REPORT

Date 2011-06-16 | Reference PX01982 rev2 | Page 1 (13)

Handled by, department
Andreas Söderberg
Electronics
+46 10 516 55 75, andreas.soderberg@sp.se

Rosemount Tank Radar AB
Emerson Process Management
P.O. Box 1305
SE-402 51 Göteborg
Sweden

Review of a hardware reliability analysis performed on the Rosemount 5400 series radar transmitter

(1 appendix)

This report (revision 2) replaces the test report PX01982 rev1, 2010-09-03. Guidance for application of the tested item has been revised.

Summary

The commission was to perform an independent review of a FMEDA (Failure Mode and Effects and Diagnostics Analysis) made on the Rosemount 5400 radar transmitter series used for level measurements in tanks.

The review showed that the hardware reliability of the Rosemount radar transmitters 5401 and 5402 were analyzed in accordance with the relevant requirements in IEC 61508-2:2010 As single devices they have the following SIL figures:

Measure	5401 transmitter	5402 transmitter
SFF	81%	83%
DC	72%	75%
HFT	1oo1D	1oo1D
λ_{DU} [FIT]	295	276
λ_{DD} [FIT]	748	809
λ_S [FIT]	493	528

Element	Proof test interval [Years]	PFDavg
5401 transmitter	1	1.29E-3
	2	2.58E-3
	5	6.41E-3
5402 transmitter	1	1.21E-3
	2	2.41E-3
	5	6.01E-3

The 5401 and 5402 transmitters are suitable for SIL 2 applications when selected on the basis of prior use according to IEC 61511-1, section 11.4.4.

This document may not be reproduced other than in full, except with the prior written approval of SP.

Contents

1 Commission

The commission was to perform an independent review of a FMEDA (Failure Mode and Effects and Diagnostics Analysis) made on the Rosemount 5400 radar transmitter series used for level measurements in tanks. The purpose with the review was to was to investigate if the hardware analysis conformed with all applicable requirements in IEC 61508-2:2010 and that the resulting PFD (average Probability of dangerous Failure on Demand) for the radar transmitter safety function corresponds with SIL1. No other requirements of IEC 61508:2010 than the hardware reliability requirements have been considered in this commission.

SP has not performed any system hardware analysis, reliability predictions, reliability modelling or reliability evaluations in this commission.

Note that IEC 61508:2010 does not define the term FMEDA but instead refers to the term FMEA (Failure Mode and Effects Analysis).

The following documents were used in this commission:

IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements

IEC 61508-2:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems

IEC 61508-4:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations

IEC 61508-6:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

IEC 61511-1:2003 Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements

ISO 13849-2:2003 Safety of machinery – Safety related parts of control systems – Part 2: Validation

1.1 Abbreviations

SIL – Safety Integrity Level

PFDavg – Average probability of dangerous failure on demand

HFT – Hardware fault tolerance

DC – Diagnostic coverage

SFF- Safe failure fraction

MTTR – Mean time to restoration (in this report = $t_{test\_interval} + t_{repair}$)

FMEDA – Failure mode and effects and diagnostics analysis

2 Client

Rosemount Tank Radar AB

Emerson Process Management

P.O. Box 1305

SE-402 51 Göteborg

Sweden

Contact: Björn Hallberg

3 Test object

No physical test object was used in this commission.

3.1 Technical documentation

The following technical documentation was delivered to SP from the client and have been used during this commission:

Table 1 Circiuit diagrams

Module name	Drawing number	Revision
Main Board (MB)	9150079-912	Iss 3
EMC Board (EB)	9150079-972	Iss 4
Terminal Block (TB)	03151-4211	IAB
Trans. Terminal block (TTB)	03151-4214	IAB
Barrier Board (BBH)	9240030-909	I03
Interface Board (IBH)	9150079-925	I02
Pulse Microwave Module (PMMC)	9150079-952	I02
Pulse Microwave Module (PMMK)	9150079-957	I03

Table 2 Bill of materials

Module name	Drawing number	Revision
Main Board (MB)	9150079-402	I07_Pxx_A4
Barrier Board (BBH)	9240030-517	r_a_090610
Interface Board (IBH)	9150079-414	r_b_081028
Pulse Microwave Module (PMMC)	9150079-001	I04
Pulse Microwave Module (PMMK)	9150079-005	I01
Pulse Microwave Module (PMMK)	9150079-957	I03
Note: For the hardware modules not included in this table their corresponding bill of material are included in the same document as the circuit diagrams.		

