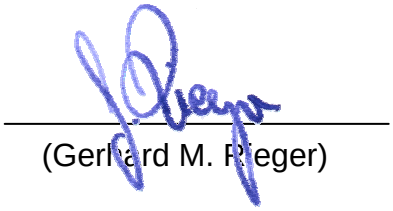
Certification Report
of the
3144P SIS Temperature Transmitter

Revision No.:	1.0
Date:	2004-10-26
Report Number:	701-063/2003T
Product:	3144P SIS Temperature Transmitter
Customer:	Rosemount Inc. 8200 Market Blvd. Chanhassen, MN 55317 USA
Order Number:	20624749
Inspection Authority:	RWTÜV Systems GmbH Safety Approval Service – SAS Hübnerstr. 3 86150 Augsburg Germany
Accredited Laboratory:	RWTÜV Systems GmbH Postfach 10 32 61 45032 Essen Germany
Responsible:	Author:  (Josef Neumann) Reviewer:  (Gerhard M. Rieger)

This document is only valid in it’s entirety and separation of any part is not allowed.

Content **Page**

1 Subject of certification

This report compiles the results of the assessment of the 3144P SIS Temperature Transmitter of Rosemount Inc. (thereafter known as Rosemount). Rosemount ordered the services of RWTÜV Systems GmbH (thereafter known as RWTÜV) to certify the 3144P SIS Temperature Transmitter because of its use in safety-relevant applications by the process industry (e.g. oil & gas and chemical industry) with the goal of achieving a successful approval of 3144P in the framework of the certification of safety-components.

The 3144P SIS Temperature Transmitter is to be certified for the T/C and RTD configurations in accordance with IEC 61508 for single use in Safety Integrity Level 2 (SIL 2) applications. The development process was certified in accordance with SIL 3 requirements allowing the use of dual redundant 3144P SIS Temperature Transmitters in SIL 3 applications.

The Rosemount 3144P SIS Temperature Transmitter is based upon the standard 3144P HART Temperature Transmitter which already has a documented history for the proven in use consideration under IEC 61508, the new industry standard for safety electronic systems.

2 Basis of certification

An effective assessment in order to meet all the requirements for a complete certification requires the following testing segments to be successfully completed:

- Safety system structure and SIRS
- Development process
- Hardware design
- Software design and implementation
- Proven in use documentation
- Safety verification steps and the validation tests
- Test specification

Including the following principal functional safety considerations:

- Hardware failure-behaviour
- Software failure-avoidance
- Probabilistic and Common Cause consideration
- Safety Manual

3 Standards

Because of the application area of the 3144P SIS Temperature Transmitter, the following standard is relevant:

Functional Safety	
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61508-1:1998	Part 1: General Requirements General definitions: Type B, Low Demand
IEC 61508-2:2000	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems, Required SIL 2
IEC 61508-3:1998	Part 3: Software requirements Required SIL 3

Quality-Management	
Laboratory-handbook SAS, version 1.0,	Laboratory-handbook of the lab (RWTÜV)

4 Definitions

FIT	Failure In Time ($1*10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
FSM	Functional Safety Management
HART	Highway Addressable Remote Transducer
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	Probability of Failure on Demand
PFDAVG	Average Probability of Failure on Demand
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SRS	Safety Requirements Specification
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
λ_{du}	Dangerous Undetected (DU) Failure Rate [1/h]

5 Overview about the system configuration

The 3144P SIS Temperature Transmitter is composed of several subassemblies which are already used in an existing product.

The basic architectural structure of the Rosemount 3144P SIS Temperature Transmitter is shown in Figure 1. The complete design of the 3144P SIS Temperature Transmitter is based on the existing 3144P HART Temperature Transmitter.

A thermo sensor, either a thermocouple or a RTD in a 2-wire, 3-wire, or 4-wire version, provides input to the transmitter. The thermo sensor signal is read by an A/D converter, controlled and read by the microprocessor through an isolation network. The microprocessor calculates the temperature, and the resulting scaled output is sent to a D/A converter, which is part of the MODAC ASIC. The loop control circuit averages the D/A converter's dynamic pulse width modulated output signal, and converts it to a 4 - 20 mA output current.

The 3144P SIS Temperature Transmitter has an intermittent sensor algorithm that have to be considered when doing process safety time calculations.

