exida.com®
excellence in dependable automation

Failure Modes, Effects and Diagnostic Analysis

Project:
3144P SIS Temperature Transmitter

Customer:
Rosemount Inc.
Chanhassen, MN
USA

Contract No.: ROS 04/08-19
Report No.: ROS 04/08-19 R003
Version V2, Revision R1, July 26, 2006
John C. Grebe – Rachel Amkreutz

Management summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the 3144P SIS Temperature Transmitter with Hardware version 1 and Software version 5.2.2. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the 3144P SIS Temperature Transmitter, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 3144P SIS Temperature Transmitter is a two wire, 4 – 20 mA smart device. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. The transmitter can be equipped with or without display.

The 3144P SIS Temperature Transmitter is classified as a Type B[1] device according to IEC61508, having a hardware fault tolerance of 0.

The 3144P SIS Temperature Transmitter together with a temperature-sensing element becomes a temperature sensor assembly. When using the results of this FMEDA in a SIL verification assessment, the failure rates and failure modes of the temperature sensing element must be considered. This is discussed in detail in Section 5.1 and Appendix B. Failure rates for the 3144P SIS Temperature Assembly when using thermocouples in a low stress environment are listed in Table 1. The dual sensing element mode assumes PV is S1, S2 or first good and drift alert is set to alarm.

Table 1 Failure rates 3144P SIS Temperature Assembly with T/C

Failure category		**Failure rate (in FIT)**			
		Single TC mode		**Dual TC mode Drift Alert = Alarm**	
Fail High (detected by the logic solver)		28		28	
Fail Low (detected by the logic solver)		5089		5347	
	Fail detected (int. diag.)*	5064		5322	
	Fail low (inherently)	25		25	
Fail Dangerous Undetected		291		44	
No Effect		103		107	
Annunciation Undetected		5		5	
Safe Failure Fraction		94.7%		99.2%	

* These failures follow the setting of the Alarm switch and result in either a High or Low output of the transmitter. It is assumed that upon the detection of a failure the output will be sent downscale, therefore all detected failures are listed as a sub-category of the Fail Low failure category. If the Alarm switch is set to High, these failures would need to be added to the Fail High failure category.

---

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

Failure rates for the 3144P SIS Temperature Assembly when using RTDs in a low stress environment are listed in Table 1. The dual sensing element mode assumes PV is S1, S2 or first good and drift alert is set to alarm.

Table 2 Failure rates 3144P SIS Temperature Assembly using RTDs

Failure category		Failure rate (in FIT)			
		Single 4-wire RTD mode		Dual 3-wire RTD mode, Drift Alert = Alarm	
Fail High (detected by the logic solver)		28		28	
Fail Low (detected by the logic solver)		2311		2338	
	Fail detected (int. diag.)*	2286		2313	
	Fail low (inherently)	25		25	
Fail Dangerous Undetected		59		42	
No Effect		107		111	
Annunciation Undetected		5		5	
Safe Failure Fraction		97.6%		98.3%	

* These failures follow the setting of the Alarm switch and result in either a High or Low output of the transmitter. It is assumed that upon the detection of a failure the output will be sent downscale, therefore all detected failures are listed as a sub-category of the Fail Low failure category. If the Alarm switch is set to High, these failures would need to be added to the Fail High failure category.

The failure rates are valid for the useful lifetime of the transmitter, see Appendix A.

A user of the 3144P SIS Temperature Transmitter 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 section 4.5 along with all assumptions.

Table of Contents

1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not include an assessment of the development process

Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511

Option 2 is an assessment by *exida* according to the relevant functional safety standard(s) like IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics. In addition, this option includes an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and may help justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices when combined with plant specific proven-in-use records.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by *exida* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This assessment shall be done according to option 1.

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the 3144P SIS Temperature Transmitter. From this, failure rates, Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

The information in this report can be used to evaluate whether a sensor (or logic / final element subsystem) meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508.

2 Project management

2.1 *exida.com*

exida.com is one of the world's leading knowledge companies specializing in automation system safety and availability with over 200 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TÜV and manufacturers, *exida.com* is a partnership with offices around the world. *exida.com* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida.com* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Rosemount Inc.	Manufacturer of the 3144P SIS Temperature Transmitter
exida.com	Project leader of the FMEDA

Rosemount Inc. contracted *exida.com* in August 2004 with the FMEDA and PFD_{AVG} calculation of the above mentioned device.

2.3 Standards / Literature used

The services delivered by *exida.com* were performed based on the following standards / literature.