Table 3 Other technical documents

Document title	Drawing number	Revision
Rosemount 5400 series radar transmitter (block diagram overview)	9150079-902	6
TEST REPORT FAULT INSERTION TESTS 5400	5400-2010-044	1

Table 4 Reliability analysis and evaluation documents

Document title	Drawing number	Revision
5401 FMEDA system	N/a	R01
5402 FMEDA system	N/a	R01

3.2 Test object description

The 5400 series radar transmitters reviewed in this commission were based on the same hardware platform boards but had different radar circuit boards:

The 5401 radar transmitter operates with a frequency of 6.3 GHz (PMMC), and

The 5402 radar transmitter operates with a frequency of 26 GHz (PMMK)

The transmitters communicates the registered levels to other systems using a 4-20 mA current loop (output). The transmitters also communicates via a HART-protocol through the current loop. However, this protocol is not safety related.

The safety function of the 5400 series radar transmitters was defined as following:

The transmitter(s) shall not be unable to reach safe-state or deviate the output current from the corresponding level with more than 2%.

The 5400 series radar transmitters outputs below 3.75 mA or above 21.75 mA depending on the application in order to indicate safe-state.

The radar 5400 series transmitters were designed with a hardware fault tolerance (HFT) of zero (i.e. no hardware redundancy) and are considered as type B elements.

4 Performance

The review was carried out by Andreas Söderberg at SP in Borås, Sweden during 2010-02-26 to 2010-07-07.

All reviews have been performed by studying the clients documentation and through discussions with the client.

4.1 Review of the identification of safety related parts of the hardware

The clients technical documentation and hardware circuit diagrams were studied in order to understand how the safety related parts in the hardware were identified and distinguished from the non-safety related parts.

Any comments or remarks found in this review were noted in this report.

4.2 Review of the FMEDA analysis

The clients performed FMEDA was studied in order to verify the plausibility of the qualitative parts of the analysis and the correspondence with the applicable requirements in IEC 61508-2, Annex C. This review included the following:

a) The used FMEDA template format

b) The included electronic components and their corresponding fault models

Any comments or remarks found in the review were noted in this report.

4.3 Review of the reliability modelling and evaluation

The clients performed FMEDA was studied in order to verify the plausibility of the quantitative parts of the analysis and the correspondence with the applicable requirements in IEC 61508-2, Annex C. This review included the following:

a) Sources of failure rates

b) Distribution of failure rates between different failure modes

c) Inclusion of hardware used solely for diagnostic tests

d) Sources for the diagnostic coverage contribution of the implemented diagnostic tests for different failures

e) Reliability model design and evaluation

Any comments or remarks found in the review were noted in this report.

4.4 Review of the proof test principle and coverage

The procedure described for performing the proof test was reviewed in order to determine its conformance with the requirements in IEC 61508. The resulting coverage of the proof test was also reviewed.

Any comments or remarks found in the review were noted in this report.

4.5 Review of fault insertion tests

The fault modes which the client selected from the FMEDA to use in the fault insertion testing were reviewed in order to:

a) Determine that certain of the selected fault modes were suitable as sample tests in order to verify the FMEDA (regarding the assignment to consequences to different failure effects)

b) Validate implemented diagnostic tests

c) Validate independence between safety related parts and non-safety related parts of the hardware

SP attended during one day when the client performed fault insertion testing on the test object.

5 Result

The result applies to the tested item only.

5.1 Review of the identification of safety related parts of the hardware

Comments 1: The client have not used any special methods (such as block diagrams) for displaying the segregation between safety related and non-safety related parts of the hardware. In order to distinguish between these two types of hardware the failure modes of each individual component in the FMEDA have to be reviewed. Please refer to IEC 61508-2, clause 7.4.2.3 and 7.4.2.5 regarding E/E/PE-systems which implements both safety and non-safety functions.

Comment 2: Discussions were made between SP and the client regarding whether some components were safety related or not (certain filtering components and decoupling capacitors). These discussions were resolved during the commission.

Remarks:

None.

5.2 Review of the FMEDA analysis

a) The used FMEDA template format

Comments:

The FMEDA template used for review was an Excel-file exported from the Exida FMEDA tool V6.5.8 which was used by the client when performing the hardware reliability analysis.

The FMEDA template contained all the information required by IEC 61508 in order to calculate the safe failure fraction and the diagnostic coverage.

Remarks:

None.

b) The included electronic components and their corresponding fault models

Comment 1: All electronic components in each element were included in the FMEDA.

Comment 2: For passive or non-complex semiconductor components have fault models which are comparable with those specified in ISO 13 849-2 (and IEC 61496-1:2004) been used.

Comment 3: For more complex semiconductor circuits (such as analog-to-digital converters) have functional failure modes been assumed based on their internal functionality. These functional failure modes were not technically motivated in the technical documentation. This deviates from the fault model in ISO 13849 where a single fault of a complex semiconductor circuit may lead to an arbitrary functional failure.

