



FMEDA and Prior-use Assessment

Project:

Intelligent Positioner TZIDC / TZIDC-200

Customer:

ABB Automation Products GmbH
Minden
Germany

Contract No.: ABB 03/09-13

Report No.: ABB 03/09-13 R003

Version V1, Revision R1.0, February 2004

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment with prior-use consideration according to IEC 61508 / IEC 61511 carried out on the intelligent positioner TZIDC / TZIDC-200 with software version V2.00. Table 1 gives an overview of the two possible 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 applications

Shutdown module
Smart positioner

For safety applications as a smart positioner only the 4..20 mA control input with the corresponding pressure output was considered. 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.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-3}$ to $< 10^{-2}$ for SIL 2 safety functions. A generally accepted distribution of PFD_{AVG} values of a SIF over the sensor part, logic solver part, and final element part assumes that 50% of the total SIF PFD_{AVG} value is caused by the final element. However, as the intelligent positioner TZIDC / TZIDC-200 is only one part of the final element it should not claim more than 20% of the range. For a SIL 2 application the total PFD_{AVG} value of the SIF should be smaller than $1,00E-02$, hence the maximum allowable PFD_{AVG} value for the positioner would then be $2,00E-03$.

The intelligent positioner TZIDC / TZIDC-200 when working as a smart positioner is considered to be a Type B¹ component with a hardware fault tolerance of 0.

If only the shutdown module of the intelligent positioner TZIDC / TZIDC-200 is used then the device is considered to be a Type A² component. It consists of certain redundant parts but overall it is considered to be a device with a hardware fault tolerance of 0.

Type B components with a SFF of 60% to $< 90\%$ must have a hardware fault tolerance of 1 according to table 3 of IEC 61508-2 for SIL 2 (sub-) systems.

For Type A components 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.

As the intelligent positioner TZIDC / TZIDC-200 is supposed to be a proven-in-use device, an assessment of the hardware with additional prior-use demonstration for the device and its software was carried out. The prior-use investigation was based on field return data collected and analyzed by ABB Automation Products GmbH. This data cannot cover the process connection. The prior-use justification for the process connection still needs to be done by the end-user.

Type B component: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

Type A component: “Non-complex” component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 5.1 the Type B intelligent positioner TZIDC / TZIDC-200 with a hardware fault tolerance of 0 and a SFF of 60% to < 90% are considered to be suitable for use in SIL 2 safety functions. The decision on the usage of prior-use devices, however, is always with the end-user.

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.

Table 2: Summary for TZIDC / TZIDC-200 as smart positioner – Failure rates

Failure category	Failure rates (in FIT)
Fail Safe Detected	45
Fail Safe Undetected	845
Fail Dangerous Detected	47
Fail Dangerous Undetected	172
No Effect	70
Annunciation Undetected	4
Not part	186
MTBF = MTTF + MTTR	84 years

Table 3: Summary for TZIDC / TZIDC-200 as smart positioner – IEC 61508 failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _S	DC _D
45 FIT	919 FIT	47 FIT	172 FIT	85%	5%	21%

Table 4: Summary for TZIDC / TZIDC-200 as smart positioner – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD _{AVG} = 7,52E-04	PFD _{AVG} = 3,75E-03	PFD _{AVG} = 7,48E-03

Table 5: 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
No Effect	23
Annunciation Undetected	0
Not part	0
MTBF = MTTF + MTTR	150 years

Table 6: 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 7: Summary for TZIDC / TZIDC-200 as shutdown module – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD _{AVG} = 1,76E-04	PFD _{AVG} = 8,78E-04	PFD _{AVG} = 1,75E-03

The boxes marked in yellow () mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 20% of this range, i.e. to be better than or equal to 2,00E-03. The boxes marked in green () mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996 and do fulfill the requirement to not claim more than 20% of this range, i.e. to be better than or equal to 2,00E-03.

The functional assessment has shown that the intelligent positioner TZIDC / TZIDC-200 has a PFD_{AVG} within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996 and a Safe Failure Fraction (SFF) of more than 85%. Based on the verification of "prior use" it can be used as a single device for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

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 section 5.2 and 5.3 along with all assumptions.

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