[N1]	IEC 61508-2: 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	FMD-91 & FMD-97, RAC 1991, 1997	Failure Mode / Mechanism Distributions, Reliability Analysis Center. Statistical compilation of failure mode distributions for a wide range of components
[N3]	NPRD-95, RAC 1995	Nonelectronic Parts Reliability Data, Reliability Analysis Center. Statistical compilation of failure rate data, incl. mechanical and electrical sensors
[N4]	SN 29500	Failure rates of components
[N5]	US MIL-STD-1629	Failure Mode and Effects Analysis, National Technical Information Service, Springfield, VA. MIL 1629.
[N6]	Telcordia (Bellcore) Failure rate database and models	Statistical compilation of failure rate data over a wide range of applications along with models for estimating failure rates as a function of the application.
[N7]	Safety Equipment Reliability Handbook, 2003	exida.com L.L.C, Safety Equipment Reliability Handbook, 2003, ISBN 0-9727234-0-4
[N8]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN #1-55617-636-8. Reference on FMEDA methods

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	03144-2110, Rev AL, 07/18/2006	CCA, Electronics Board Coated, Sheet 1 & 2
[D2]	03144-2109, Rev AH, 07/18/2006	PWB, Main Board, Sheet 1 through 3
[D3]	03144-2108, Rev AJ, 07/18/2006	Schematic, 3144P Electronics Board Fieldmount, Sheet 1 through 3
[D4]	ROS 04-08-19 R001 V110, 10/04/04	3144 Regression Fault Injection Test Report
[D5]	3144P SIS Diagnostic design proposal	3144P SIS Diagnostics
[D6]	E-mails: 3144P FMEDA	E-mail conversations on 3144P SIS Diagnostics

2.4.2 Documentation generated by *exida.com*

[R1]	3144P Temp Transmitter 3 Wire RTD Portion of sheet 3 of 3 Rev 03.xls	Failure rate calculations 3 Wire RTD, 3144P SIS Temperature Transmitter, June 15 2006
[R2]	3144P Temp Transmitter Common Portion of sheet 3 of 3 Rev 03.xls	Failure rate calculations Common Portion, 3144P SIS Temperature Transmitter, June 15 2006
[R3]	3144P Temp Transmitter Dual 3 Wire RTD Portion of sheet 3 of 3 Rev 03.xls	Failure rate calculations Dual 3 Wire RTD, 3144P SIS Temperature Transmitter, June 15 2006
[R4]	3144P Temp Transmitter Dual TC Portion of sheet 3 of 3 Rev 03.xls	Failure rate calculations Dual TC, 3144P SIS Temperature Transmitter, June 15 2006
[R5]	3144P Temp Transmitter sheet 1 of 3 Rev 03.xls	Failure rate calculations, 3144P SIS Temperature Transmitter, June 15 2006
[R6]	3144P Temp Transmitter sheet 2 of 3 Rev 03.xls	Failure rate calculations, 3144P SIS Temperature Transmitter, June 15 2006
[R7]	3144P Temp Transmitter Summary Rev 03.xls	Failure rate calculations Summary, 3144P SIS Temperature Transmitter, June 15 2006
[R8]	3144P Temp Transmitter TC Portion of sheet 3 of 3 Rev 03.xls	Failure rate calculations TC Portion, 3144P SIS Temperature Transmitter, , June 15 2006
[R9]	ROS 04-08-19 R003 V2 R1 3144P SIS FMEDA.doc	FMEDA report, 3144P SIS Temperature Transmitter, July 26, 2006

3 Product Description

This report documents the results of the Failure Modes, Effects and Diagnostics Analysis performed for the 3144P SIS Temperature Transmitter with Hardware version 1 and Software version 5.2.2. The 3144P SIS Temperature Transmitter is a two wire, 4 – 20 mA smart device. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. The transmitter can be equipped with or without display.

The 3144P SIS Temperature Transmitter is classified as a Type B[2] device according to IEC61508, having a hardware fault tolerance of 0. Combined with one or two temperature sensing elements, the 3144P SIS transmitter becomes a temperature sensor assembly. The temperature sensing elements that can be connected to the 3144P SIS Temperature Transmitter are:

- 2-, 3-, and 4-wire RTD
- Thermocouple
- Millivolt input (–10 to 100mV)
- 2-, 3-, and 4-wire Ohm input (0 to 2000Ω)

The FMEDA has been performed for different input sensing element configurations of the 3144P SIS transmitter, i.e. 3-wire RTD, 4-wire RTD, and thermocouple. Estimates have been made of the temperature sensing element failure rates given the ability of the 3144P SIS transmitter to detect several failure modes of the temperature sensing element.

---

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

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation received from Rosemount Inc. and is documented in [R1] through [R8]. When the effect of a certain failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level [D4].

4.1 Description of the failure categories

In order to judge the failure behavior of the 3144P SIS Temperature Transmitter, the following definitions for the failure of the product were considered.

Fail-Safe State	State where the process reaches a safe situation. Depending on the application the fail-safe state is defined as the output going to fail low or fail high.
Fail Safe	Failure that causes the transmitter to go to the defined fail-safe state without a demand from the process. Safe failures are divided into safe detected (SD) and safe undetected (SU) failures.
Fail Dangerous	Failure that deviates the measured input state or the actual output by more than 2% of span and that leaves the output within active scale.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by internal diagnostics (These failures may be converted to the selected fail-safe state).
Fail High	Failure that causes the output signal to go to the maximum output current (> 20.9 mA, output saturate high) or high alarm (>21 mA)
Fail Low	Failure that causes the output signal to go to the minimum output current (< 3.7 mA, output saturate low) or low alarm (3.5, 3.75 mA)
Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Annunciation Undetected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics.

