under evaluation can be considered to be Type B components. However, the components that can contribute to a disturbance of the safety system are considered to be Type A components.

For **Type A** components the SFF has to fulfill the requirements as stated in table 2 of IEC 61508-2 which are the following:

	Hardware fault tolerance (HFT)		
	0	1	2
SIL 2	$60\% \leq \text{SFF} < 90\%$	$\text{SFF} < 60\%$	
SIL 3	$90\% \leq \text{SFF} < 99\%$	$60\% \leq \text{SFF} < 90\%$	$\text{SFF} < 60\%$

The following tables show under which conditions the critical components of the two modules that can contribute to a disturbance of the safety system fulfill this requirement (considering only one communication line being part of the safety function).

Table 1: KFD2-HMM-16 together with KFD0-HMS-16 without additional module interface

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD _{AVG} = 1.23E-06	PFD _{AVG} = 6.13E-06	PFD _{AVG} = 1.23E-05

The boxes marked in green () mean that the calculated PFD values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 10^{-3} . The PFD values even fulfill the requirements of higher SILs but the system does only fulfill the architectural constraints requirements (HFT/SFF) for SIL 2 which are set by table 2 of IEC 61508-2 for type A components having a hardware fault tolerance of 0.

If the HART multiplexer KFD2-HMM-16 and KFD0-HMS-16 are used together with the module interface as described in section 4.1 then two de-coupling capacitors have to fail to bring the (sub)system into a dangerous state. This corresponds to a hardware fault tolerance of 1.

Table 2: KFD2-HMM-16 together with KFD0-HMS-16 with additional module interface

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD _{AVG} = 6.13E-08	PFD _{AVG} = 3.07E-07	PFD _{AVG} = 6.13E-07

The boxes marked in green () mean that the calculated PFD values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 10^{-4} . The PFD values even fulfill the requirements of a higher SIL but the system does only fulfill the architectural constraints requirements (HFT/SFF) for SIL 3 which are set by table 2 of IEC 61508-2 for type A components having a hardware fault tolerance of 1.

Table 3: 2700 HART Signal Multiplexer

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD _{AVG} = 2.50E-07	PFD _{AVG} = 1.25E-06	PFD _{AVG} = 2.50E-06

The boxes marked in green () mean that the calculated PFD values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to 10^{-4} . The PFD values even fulfill the requirements of higher SILs but the system does only fulfill the architectural constraints requirements (HFT/SFF) for SIL 3 which are set by table 2 of IEC 61508-2 for type A components having a hardware fault tolerance of 1.

The calculations are based on the assumption that the HART multiplexer are mounted in an environment that is IP 54 compliant (e.g. housing, control cabinet or control room).