Failure Modes, Effects and Diagnostic Analysis

Project:
Electro-pneumatic Valve Positioner PositionMaster EDP300

Customer:

ABB Automation Products GmbH
Minden
Germany

Contract No.: ABB 06/05-37
Report No.: ABB EDP300 06/05-37 R021
Version V1, Revision R1; July 2011

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the Electro-pneumatic Valve Positioner PositionMaster EDP300 with hardware version 1.0. Table 1 gives an overview of the two possible safety applications of the considered Electro-pneumatic Valve Positioner PositionMaster EDP300.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) can be calculated for a subsystem. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 1: Overview of possible safety applications

[SA1]	Shutdown module
[SA2]	Fail-safe position with supply current of 0 mA

All other possible input and output variants or electronics are not covered by this report.

For [SA2] only the mechanical components of the Electro-pneumatic Valve Positioner PositionMaster EDP300 have been considered as all electronic components will only lead to additional "safe" or "no effect" failures. Considering the mechanical components only represents the worst-case.

As only the mechanical components and the shutdown module of the Electro-pneumatic Valve Positioner PositionMaster EDP300 are used for safety applications the device is considered to be a Type A[1] element. It consists of certain redundant parts but overall it is considered to be a device with a hardware fault tolerance of 0.

ABB Automation Products GmbH and *exida* together did a quantitative analysis of the Electro-pneumatic Valve Positioner PositionMaster EDP300 to calculate the failure rates using *exida*'s component database (see [N2]) for the different components. The failure rates used in this analysis are from the *exida* Electrical & Mechanical Component Reliability Handbook for Profile 3 [2].

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.2.

The following tables show how the above stated requirements are fulfilled for the considered Electro-pneumatic Valve Positioner PositionMaster EDP300.

[1] Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

[2] For details see Appendix 3.

Table 2: EDP300 with shutdown module ([SA1]) – IEC 61508 failure rates

Failure category	*exida* Profile 3 [FIT]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**1407**
Fail Dangerous Detected (λ_{DD}) [3]	**10**
Fail Dangerous Undetected (λ_{DU})	**181**

Annunciation Undetected [3]	11
No effect	1134
No part	5

Total failure rate of the safety function (λ_{Total})	**1598**
Safe failure fraction (SFF) [4]	**88%**
PTC	**90%**

SIL AC [5]	**---**

[3] There are not direct diagnostics but the shutdown module is equipped with a secondary output switch which has been treated as a safety measure for the primary output switch. Therefore dangerous detected and annunciation undetected failure rates are listed.

[4] The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[5] The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

Table 3: EDP300 with supply current of 0 mA ([SA2]) – IEC 61508 failure rates

Failure category	*exida* Profile 3 [FIT]
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**1347**
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Undetected (λ_{DU})	**176**

No effect	1105
No part	0

Total failure rate of the safety function (λ_{Total})	**1523**
Safe failure fraction (SFF) [6]	**88%**
PTC	**90%**

SIL AC [7]	**---**

A user of the considered Electro-pneumatic Valve Positioner PositionMaster EDP300 can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in sections 4.4.1 and 4.4.2 along with all assumptions.

The failure rates are valid for the useful life of the considered Electro-pneumatic Valve Positioner PositionMaster EDP300 (see Appendix 2) when operating as defined in the considered scenarios.

[6] The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[7] The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.