The failure categories listed above expand on the categories listed in [N1] which are only safe and dangerous, both detected and undetected. The reason for this is that, depending on the application, a Fail High or a Fail Low can either be safe or dangerous and may be detected or undetected depending on the programming of the logic solver. Consequently, during a Safety Integrity Level (SIL) verification assessment the Fail High and Fail Low failure categories need to be classified as either safe or dangerous.

The Annunciation Undetected failures are provided for those who wish to do reliability modeling more detailed than required by IEC61508. In IEC 61508 [N1] the No Effect and Annunciation Undetected failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with the extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure rates

The failure rate data used by *exida.com* in this FMEDA is from a proprietary component failure rate database derived using the Telcordia [N6] failure rate database/models, the SN29500 [N4] failure rate database and other sources. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 645-1, Class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 3144P SIS Temperature Transmitter with 4..20 mA output.

- Only a single component failure will fail the entire product
- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:

  - IEC 645-1, Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40ºC. Humidity levels are assumed within manufacturer's rating.
- External power supply failure rates are not included.

4.4 Behavior of the safety logic solver

Depending on the application, the following scenarios are possible:

- Low Trip: the safety function will go to the predefined fail-safe state when the process value below a predefined low set value. A current < 3.75mA (Fail Low) is below the specified trip-point.
- High Trip: the safety function will go to the predefined fail-safe state when the process value exceeds a predefined high set value. A current > 21mA (Fail High) is above the specified trip-point.

The Fail Low and Fail High failures can either be detected or undetected by a connected logic solver. The PLC Detection Behavior in Table 3 represents the under-range and over-range detection capability of the connected logic solver.

Table 3 Application example

Application	**PLC Detection Behavior**	λ_{low}	λ_{high}
Low trip	< 4mA	$= \lambda_{sd}$	$= \lambda_{du}$
Low trip	> 20mA	$= \lambda_{su}$	$= \lambda_{dd}$
Low trip	< 4mA and > 20mA	$= \lambda_{sd}$	$= \lambda_{dd}$
Low trip	-	$= \lambda_{su}$	$= \lambda_{du}$
High trip	< 4mA	$= \lambda_{dd}$	$= \lambda_{su}$
High trip	> 20mA	$= \lambda_{du}$	$= \lambda_{sd}$
High trip	< 4mA and > 20mA	$= \lambda_{dd}$	$= \lambda_{sd}$
High trip	-	$= \lambda_{du}$	$= \lambda_{su}$

In this analysis it is assumed that the logic solver is able to detect under-range and over-range currents, therefore the yellow highlighted behavior is assumed.

4.5 Results

Using reliability data extracted from the exida.com component reliability database the following failure rates resulted from the 3144P SIS Temperature Transmitter FMEDA.

Table 4 Failure rates 3144P SIS Temperature Transmitter (T/C configuration)

Failure category		**Failure rate (in FIT)**	
		Single TC mode	**Dual TC mode**
Fail High (detected by the logic solver)		28	28
Fail Low (detected by the logic solver)		339	349
	Fail detected (int. diag.)[3]	314	324
	Fail low (inherently)	25	25
Fail Dangerous Undetected		41	41
No Effect		103	107
Annunciation Undetected		5	5

Table 5 Failure rates 3144P SIS Temperature Transmitter (RTD configuration)

Failure category		**Failure rate (in FIT)**	
		Single RTD mode	**Dual RTD mode (3-wire RTD)**
Fail High (detected by the logic solver)		28	28
Fail Low (detected by the logic solver)		331	342
	Fail detected (int. diag.)[3]	306	317
	Fail low (inherently)	25	25
Fail Dangerous Undetected		39	38
No Effect		107	111
Annunciation Undetected		5	5

According to IEC 61508 [N1], the Safe Failure Fraction (SFF) of the 3144P SIS Temperature Transmitter should be calculated. The SFF is the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault. As both the Fail High and Fail Low failure categories are assumed to be detected by the logic solver (regardless of the fact if their effect is safe or dangerous), the Safe Failure Fraction can be calculated independently of the 3144P SIS Temperature Transmitter application.

This is reflected in the following formula for SFF:

$SFF = 1 – \lambda_{du} / \lambda_{total}$

Note that according to IEC61508 definition the No Effect and Annunciation Undetected failures are classified as safe and therefore need to be considered in the Safe Failure Fraction calculation and are included in the total failure rate.

---

[3] These failures follow the setting of the Alarm switch and result in either a High or Low output of the transmitter. It is assumed that upon the detection of a failure the output will be sent downscale, therefore all detected failures are listed as a sub-category of the Fail Low failure category. If the Alarm switch is set to High Alarm, these failures would need to be added to the Fail High failure category.