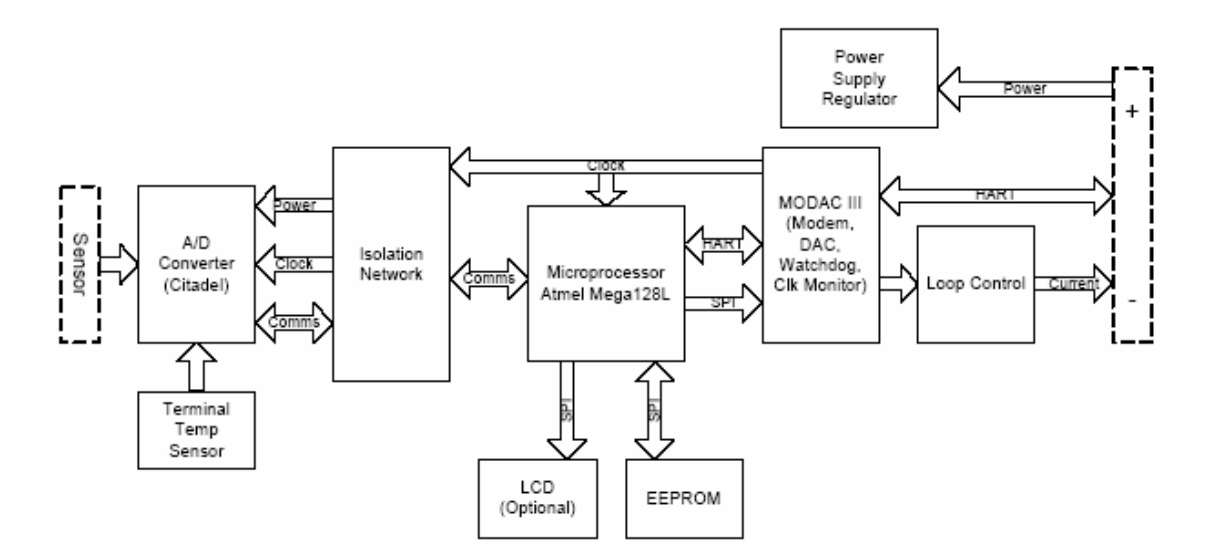


Figure 1: Block structure

A thermo sensor, either a thermocouple or a RTD in a 2-wire, 3-wire, or 4-wire version, provides input to the transmitter. The thermo sensor signal is read by the A/D converter, passed through an isolation network and then read by the micro-processor. The microprocessor calculates the output temperature and feeds the calculated result to a modem. From there the calculated result is send to the loop control circuit, a pulse width modulation circuit, which generates a dynamic signal that is averaged and converted into a 4 – 20 mA current.

The 3144P SIS Temperature Transmitter is classified as a Type B device according to IEC61508, having a hardware fault tolerance of 0. Combined with a temperature sensing device, the 3144P SIS Temperature Transmitter becomes a temperature sensor assembly. This is also indicated in Figure 2.

For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. The device can be equipped with or without display.

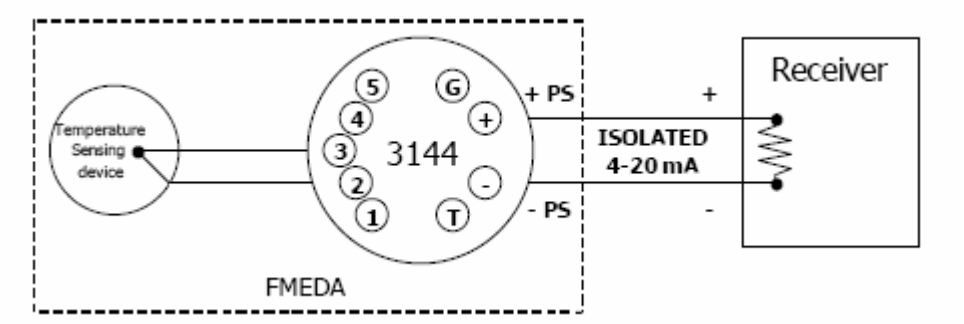


Figure 2: 3144P SIS Temperature Transmitter

The temperature sensing devices that can be connected to the 3144P SIS Temperature Transmitter are listed underneath.

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

The FMEDA has been performed for four different input sensor configurations of the 3144P SIS Temperature Transmitter, i.e. 2-, 3-, 4-wire RTD, and thermocouple. Estimates have been made of the temperature sensing device failure rates given the ability of the 3144P SIS Temperature Transmitter to detect several failure modes of the temperature sensing device.