Comment 4: For microprocessors are the same fault model used as specified in IEC 61508-2, Table A.1.

Remarks:

None.

General comments:

Comment 5: During the review, SP and the client made some minor modifications to ensure consistency between the circuit diagrams and the FMEDA.

5.3 Review of the reliability modelling and evaluation

All results which Rosemount concluded from the reliability modelling and evaluation were presented in Table 5 and Table 6 in this report.

a) Sources of failure rates

Comments:

All failure rates for the electronic components were retrieved from the database in the Exida FMEDA tool V6.5.8. The failure rates are based on a operating temperature of 40C.

Remarks:

None.

b) Distribution of failure rates between different failure modes

Comments:

The distribution of the failure rate between different fault modes was derived from the Exida FMEDA tool V6.5.8.

Remarks:

None.

c) Inclusion of hardware used solely for diagnostic tests

Comments:

Faults in components used for diagnostic tests were initially classified with the consequence: "Annunciation" which means that 5% of the failure rate for the particular failure mode is treated as dangerous and 95% as safe. This fault consequence is not supported in IEC 61508. According to IEC 61508-2, annex C the calculation of the SFF and the DC shall only include those components which are necessary for processing the safety function. The client changed all "annunciation" consequences to "dangerous undetected" which is conservative.

Remarks:

None.

d) Sources for the diagnostic coverage contribution of the implemented diagnostic tests for different failures

Comments:

The diagnostic coverage contribution used in this analysis was retrieved by the client from a previously performed analysis carried out by Exida. No sources for diagnostic coverage contribution have been reviewed in this commission.

Remarks:

None.

e) Reliability model design and evaluation

Comments:

The Exida FMEDA tool V6.5.8 was used to evaluate the resulting PFDavg-value, the SFF and the DC for the transmitters. The PFDavg was evaluated for three different proof-test intervals;

1 year, 2 years and 5 years. The architecture 1oo1D was used for both the 5401 and the 5402 transmitters.

Remarks:

None.

5.4 Review of the proof test principle and coverage

Comments:

The proof test procedure described by the client is included as appendix 1 in this report. This procedure is similar to the proof test procedure previously approved by Exida for the 5300 transmitter. This procedure provides a non-perfect proof test with a coverage no less than 95%. This coverage was accepted because of the similarities between the 5401/2 transmitters and the 5300 transmitter. However, no analysis to prove this coverage have been made by SP.

Remarks:

None.

5.5 Review of the fault insertion tests

Andreas Söderberg attended when the client performed the fault insertion tests on 2010-06-17 in the Rosemount laboratory in Gothenburg.

All fault modes applied and the used test configuration are described in the clients: TEST REPORT FAULT INSERTION TEST 5400.

a) Determine that some of the selected fault modes were suitable as sample tests in order to verify the FMEDA (regarding the assignment to consequences to different failure effects)

Comments:

The fault modes used were selected by discussions between the client and SP.

Remarks:

None.

b) Validate implemented diagnostic tests

Comments:

Certain fault modes used were selected because they were analyzed to lead to a dangerous failure which is detected with a high diagnostic coverage.

Remarks:

None.

c) Validate independence between safety related parts and non-safety related parts of the hardware

Comments:

Certain fault modes used were selected because they were analyzed to lead to a safe failure.

Remarks:

None.

d) Performance of fault insertion tests

Comments:

Two fault modes could not be inserted because the target card (BBH) was covered with material for protection which could not be removed. However, these two fault modes were not crucial for the insertion testing and were treated as dangerous and undetected in the analysis. The other inserted fault modes resulted in the expected fault behaviour in the FMEDA.

Remarks:

None.