Table 6 Safe Failure Fraction of 3144P SIS Temperature Transmitter

3144P SIS Temperature Transmitter	SFF
3144P SIS, Single T/C mode	92.1%
3144P SIS, Dual T/C mode	92.2%
3144P SIS, Single RTD mode	92.3%
3144P SIS, Dual RTD mode	92.8%

The architectural constraint type for 3144P SIS Temperature Transmitter is B. The SFF and required SIL determine the level of hardware fault tolerance that is required per requirements of IEC 61508 [N1] or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

5 Using the FMEDA results

5.1 Temperature sensing elements

The 3144P SIS Temperature Transmitter together with a temperature-sensing element becomes a temperature sensor. When using the results of this FMEDA in a SIL verification assessment, the failure rates and failure modes of the temperature sensing element must be considered. Typical failure rates for thermocouples and RTDs are listed in Table 7.

Table 7 Typical failure rates thermocouples and RTDs

Temperature Sensing Element	Failure rate (in FIT)
Thermocouple low stress environment	5,000
Thermocouple high stress environment	20,000
RTD low stress environment	2,000
RTD high stress environment	8,000

The following sections give examples on how to combine the temperature-sensing element failure rates and the transmitter failures. The examples given are for PV (Process Value) set to represent Sensor 1 or Sensor 2 when using a single sensor, either TC or RTD. More information on how to combine temperature-sensing element failure rates and transmitter failure rates for other configurations, including the use of dual sensing-elements is given in Appendix B.

5.1.1 3144P SIS Temperature Transmitter with single thermocouple

The failure mode distributions for thermocouples vary in published literature but there is strong agreement that open circuit or “burn-out” failure is the dominant failure mode. While some estimates put this failure mode at 99%+, a more conservative failure rate distribution suitable for SIS applications is shown in the Table 8 when close-coupled thermocouples are used with the transmitter. The drift failure mode is primarily due to T/C aging. The 3144P SIS Temperature Transmitter will detect a TC burnout failure and drive its output to the specified failure state.

Table 8 Typical failure mode distributions for thermocouples

Temperature Sensing Element	Percentage
Open Circuit (Burn-out)	95%
Wire Short (Temperature measurement in error)	1%
Drift (Temperature measurement in error)	4%

A complete temperature sensor assembly consisting of 3144P SIS Temperature Transmitter and a closely coupled thermocouple supplied with the 3144P SIS Temperature Transmitter can be modeled by considering a series subsystem where failure occurs if there is a failure in either component. For such a system, failure rates are added. Assuming that the 3144P SIS Temperature Transmitter is programmed to drive its output low on detected failure, the failure rate contribution for the thermocouple in a low stress environment is:

- λ^{L} = (5000) * (0.95) = 4750 FIT
- λ^{DU} = (5000) * (0.05) = 250 FIT

When these failure rates are added to the failure rates of the 3144P SIS Temperature Transmitter, single TC mode (see Table 4), the total for the temperature sensor subsystem is:

- $\lambda^L = 4750 + 339 = 5089$ FIT
- $\lambda^H = 28$ FIT
- $\lambda^{DU} = 250 + 41 = 291$ FIT

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions. For these circumstances, the Safe Failure Fraction of this temperature sensor subsystem is 94.7%.

5.1.2 3144P SIS Temperature Transmitter with RTD

The failure mode distribution for an RTD also depends on application with the key variables being stress level, RTD wire length and RTD type (3-wire or 4-wire). The key stress variables are high vibration and frequent temperature cycling as these are known to cause cracks in the substrate leading to broken lead connection welds. Failure rate distributions obtained from a manufacturer are shown in Table 9. The 3144P SIS Temperature Transmitter will detect open circuit and short circuit RTD failures and drive its output to the specified failure state.

Table 9 Typical failure mode distributions for 3-Wire and 4-Wire RTDs in a Low Stress environment or using a cushioned sensor construction

RTD Failure Modes – Close coupled element	Percentage	
	3-wire RTD	4-wire RTD
Open Circuit	50%	70%
Short Circuit	30%	29%
Drift (Temperature measurement in error)	20%	1%

A complete temperature sensor assembly consisting of 3144P SIS Temperature Transmitter and a closely coupled, cushioned 4-wire RTD supplied with the 3144P SIS Temperature Transmitter can be modeled by considering a series subsystem where failure occurs if either component fails. For such a system, failure rates are added. Assuming that the 3144P SIS Temperature Transmitter is programmed to drive the output low on detected failure, the failure rate contribution for the 4-wire RTD in a low stress environment is:

- $\lambda^L = (2000) * (0.70 + 0.29) = 1980$ FIT
- $\lambda^{DU} = (2000) * (0.01) = 20$ FIT

When these failure rates are added to the failure rate of the 3144P SIS Temperature Transmitter, single RTD mode (see Table 5), the total for the temperature sensor subsystem is:

- $\lambda^L = 1980 + 331 = 2311$ FIT
- $\lambda^H = 28$ FIT
- $\lambda^{DU} = 20 + 39 = 59$ FIT

These numbers could be used in safety instrumented function SIL verification calculations for this set of assumptions. The Safe Failure Fraction for this temperature subsystem, given the assumptions, is 97.6%.