The 3144P SIS Temperature Transmitter is intended for use as a temperature measurement component in a safety instrumented system. The following description shows the principal system aspects of the 3144P SIS Temperature Transmitter:

- Temperature transmitter coupled to a temperature sensor, which is coupled to the customer process for purposes of measuring temperature. This is represented by the hardware elements within the 'system'.
- Major elements of the transmitter consist of 3144P electronics module, and dual compartment housing assembly.
- Dual compartment housing contains transition board, filter assembly and terminal block, which provides customer sensor and loop wiring termination points. The optional transient protector may be added between the terminal block and the customer loop connections.
- Dual compartment housing contains safety module with Alarm and Security hardware adjustments. Adjustments are a user interaction point.
- Dual compartment housing contains optional LCD display if present. LCD Display is a user interaction point.
- Transmitter provides HART digital communication and 4-20 mA analog output allowing connection of Model 275, AMS, or SCS. These analog and digital connections are user interaction points.
- Only the 4-20mA analog output is safety rated.

6 Hardware and software identification

The following versions are considered for the certification:

- Schematic: 03144-2110, Rev AK, 2004-09-20
  03144-2108, Rev AG, 2003-07-01
- Hardware version: 1.0
- Software version: 5.2.x

7 Documentation

[M1] 3144P Safety Transmitter Safety Integrity Requirements Specification, Rev. B.2, 2004-09-22

[M2] Project Plan, Rev 0.2, 2004-09-09

[M3] 3144P Architecture, ROS 03/09-21 R002, Rev 2.0, 2004-02-25

[M4] System Test Plan for the 3144P, Rev B

[M5] System Test Objectives, Rev 0,2, 2004-09-09

[M6] Validation Test Specification and Plan, Version 0, Rev. 0.7, 2004-09-21

[M7] Validation Test Report, ROS 04/08-19 R002, Rev 1.0, 2004-10-07

[M8] Failure Modes, Effects and Diagnostic Analysis – FMEDA, 3144P HART Temperature Transmitter, ROS 01/06-01 R010, Version 2, Rev. 1.0, August 2003

[M9] Failure Modes, Effects and Diagnostic Analysis – FMEDA, 3144P SIS Temperature Transmitter, ROS 04/08-19 R003, Version 1, Rev. 2.0, 2004-10-25

[M10] Inspection Report, 3144P SIS Temperature Transmitter, 2004-09-20

[M11] Fault Injection Test Report (Regression Testing) for the 3144P SIS Temperature Transmitter, ROS 04/08-19 R001, V1.0, Rev 1.0, 2004-10-04

[M12] DOP416, DOP416 SIS Product Design and Development Process, Rev. E

[M13] DOP440, Engineering Change Order, Rev AD

[M14] 1110 Metrology, Rev W, Requirements for a calibration system to control test and measurement equipment

[M15] Project Coding Standard for the 3144P SIS Temp. Transmitter, Rev 1.1 2004-06-28

[M16] EDP 400-300 Configuration and Change Management Procedure, Rev B

[M17] EDP 400-500 Peer Review Procedure, Reb A.1

[M18] Proven in Use Assessment for 3144P Temperature Transmitter, ROS 03/09-21 R001, Rev 2.0, 2004-02-25

[M19] Proven in Use Assessment for CMX Tiny + RTOS for Atmel AVR micro-processors, ROS 02/11-07 R003, Rev 1.0, 2004-02-09

[M20] Proven in Use Assessment for IAR Compiler for Atmel AVR micro-processors, ROS 03/11-07 R002, Rev 1.0, 2004-02-03

[M21] Reference Manual 3144P, 00809-0100-4021, Rev DA

[M22] Product Data Sheet 3144P, 00813-0100-4021, Rev DA, July 2004

Documents of RWTÜV:

[M23] Assessment of the Functional Safety Management, V1.0, Visit 2003-09-16

[M24] Assessment of the Functional Safety Management, V1.0, Visit 2004-06-29

[M25] Architecture approval report of the 3144P Temperature Transmitter, V1.0, 2003-12-05

[M26] Review of the Requirement Specification of the 3144P Temp. transmitter V1.0, 2004-04-23

[M27] Fault Injection Test Report 3144P, Version 1.0, 2004-06-29

[M28] Protocol of the fault injection activities for the 3144P Temp. Transmitter, V1.0, 2004-06-29

[M29] Checklist according IEC 61508, V1.0, 2004-10-22

8 Assessment activities and results

8.1 Development Process

General aspects and scope:

The assessment of the development process has already been performed within the certification of the Rosemount 3051S Pressure Transmitter (see report 701-070/2002T, 2004-03-14). In that certification process a safety management audit has been performed to cover the relevant requirements of the IEC 61508, in respect of the fulfilment of the requirements to the safety quality procedures.
The scope of the Functional Safety Management Audit covers the specified Safety Lifecycle Phases of the IEC61508. The scope is as follows:

For design, developing, manufacturing and integration of microprocessor based safety transmitters.