6 Conclusion

Table 5 Information to be provided according to IEC 61508-2, clause 7.4.9.4

Item	Description	Result
a)	The failure modes of the elements in terms of its outputs that results in failure of the safety function and that are not detected by diagnostic tests	Failure modes causing the output current to deviate more than 2% of full span in respect to the actual measured level or failure modes disabling the transmitters ability to enter its fail-safe state.
b)	The estimated failure rate for the failure modes mentioned in a)	5401, λ_{DU} = 295 FIT 5402, λ_{DU} = 276 FIT
c)	The failure modes of the elements in terms of its outputs that results in the loss of the safety function and that are detected by diagnostic tests	These failure modes which are all listed in the FMEDA will cause the transmitter to enter its fail-safe state which is either to output a current < 3.75 mA or > 21.75mA.
d)	The estimated failure rate for the failure modes mentioned in c)	5401, λ_{DD} = 748 FIT 5402, λ_{DD} = 809 FIT
e)	Limits on the environment of the element that should be observed in order to maintain the validity of the estimated failure rates	The client have assumed an ambient temperature of 40C when predicting the failure rates. Also consult the reference manuals for the 5401 and 5402 transmitters for commissioning.
f)	Limits on the lifetime of the element	The useful lifetime for this type of transmitters is typically in the range of 8-12 years, in conformity with IEC 61508-2, clause7.4.9.5 (NOTE electrolytic capacitors may limit the useful lifetime).
g)	Proof tests and/or maintenance requirements	Proof tests shall be carried out on the element at an interval of 1 year, 2 years or 5 years according to the procedure described in appendix 1 in this report.
h)	The diagnostic coverage (DC) of the elements and the diagnostic test interval	5401, DC = 72% 5402, DC = 75%
i)	The diagnostic test interval for every failure mode detected by diagnostic tests	The sum of the diagnostic test interval and the repair time is less than the used MTTR ($t_{reparir}$ was selected to 8 hours and $t_{test\ interval}$ is 1 hour).
j)	The failure rate of the hardware used for diagnostics	5401, $\lambda_{diagnostics}$ = 70 FIT 5402, $\lambda_{diagnostics}$ = 70 FIT
k)	The mean repair time (MRT)	Refer to the Rosemount reference manuals for 5401 and 5402 transmitters for guidance regarding repair.
l)	The type of elements and the safe failure fraction (SFF) of the elements	5401, Type B element, λ_S = 493 FIT, SFF = 81% 5402, Type B element, λ_S = 528 FIT, SFF = 83%
m)	The hardware fault tolerance (HFT) of the elements	5401, HFT = 0 (1oo1D) 5402, HFT = 0 (1oo1D)

Table 6 Resulting safety integrity

Element	Proof test interval [Years]	PFDavg	Hardware safety integrity level (SIL), HFT=0 (See table 5)	Hardware safety integrity level (SIL), HFT=1 (note 1 and 2)	Hardware safety integrity level (SIL), HFT=0, Prior use applications (note 3)
5401 transmitter	1	1.29E-3	1	2	2
	2	2.58E-3	1	2	2
	5	6.41E-3	1	2	2
5402 transmitter	1	1.21E-3	1	2	2
	2	2.41E-3	1	2	2
	5	6.01E-3	1	2	2

Note 1: Regarding applications with these transmitters, when used as components in complete safety functions, please refer to IEC 61508-2, clause 7.4.4.2.3 and 7.4.4.2.4 or sector specific standards such as IEC 61511. These references describes how to increase the total safety integrity level (SIL) for a complete safety function by applying its components (e.g. the 5401 or the 5402 transmitters) in different redundant configurations.

Note 2: No conclusions can be made regarding the total achieved hardware safety integrity level (SIL) for a complete safety function only based on the internal design of the 5401 and 5402 transmitters. The reason for this is that how transmitters are combined (single- or redundant configurations) will be specific for each individual application and therefore the total achieved safety integrity level (SIL) must be evaluated separately in each different application.

Note 3: According to IEC 61511-1, section 11.4.4 the achieved safety integrity level (SIL) for sensors may be increased by one if the hardware of the device is selected on the basis of prior use, which is always decided by the end user.

SP Technical Research Institute of Sweden
Electronics - Software

Andreas Söderberg
Technical Officer

Johan Hedberg
Technical Manager

Appendix

Appendix 1 Proof test

A possible proof test consists of the following steps.

Required Tools: HART host/communicator and mA meter.

1. Bypass the logic solver or take other appropriate actions to avoid false trip.

2. Disable write protection if the function is enabled.

3. Using Loop Test, enter the mA value representing a high alarm current output and verify that the analog current reaches that value using the reference meter.
   This step tests for compliance voltage problems, such as low loop power supply voltage or increased wiring resistance.

4. Using Loop Test, enter the mA value representing a low alarm current output and verify that the analog current reaches that value using the reference meter.
   This step tests for possible quiescent current related failures.

5. Perform a two-point calibration check of the transmitter by adjusting the product level in two points in the measuring range.[1] Verify that the current output corresponds to the level input values using a known reference measurement.
   This step verifies that the analog output is correct in the operating range and that the Primary Variable is properly configured.

6. Enable write protection.

7. Restore the loop to full operation.

8. Remove the bypass from the safety logic solver or otherwise restore normal operation.

9. Document the test result for future reference.

This test detects approximately 95% of the possible Dangerous Undetected (DU) failures of the transmitter.

[1] *For best performance, use the 4 - 20 mA range points as calibration points.*