5.2 Converting failure rates to IEC 61508 format

The failure rates that are derived from the FMEDA for the 3144P SIS Temperature Transmitter are in a format different from the IEC 61508 format. This section will explain how the failure rates can be converted into the IEC 61508 format.

First of all, depending on the application, the high and low failure rates of the 3144P SIS Temperature Transmitter must be classified as either safe or dangerous. Assume an application where a safety action needs to be performed if the temperature drops below a certain level. The 3144P SIS Temperature Transmitter will therefore be configured with a low trip level. A low failure of the transmitter will cause the transmitter output to go through the low trip level. Consequently the transmitter will indicate that the safety action needs to be performed. Therefore a low failure can be classified as a safe failure for this application. A high failure on the other hand will cause the transmitter output to move away from the trip level and therefore not cause a trip. The failure will prevent the transmitter from indicating that the safety action needs to be performed and is therefore classified as a dangerous failure for this application.

Assuming that the logic solver can detect both over-range and under-range, a low failure can be classified as a safe detected failure and a high failure can be classified as a dangerous detected failure. For this application, assuming 3144P SIS Temperature Transmitter with single RTD, the following would then be the case:

$\lambda^{H} = \lambda^{DD} =$ 28 FIT

$\lambda^{L} = \lambda^{SD} =$ 2311 FIT

$\lambda^{DU} =$ 59 FIT

In a similar way the high and low failure rates can be classified as respectively safe detected and dangerous detected in case the application has a high trip level. The failure rates as displayed above are the same failure rates as stored in the exida.com equipment database that is part of the online SIL verification tool, SILver.

Furthermore the No Effect failures and Annunciation Undetected failure are classified as Safe Undetected failures according to IEC 61508. Note that these failures will not affect system reliability or safety, and should not be included in spurious trip calculations.

$\lambda^{SU} =$ 112 FIT

Note that the dangerous undetected failures will of course remain dangerous undetected.

Table 10 shows the failure rates according to IEC 61508 for this application, assuming 3144P SIS Temperature Transmitter with single RTD.

Table 10: Failure rates according to IEC 61508 – 3144P SIS with single RTD

Failure Categories	λ^{SD}	λ^{SU}	λ^{DD}	λ^{DU}	**SFF**
Low trip	2311 FIT	112 FIT	28 FIT	59 FIT	97.6%
High trip	28 FIT	112 FIT	2311 FIT	59 FIT	97.6%

5.3 PFD_{AVG} calculation 3144P SIS Temperature Transmitter

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) 3144P SIS Temperature Transmitter with single 4-wire RTD. The failure rate data used in this calculation is displayed in section 5.1.2. It is assumed that the transmitter output is send low upon detection of failure and the safety function has a low trip point.

The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Figure 1. As shown in the figure the PFD_{AVG} value for a single 3144P SIS Temperature Transmitter with single 4-wire RTD, with a proof test interval of 1 year equals 2.58E-04.

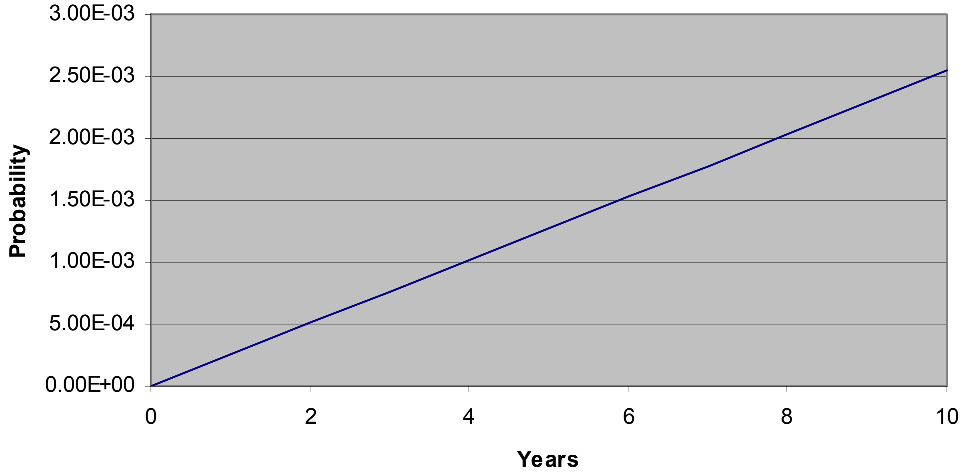

Figure 1: PFD_{AVG} 3144P SIS Temperature Transmitter with single RTD

For SIL 2 applications, the PFD_{AVG} value for the a safety function needs to be < 10^{-2}. This means that for a SIL 2 application, the PFD_{AVG} for a 1-year Proof Test Interval of the 3144P SIS Temperature Transmitter with single 4-wire RTD is equal to 2.6% of the range. These results must be considered in combination with PFD_{AVG} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

6 Terms and Definitions

FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HART	Highway Addressable Remote Transducer
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A component	"Non-Complex" component (using discrete elements); for details see 7.4.3.1.3 of IEC 61508-2
Type B component	"Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2

7 Status of the document

7.1 Liability

exida.com prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida.com* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