For the Functional Safety Management Audit according to IEC 61508 it was essential that the functional safety management and the software development process are designed for the SIL 3 level to allow the set up of a redundant 3144P SIS Temperature Transmitter system in a SIL 3 environment. The FSM procedures are used to reduce the systematic failure rate.

Structuring of the development process:

The document DOP 416 describes the Rosemount development processes, procedures and work-instructions. The functional management system is based on the company management system which is already certified by RWTÜV. The aim of the assessment was to show that the defined procedures are not only defined but also used and lived in the project. Therefore interviews to the participants and reviews of documents (e.g. review reports) were performed. This should give the right overview to define whether the project specific management activities are sufficient for the actual assessment. For the Functional Safety Management Audit according to IEC 61508 it was essential that the functional safety management and the software development process are designed for the SIL 3 level to allow to set up a redundant 3144P Temperature Transmitter in a SIL 3 environment.

The Functional Safety Management Audit covered the following areas:

- Product marketing and safety policy
- Overall safety planning (regarding quality)
- Company FSM procedure
- Feedback control and improvement of safety processes
- Validation test planning
- Change and Configuration management
- Hardware design and development method
- Operation and maintenance method
- Software design and development method
- Requirement specifications
- Operation and modification method

An important part of the audit was to discuss safety aspects of the project with the participants and to ask for the relevant documents and the access to the relevant information. Also the specific knowledge about safety processes and internal review activities were reviewed. Actual documentation was partly reviewed and the statements of the participants were compared with the relevant parts of the documents.

Result:

The audits, interviews and document reviews performed at June 29, 2004 have shown that the Functional Safety Management System defined in the listed documents complies with the applicable sections of the IEC 61508.

No major findings were detected in the audit.

If changes to the Safety Management Systems are performed than RWTÜV – SAS must be informed.

8.2 System Architecture

The system documents have been reviewed to verify compliance of the system architecture with the standard listed in clause 3 "Standards".

Based on the set of requirements RWTÜV Safety Approval Service –SAS has evaluated whether the implemented fault detection and fault control measures which are defined for the 3144P SIS Temperature Transmitter were sufficient to meet the requirements. The system architecture was evaluated in regards to completeness and correctness against the Safety Requirements Specification and the System FMEDA. The system architecture has to be designed for a Type B subsystem according the IEC 61508-2 with a Safe Failure Fraction of 90% or higher.

The FMEDA verified the defined safe state of the 3144P SIS Temperature Transmitter in the event of possible malfunctions. Probable deviation from the specified function of the unit was also considered to be a malfunction.

Result:

The review from RWTÜV Safety Approval Service – SAS has shown that the system architecture of the 3144P SIS Temperature Transmitter is consistent against the Safety Requirements Specification. The specifications in the documentation are consistent and complete and clearly presented. The system concept with the chosen architecture design and the selected measures of fault detection and fault control is able to fulfil the Safety Integrity Level 2 with a Safe Failure Fraction of >90%.

8.3 Proven In Use

For a device to be considered proven-in-use the volume of operating experience needs to be considered. For the Rosemount 3144P HART Temperature Transmitter this information is obtained from the Operation Experience and Warranty Information.
The Rosemount 3144P HART Temperature Transmitter was first introduced in January 2002. In this time period there have been no significant revisions or changes to the design. The operating experience and warranty information indicates that the total number of shipped units during this time period is 52,658. For failure rates calculated on the basis of field returns only the hours recorded during the warranty period of the manufacturer are used, since this is the only time frame when failures can be expected to be reported. It must be assumed that all failures after the warranty period are not reported to the manufacturer.
Rosemount offers a 12-mounth warranty period from the date of installation or a 18-mounth warranty period from the date of shipment, whichever ends first. Volume of operating experience must be based on installation dates and not on shipment dates. Since installation dates are not available, it is assumed that the 3144P SIS Temperature Transmitters are installed 6 months after shipment. Using this assumptions and restrictions the number of operational hours is estimated to be:

Operation Hours = 188,518,488 hrs

The analysis is taking into account the medium complexity of the sub-system and the use in SIL 3 safety functions [M18][M19][M20].
In the calculation of the operation hours it is assumed that the units shipped include units up to a year before the field failure reporting hereby ensuring that all failures that occur to the included units are accounted for.

Result:

The documented operating hours are considered to be sufficient for the use at SIL 2 or SIL 3 applications, depending on redundancy and the calculation of the PDF and SFF and taking into account the medium complexity of the subsystem.

