Failure Modes, Effects and Diagnostic Analysis

Project:

Repeater / Driver / Interface Boards
D1010, D1014, D1020, D1021, D1032, D1033, D1034

Customer:

G.M. International s.r.l
Villasanta
Italy

Contract No.: GM 03/07-24
Report No.: GM 03/07-24 R001
Version V1, Revision R1.0, April 2004

Stephan Aschenbrenner

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.
© All rights reserved.

Management summary

This report summarizes the results of the hardware assessment carried out on the Repeater / Driver / Interface Boards D1010, D1014, D1020, D1021, D1032, D1033 and D1034. Table 1 gives an overview of the different types that have been assessed.

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 the assessed boards

Type	Function	Output channels
D1010	Repeater Power Supply	1/2
D1014	Repeater Power Supply (HART compatible)	1/2
D1020	Powered Isolating Driver	1/2
D1021	Powered Isolating Driver with fault detection	1
D1032	Switch/Proximity Detector Repeater (relay output)	2/4
D1033	Switch/Proximity Detector Repeater (transistor output)	2/4
D1034	Contact/Proximity Detector Interface	1/2

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. 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. For a SIL 2 application the total PFD_{AVG} value of the SIF must be smaller than 1,00E-02, hence the maximum allowable PFD_{AVG} value for the assessed boards would then be 1,00E-03.

The Repeater / Driver / Interface Boards are considered to be Type A[1] components with a hardware fault tolerance of 0.

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.

Assuming that a connected logic solver can detect both over-range (fail high) and under-range (fail low), high and low failures can be classified as safe detected failures or dangerous detected failures depending on the application. The following tables show how the above stated requirements are fulfilled (considering one input / one output being part of the safety function).

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

Summary for D1010

Table 2: Failure rates

Failure category	Failure rates in FIT
Fail High (detected by the logic solver)	38
Fail Low (detected by the logic solver)	97
Fail Dangerous Undetected	70
No Effect	180
Annunciation Undetected	0
Not part	23
MTBF = MTTF + MTTR	280 years

Table 3: Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S [2]	DC_D [2]
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	97 FIT	180 FIT	38 FIT	70 FIT	81%	35%	35%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	38 FIT	180 FIT	97 FIT	70 FIT	81%	17%	58%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	135 FIT	180 FIT	0 FIT	70 FIT	81%	43%	0%

Table 4: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 3,07E-04	**PFD_{AVG} = 1,54E-03**	**PFD_{AVG} = 3,07E-03**

[2] DC means the diagnostic coverage (safe or dangerous) of the safety logic solver for the considered board.

Summary for D1014

Table 5: Failure rates

Failure category	Failure rates in FIT
Fail High (detected by the logic solver)	63
Fail Low (detected by the logic solver)	126
Fail Dangerous Undetected	34
No Effect	128
Annunciation Undetected	0
Not part	15
MTBF = MTTF + MTTR	312 years

Table 6: Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	126 FIT	128 FIT	63 FIT	34 FIT	90%	50%	65%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	63 FIT	128 FIT	126 FIT	34 FIT	90%	33%	79%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	189 FIT	128 FIT	0 FIT	34 FIT	90%	60%	0%

Table 7: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 1,47E-04	**PFD_{AVG} = 7,36E-04**	**PFD_{AVG} = 1,47E-03**

Summary for D1020

Table 8: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0 FIT	279 FIT	0 FIT	114 FIT	70%

Table 9: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 5,00E-04	**PFD_{AVG} = 2,50E-03**	**PFD_{AVG} = 4,99E-03**

Summary for D1021

Table 10: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0 FIT	285 FIT	0 FIT	118 FIT	70%

Table 11: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 5,18E-04	PFD_{AVG} = 2,59E-03	PFD_{AVG} = 5,16E-03

Summary for D1032

Table 12: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0 FIT	210 FIT	0 FIT	28 FIT	88%

Table 13: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 1,20E-04	PFD_{AVG} = 6,02E-04	PFD_{AVG} = 1,20E-03

Summary for D1033

Table 14: Failure rates according to IEC 61508

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0 FIT	212 FIT	0 FIT	35 FIT	85%

Table 15: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 1,55E-04	PFD_{AVG} = 7,72E-04	PFD_{AVG} = 1,54E-03

Summary for D1034

Table 16: Failure rates

Failure category	Failure rates in FIT
Fail High (detected by the logic solver)	41
Fail Low (detected by the logic solver)	66
Fail Dangerous Undetected	32
No Effect	168
Annunciation Undetected	0
Not part	6
MTBF = MTTF + MTTR	365 years

Table 17: Failure rates according to IEC 61508

Failure Categories	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{dd}$	66 FIT	168 FIT	41 FIT	32 FIT	89%	28%	56%
$\lambda_{low} = \lambda_{dd}$ $\lambda_{high} = \lambda_{sd}$	41 FIT	168 FIT	66 FIT	32 FIT	89%	20%	67%
$\lambda_{low} = \lambda_{sd}$ $\lambda_{high} = \lambda_{sd}$	107 FIT	168 FIT	0 FIT	32 FIT	89%	39%	0%

Table 18: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFD_{AVG} = 1,39E-04	PFD_{AVG} = 6,97E-04	PFD_{AVG} = 1,39E-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 10% of this range, i.e. to be better than or equal to 1,00E-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 10% of this range, i.e. to be better than or equal to 1,00E-03.

A user of the Repeater / Driver / Interface Boards D1010, D1014, D1020, D1021, D1032, D1033 and D1034 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 5.1 to 5.7 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.

The two channels on the D1010 and D1020 boards and the four channels on the D1032 and D1033 boards should not be used to increase the hardware fault tolerance, needed for a higher SIL of a certain safety function, as they contain common components.