7.2 Releases

Version:	V2	
Revision:	R1	
Version History:	V2, R1:	Minor hardware revision; July 26, 2006
	V1, R2:	Integrated comments from Rosemount, October 25, 2004
	V1, R1:	Released to Rosemount; October 21, 2004
	V0, R1:	Initial version; October 12, 2004
Authors:	John C. Grebe – Rachel Amkreutz	
Review:	V1, R1:	Wally Baker and Randy Paschke (Rosemount); October 22, 2004
	V0, R1:	Wally Baker and Randy Paschke (Rosemount); October 18, 2004
Release status:	Released	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Ir. Rachel Amkreutz, Safety Engineer

John C. Grebe Jr., Principal Engineer

William M Goble

Dr. William M. Goble, Principal Partner

Appendix A: Lifetime of critical components

According to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.3) this only applies provided that the useful lifetime[4] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components. Therefore it is obvious that the PFD_{AVG} calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

Table 11 shows which electrolytic capacitors are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 11: Useful lifetime of electrolytic capacitors contributing to λ^{DU}

Type	Useful life at 40°C
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	Appr. 500 000 hours

As there are no aluminium electrolytic capacitors used, the limiting factors with regard to the useful lifetime of the system are the Tantalum electrolytic capacitors. The Tantalum electrolytic capacitors have an estimated useful lifetime of about 50 years.

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

---

[4] Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

Appendix B: Failure rates for various transmitter modes

This Appendix discusses in more detail how to combine the 3144P SIS Temperature Transmitter failure rates with sensing element failure rates and how to take credit for diagnostics provided by the transmitter on the sensing element (Drift Alert = Alarm).

Table 12 3144P SIS Temperature Transmitter modes

S1 Type	S2 Type	Suspend Non-PV Faults	Drift Alert[5]	Primary Variable (PV)	Calculation
T/C, 3 Wire RTD, 4 wire RTD	Disabled	X	N/A	S1	1
Disabled	T/C, 3 Wire RTD	X	N/A	S2	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	S1	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	S1	2
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	S1	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	S1	2*
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	S2	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	S2	2
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	S2	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	S2	2
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	Differential	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	Differential	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	Differential	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	Differential	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	Average	3
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	Average	4
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	Average	3*
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	Average	4*
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Disable	First Good	1
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Disable	Alarm	First Good	2
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Disable	First Good	1*
T/C, 3 Wire RTD	T/C, 3 Wire RTD	Enable	Alarm	First Good	2

* These modes represent “Hot back-up”. Using the calculation method as described will results in accurate numbers for PFD_{AVG}, but will overestimate the false trip rate. (The sensing elements are configured as a 2oo2 voting and will not alarm on a single sensor failure).

Calculation 1

Single Sensor configured, PV = S1 or PV = S2 or,

Dual Sensors configured, PV = S1, PV = S2 or PV = First Good and Drift Alert = disabled

Modeled as a series subsystem where failure occurs if either sensing element or transmitter fails. For such a system, failure rates are added. Use single mode failure rates for the 3144P SIS Temperature transmitter and add sensing element failure rates (single element). This has been described in detail in sections 5.1.1 and 5.1.2.

---

[5] For purposes of safety validation, Drift Alert = Warning is considered the same as Drift Alert = disabled

Calculation 2

Dual Sensors configured, PV = S1 or PV = S2 or PV = First Good, and Drift Alert = alarm

Modeled as a series subsystem where failure occurs if either component fails. For such a system, failure rates are added. Use dual mode failure rates for the 3144P SIS Temperature transmitter and add sensing element failure rates (single element). The sensing element failure rates should reflect the additional coverage on the drift failures (99%) provided by the Drift Alert.

Example: 3144P SIS with dual 3-wire RTDs

Table 13 Typical failure rates for 3-wire RTDs, Low Stress environment / cushioned sensor

RTD Failure Rates – Close coupled element	FIT
Open Circuit	50%
Short Circuit	30%
Drift (Temperature measurement in error)	20%

Assuming that the 3144P SIS Temperature Transmitter is programmed to drive the output low on detected failure, the failure rate contribution for the 3-wire RTD in a low stress environment is:

- λ^{L} = (2000) * (0.50 + 0.30 + 0.99·0.2) = 1996 FIT
- λ^{DU} = (2000) * (0.01·0.20) = 4 FIT

When these failure rates are added to the failure rate of the 3144P SIS Temperature Transmitter, single RTD mode (see Table 5, second column), the total for the temperature sensor subsystem is:

- λ^{L} = 1996 + 342 = 2338 FIT
- λ^{H} = 28 FIT
- λ^{DU} = 4 + 38 = 42 FIT

Calculation 3

Dual Sensors configured, PV = Average or PV = Differential mode, Drift Alert = disabled

Both sensing elements need to function. Use single mode failure rates for the 3144P SIS Temperature transmitter (single mode failure rates are selected because Drift Alert = disabled) and add failure rates for both sensing elements.