8.4 Hardware Design and 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.

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an extension of the FMEA. It combines standard FMEA techniques with additional analysis to identify online diagnostic techniques and the failure modes relevant to safety system design. It is a technique recommended to generate failure rates for each important category (detected, dangerous undetected, fail high, fail low, annunciation) in the safety model.

The following tables show the failure rates resulted from the Rosemount 3144P SIS Temperature Transmitter FMEDA for the T/C and RTD configuration [M9].

Table 1 Failure rates 3144P SIS Temperature Transmitter (T/C configuration)

Failure category	**Failure rate (in FITs)**			
	Single TC mode		**Dual TC mode**	
Fail High (detected by the logic solver		28		28
Fail Low (detected by the logic solver		328		338
- Fail detected (internal diag.)	303		313	
- Fail low (inherently)	25		25	
Fail Dangerous Undetected		40		40
No Effect		100		104
Annunciation Undetected		5		5

Table 2 Failure rates 3144P SIS Temperature Transmitter (RTD configuration)

Failure category	**Failure rate (in FITs)**			
	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		320		331
- Fail detected (internal diag.)	295		306	
- Fail low (inherently)	25		25	
Fail Dangerous Undetected		38		37
No Effect		104		108
Annunciation Undetected		5		5

Safe Failure Fraction

According to IEC 61508, the Safe Failure Fraction (SFF) of the 3144P SIS Temperature Transmitter must 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. Note that according to IEC61508 definitions the no effect failures need to be considered in the Safe Failure Fraction calculation as safe failures. The Safe Failure Fractions that result for the 3144P SIS Temperature Transmitter are listed in the following table:

Table 3 Safe Failure Fraction of the 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 the 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. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

The expected lifetime of the Rosemount 3144P SIS Temperature Transmitter is 50 years. The reliability data listed the FMEDA report is only valid for this period. The failure rates of the Rosemount 3144P SIS Temperature Transmitter may increase sometime after this period.

Result:

With these results from the calculation it can be shown, that the 3144P SIS Temperature Transmitter is able to fulfil SIL 2 for the hardware design in a single configuration.

8.5 Software Design and Implementation

The software of the 3144P SIS Temperature Transmitter is based on the 3144P HART Temperature Transmitter and is considered to be proven in use according to the calculated operating hours.
The internal test routines and detection of corrupted RAM areas, reach a sufficient safe failure fraction > 90%.

Result:
The software design and Implementation is compliant to IEC 61508 part 3.

8.6 Verification and Validation

The test specification defined in the Validation Test Specification and Plan from the manufacturer has been reviewed. The list of validation tests are referenced to the Requirement Specification. The review has shown that the requirements are covered by the validation plan.
After the execution of the validation tests by the manufacturer, the test results have been reviewed by RWTÜV. The test results are also referenced to the Design Specification.
Additional sample testing of the 3144P SIS Temperature Transmitter have been defined by RWTÜV and a separate list of test items has been generated. The defined of tests have been executed by the manufacturer by RWTÜV. The definition and results are documented in the 3144P Fault Injection Test Report.

Result:
The review of the Validation Test Specification, the Validation Test Report from the manufacturer and the performing of the sample tests by RWTÜV have shown, that the defined tests are consistent to the Design Specification and the tested results can be compared to the tests of the manufacturer. The test definitions are sufficient to prove compliance with the standard.

8.7 Safety Manual

The safety manual is included in the "3144P Quick Installation Guide" and has been reviewed to fulfil the requirements of the considered standard. Specifically the section about Proof Testing has been checked according the defined measures to be followed up by the end user to be compliant with the considered standard according failure detection which are not covered by the diagnostic of the transmitter.

Result:

The review has shown that the safety manual meets the requirement of the considered standard. Detailed descriptions are included for the end user to install, operate and maintain the transmitter in the required safety level.

9 Summary

The assessment of the 3144P SIS Temperature Transmitter has shown that for the transmitter together with the T/C and RTD sensors as well as the system design, the safety functional management and the system structure are compliant with the IEC 61508, SIL 2 under consideration of the proven in use of the transmitter and the additional measures implemented to the transmitter. The defined development process of the software for modifications together with the proven in use consideration is in accordance with SIL 3 requirements allowing the use of dual redundant 3144P SIS Temperature Transmitter in SIL 3 applications.

The validation and testing activities have shown the compliances between the realised transmitter implementation and the safety requirements specification.

The actual version of the Safety Manual (Product Data Sheet 3144P) must be considered for the use in safety relevant applications.