Failure Modes, Effects and Diagnostic Analysis

Project:
Intelligent Positioner TZIDC / TZIDC-200

Customer:
ABB Automation Products GmbH
Minden
Germany

Contract No.: ABB 07/07-40
Report No.: ABB 07/07-40 R016
Version V1, Revision R0, January 2008
Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the intelligent positioner TZIDC / TZIDC-200. Table 1 gives an overview of the two possible safety applications of the considered intelligent positioner TZIDC / TZIDC-200.

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) is calculated for the device. 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.

The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500.

For [SA2] only the mechanical components of the intelligent positioner TZIDC / TZIDC-200 have been considered as all electronic components will only lead to safe or residual failures. Considering the mechanical components only represents the worst-case.

As only the mechanical components and the shutdown module of the intelligent positioner TZIDC / TZIDC-200 are used for safety applications the device is considered to be a Type A[1] subsystem. It consists of certain redundant parts but overall it is considered to be a device with a hardware fault tolerance of 0.

For Type A subsystems the SFF has to be between 60% and 90% for SIL 2 (sub-) systems with a hardware fault tolerance of 0 according to table 2 of IEC 61508-2.

Failure rates that are assigned to the various failure modes of the (electro-)mechanical and pneumatic components of the intelligent positioner TZIDC / TZIDC-200 were obtained from field failure data collected and analyzed by ABB Automation Products GmbH using only operational hours from the warranty period of operation. Confidence Interval calculations were done using a chi-square distribution and an upper limit failure rate based on a 70% confidence factor per IEC 61508. The failure rate results were compared with industry databases and found to be within a reasonable range.

[1] Type A subsystem: "Non-complex" subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

Table 2: Summary for TZIDC / TZIDC-200 as shutdown module – Failure rates

Failure category	Failure rates (in FIT)
Fail Safe Detected	0
Fail Safe Undetected	695
Fail Dangerous Detected	0
Fail Dangerous Undetected	40
Residual	23
MTBF = MTTF + MTTR	150 years

Table 3: Summary for TZIDC / TZIDC-200 as shutdown module – IEC 61508 failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0 FIT	718 FIT	0 FIT	40 FIT	94%	0%	0%

Table 4: Summary for TZIDC / TZIDC-200 with supply current of 0 mA – Failure rates

Failure category	Failure rates (in FIT)
Fail Safe Detected	0
Fail Safe Undetected	651
Fail Dangerous Detected	0
Fail Dangerous Undetected	40
Residual	0
MTBF = MTTF + MTTR	165 years

Table 5: Summary for TZIDC / TZIDC-200 with supply current of 0 mA – IEC 61508 failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0 FIT	651 FIT	0 FIT	40 FIT	94%	0%	0%

A user of the intelligent positioner TZIDC / TZIDC-200 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 for different operating conditions is presented in sections 5.2 and 5.3 along with all assumptions.

It is important to realize that the “residual” failures are included in the “safe undetected” failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations.

The failure rates are valid for the useful life of the intelligent positioner TZIDC / TZIDC-200 (see Appendix 2).