Example: 3144P SIS with dual 3-wire RTDs

Assuming that the 3144P SIS Temperature Transmitter is programmed to drive the output low on detected failure, the failure rate contribution for the 3-wire RTD in a low stress environment is:

- λ^{L} = 2 * ((2000) * (0.50 + 0.30)) = 3200 FIT
- λ^{DU} = 2 * ((2000) * (0.20)) = 800 FIT

When these failure rates are added to the failure rate of the 3144P SIS Temperature Transmitter, single RTD mode (see Table 5, first column), the total for the temperature sensor subsystem is:

- λ^{L} = 3200 + 331 = 3531 FIT
- λ^{H} = 28 FIT
- λ^{DU} = 800 + 39 = 839 FIT

Calculation 4

Dual Sensors configured, PV = Average and Drift Alert = alarm

To obtain the overall failure rates of the sensor assembly, use the dual mode failure rates for the 3144P SIS Temperature transmitter and add failure rates for both sensing elements. The sensing element failure rates should be adjusted to reflect the additional coverage on the drift failures (99%) provided by the Drift Alert.

Example: 3144P SIS with dual 3-wire RTDs

Assuming that the 3144P SIS Temperature Transmitter is programmed to drive the output low on detected failure, the failure rate contribution for the 3-wire RTD in a low stress environment is:

- $\lambda^{L} = 2 * ((2000 * (0.50 + 0.30 + 0.99\cdot0.2)) = 3992$ FIT
- $\lambda^{DU} = 2 * ((2000 * (0.01\cdot0.20)) = 8$ FIT

When these failure rates are added to the failure rate of the 3144P SIS Temperature Transmitter, dual RTD mode (see Table 5, second column), the total for the temperature sensor subsystem is:

- $\lambda^{L} = 3992 + 342 = 4334$ FIT
- $\lambda^{H} = 28$ FIT
- $\lambda^{DU} = 8 + 38 = 46$ FIT

Appendix C: Proof tests to reveal dangerous undetected faults

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

B.1 Proof test 1

Proof test 1 consists of an analog output Loop Test, as described in Table 14. This test will detect approximately 63% of possible DU failures in the transmitter and approximately 90% of the simple sensing element DU failures. This means a Proof Test Coverage of 72% for the overall sensor assembly, assuming a single 4-wire RTD is used.

Table 14 Steps for Proof Test 1

Step	Action
1.	Bypass the safety PLC or take other appropriate action to avoid a false trip
2.	Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value. This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.
3.	Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value. This tests for possible quiescent current related failures
4.	Use the HART communicator to view detailed device status to ensure no alarms or warnings are present in the transmitter
5.	Perform reasonability check on the sensor value(s) versus an independent estimate (i.e. from direct monitoring of BPCS value) to show current reading is good
6.	Restore the loop to full operation
7.	Remove the bypass from the safety PLC or otherwise restore normal operation

B.1 Proof test 2

The alternative proof test consists of the following steps, as described in Table 15. This test will detect approximately 96% of possible DU failures in the transmitter and approximately 99% of the simple sensing element DU failures. This results in a Proof Test Coverage of 97% for the overall sensor assembly, assuming a single 4-wire RTD is used.

Table 15 Steps for Proof Test 2

Step	Action
1.	Bypass the safety PLC or take other appropriate action to avoid a false trip
2.	Perform Proof Test 1
3.	Verify the measurement for two temperature points for Sensor 1. Verify the measurement for two temperature points for Sensor 2, if second sensor is present.
4.	Perform reasonability check of the housing temperature
5.	Restore the loop to full operation
6.	Remove the bypass from the safety PLC or otherwise restore normal operation

Appendix D: Common Cause for redundant transmitter configurations

A method for estimating the beta factor is provided in IEC 61508, part 6. This portion of the standard is only informative and other techniques may be used to estimate the beta factor. Based on the approach presented in IEC 61508 a series of questions are answered. Based on the total points scored for these questions, the beta factor number is determined from IEC61508-6 Table D.4.

Example – 2oo3 Temperature Transmitters

A design is being evaluated where three Rosemount 3144P SIS Temperature transmitters are chosen. The transmitters are connected to a logic solver programmed to detect over-range and under-range currents as a diagnostic alarm. The process is not shutdown when an alarm occurs on one transmitter. The logic solver has a two out of three (2oo3) function block that votes to trip when two of the three transmitters indicate the need for a trip. Following the questions from the sensor portion of Table D.1 of IEC 61508, Part 6, the following results are obtained.

Table 16 Example version of Table D.1, Part 6 IEC 61508

Item	X_{SF}	Y_{SF}	Example	Score
Are all signal cables for the channels routed separately at all positions?	1.0	2.0	Not guaranteed	0.0
If the sensors/final elements have dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?	2.5	1.5	Transmitters are separate	4.0
If the sensors/final elements have dedicated control electronics, is the electronics for each channel indoors and in separate cabinets?	2.5	0.5	Transmitters are in different housings	3.0
Do the devices employ different physical principles for the sensing elements for example, pressure and temperature, vane anemometer and Doppler transducer, etc.?	7.5		No – transmitters are identical	0.0
Do the devices employ different electrical principles/designs for example, digital and analogue, different manufacturer (not re-badged) or different technology?	5.5		No – transmitters are identical	0.0
Do the channels employ enhanced redundancy with MooN architecture, where N > M + 2?	2.0	0.5	No – 2oo3	0.0
Do the channels employ enhanced redundancy with MooN architecture, where N = M + 2?	1.0	0.5	No – 2oo3	0.0
Are separate test methods and people used for each channel during commissioning?	1.0	1.0	No - impractical	0.0
Is maintenance on each channel carried out by different people at different times?	2.5		No - impractical	0.0
Does cross-connection between channels preclude the exchange of any information other than that used for diagnostic testing or voting purposes?	0.5	0.5	No cross channel information between transmitters	1.0
Is the design based on techniques used in equipment that has been used successfully in the field for > 5 years?	1.0	1.0	3144P based on well proven design	2.0
Is there more than 5 years experience with the same hardware used in similar environments?	1.5	1.5	Extensive experience in process control	3.0
Are inputs and outputs protected from potential levels of over-voltage and over-current?	1.5	0.5	Transient voltage and current protection provided	2.0

Item	X_{SF}	Y_{SF}	Example	Score
Are all devices/components conservatively rated? (for example, by a factor of 2 or more)	2.0		Design has conservative rating factors proven by field reliability	2.0
Have the results of the failure modes and effects analysis or fault tree analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?		3.0	FMEDA done by third party – exida. No common cause issues	3.0
Were common cause failures considered in design reviews with the results fed back into the design? (Documentary evidence of the design review activity is required.)		3.0	Design review is part of the development process. Results are always fed back into the design	3.0
Are all field failures fully analyzed with feedback into the design? (Documentary evidence of the procedure is required.)	0.5	3.5	Field failure feedback procedure reviewed by third party – exida. Results are fed back into the design.	4.0
Is there a written system of work which will ensure that all component failures (or degradations) are detected, the root causes established and other similar items are inspected for similar potential causes of failure?	0.5	1.5	Proof test procedures are provided but they cannot ensure root cause failure analysis.	0.0
Are procedures in place to ensure that: maintenance (including adjustment or calibration) of any part of the independent channels is staggered, and, in addition to the manual checks carried out following maintenance, the diagnostic tests are allowed to run satisfactorily between the completion of maintenance on one channel and the start of maintenance on another?	2.0	1.0	Procedures are not sufficient to ensure staggered maintenance.	0.0
Do the documented maintenance procedures specify that all parts of redundant systems (for example, cables, etc.), intended to be independent of each other, must not be relocated?	0.5	0.5	MOC procedures require review of proposed changes, but relocation may inadvertently be done.	0.0
Is all maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair centre and have all the repaired items gone through a full pre-installation testing?	0.5	1.5	Repair is done by returning product to the factory, therefore this requirement is met.	2.0
Do the system diagnostic tests report failures to the level of a field-replaceable module?	1.0	1.0	Logic solver is programmed to detect current out of range and report the specific transmitter.	2.0
Have designers been trained (with training documentation) to understand the causes and consequences of common cause failures	2.0	3.0	Control system designers have not been trained.	0.0
Have maintainers been trained (with training documentation) to understand the causes and consequences of common cause failures	0.5	4.5	Maintenance personnel have not been trained.	0.0

Item	X_{SF}	Y_{SF}	Example	Score
Is personnel access limited (for example locked cabinets, inaccessible position)?	0.5	2.5	A tool is required to open the transmitter therefore this requirement is met.	3.0
Is the system likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?	3.0	1.0	Environmental conditions are checked at installation.	4.0
Are all signal and power cables separate at all positions?	2.0	1.0	No	0.0
Has a system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?	10.0	10.0	Rosemount has complete testing of all environmental stress variables and run-in during production testing.	20.0
Totals	23	37	S=X+Y	58

A score of 58 results in a beta factor of 5%. If the owner-operator of the plant would institute common cause training and more detailed maintenance procedures specifically oriented toward common cause defense, a score of greater than 70 could be obtained. Then the beta factor would be 2%.

Note that the diagnostic coverage for the transmitter is not being considered. Additional points can be obtained when diagnostics are taken into account. However this assumes that a shutdown occurs whenever any diagnostic alarm occurs. In the process industries this could even create dangerous conditions. Therefore the practice of automatic shutdown on a diagnostic fault is rarely implemented. IEC 61508, Part 6 has a specific note addressing this issue. The note states:

> *"NOTE 5 In the process industries, it is unlikely to be feasible to shut down the EUC when a fault is detected within the diagnostic test interval as described in table D.2. This methodology should not be interpreted as a requirement for process plants to be shut down when such faults are detected. However, if a shut down is not implemented, no reduction in the b-factor can be gained by the use of diagnostic tests for the programmable electronics. In some industries, a shut down may be feasible within the described time. In these cases, a non-zero value of Z may be used."*

In this example, automatic shutdown on diagnostic fault was not implemented so no credit for diagnostics was taken.