Technical Report
Proven In Use – SITRANS P500

Client: Siemens AG, Industry Sector, Industry Automation Division, Sensors and Communication, PD PA PI R&D PM CRT
Oestliche Rheinbrueckenstr. 50
76187 Karlsruhe, Germany
Products: SITRANS P500
Number: 4.92.100
Revision: 1.2
Date: 2014-10-23

Author(s): W. Velten-Philipp

Risknowlogy Germany GmbH
Unterreut 6
76135 Karlsruhe
Germany
www.risknowlogy.com

Revisions

Revision	Date	Who	Description
0	2013-09-16	WVP	draft
1	2013-09-16	WVP	release
1.1	2014-07-14	WVP	Minor software modification
1.2	2014-10-23	WVP	Minor software modification

Table of Contents

List of Tables

List of Figures

Terms and Definitions

Term	Definition
Dangerous failure	An internal failure that prevents the product from carrying out its safety function upon demand. See also safe failure
Detected failure	An internal failure that is detected by built-in diagnostics. Because of the diagnostics the product can act upon the failure. See also undetected failure
FMEDA	Failure mode, effects and diagnostics analysis
Functional safety	A product is functionally safe if random, systematic and common cause failures do not lead to malfunctioning of the system and do not result in injury or death of humans, spills to the environment, or loss of equipment or production
Hardware fault tolerance	Hardware fault tolerance indicates the number of failures the product or subsystem can withstand without losing the safety function
HFT	See hardware fault tolerance
PFD	The probability that the safety function has failed upon demand
PFS	The probability that the safety function causes a spurious trip of the process
Safe failure	An internal failure where a product carries out its safety function without a demand from the process. This failure can lead to a spurious trip. See also dangerous failure
Safety function	Function implemented in the product required to achieve a safe state of the process
SFF	Safe failure fraction
SIL	Safety Integrity Level
STL	Spurious Trip Level®
Type	The complexity of a product is designated by Type A or Type B. See IEC 61508, part 2, clause 7.4.3.1.2 and 7.4.3.1.3
Undetected failure	An internal failure that is not detected by built-in diagnostics. See also detected failure

1 Introduction

1.1 Objective

The objective of this report is to document the proven in use study carried out for the Siemens SITRANS P500 pressure transmitter. The purpose of the proven in use study is to demonstrate that the device is suitable to be used in safety instrumented functions up to SIL 2 according to IEC 61511 and IEC 61508 [1,2].

Note: According to IEC 61511, 11.4.4 SIL3 is possible in 1oo2 configuration in conjunction with prior use experience of the instrument user.

1.2 About Siemens

Siemens offers a comprehensive range of products and systems for process instrumentation and process analytics for non safety and safety related applications.

The process instrumentation portfolio covers positioners, process instruments for pressure, temperature, flow and level measurement. Products for process analytics include continuous gas analyzers for stand-alone and system solutions as well as process gas chromatographs.

1.3 About Risknowlogy

Risknowlogy is an international operating company that offers services, consulting, certification and training in the field of risk, reliability and safety. Risknowlogy was established in 2002 and has offices in Switzerland, Argentinia, Columbia, Germany, The Netherlands and United Arab Emirates. We consider the world as our work area and each location has obliged to maintain the same quality standards, rules, and business practices.

The headquarters of the Risknowlogy Corporation is located in Switzerland. Here we perform certification, business development, market our products and services, create new products and services, train our employees and service any country in the world that is not serviced by a local organization.

2 Product Description

2.1 Introduction

The product subject to the proven in use analysis is the SITRANS P500 pressure transmitter.

The product is shown in Figure 1.

Figure 1 – SITRANS P500

The functional safety properties according to IEC 61508 are:

- Safety function:
  Measurement of differential, absolute, relative pressure, level and flow within the specified safety accuracy of 1.1% from full span.
- The safety function response time is 2s.
- This is a type B device with hardware fault tolerance 0.
- The operation mode is low demand mode.

The conditions of use and constraints are described by the safety manual [8].

The end user is responsible for the validation of the safety function.

The suitable SITRANS P500 types are:

7MF54*3-****0	Differential Pressure Transmitter, HART
7MF56*3-****0-****	Level Transmitter, HART

*: Wildcard for different process connectors and other properties.

Hardware Version: 11.01.01

Software Version: 35.03.00

3 Proven In Use Demonstration

3.1 Restricted Functionality

The purpose of the transmitter is to measure the pressure and to transmit this pressure as a 4-20mA signal. The functionality is restricted to pressure related measurements. Possible configurations are related to process parameters. Access to the configuration is protected.

3.2 Conditions Of Use

The instrument considered for proven in use have been used in widely in the process industry in different operating environments [5]. These include more than 10 typical industrial process environments.

3.3 Field Data

Siemens collected field data for the instruments since 2011 [5]. From the operating hours of each instrument 3 month have been taken into account to exclude non-operating hours (e.g. from storage times, non-operation, etc). The typical operating time in the process industry is assumed 24 hours per day.

Siemens has compiled customer feedback and repair data [5]. The data demonstrates that during the time under consideration no dangerous failures have occurred, see Table 1.

Table 1 – Operating hours and failures

Type	Operating hours	Safe Failures	Dangerous Failures
SITRANS P500	4 903 758 h	4	0

3.4 Software and Modifications

During the time span used for the proven in use demonstration the products were subject to modifications.

The modifications were related to additional measurement ranges and are without influence to the proven in use properties of the product [10, 12].

Current firmware version is 35.03.00, hardware version is 11.01.01.

The modification from 35.02.01 to 35.03.00 is described by impact analyses [10, 12]. The modification scope is limited and minor and was related to improvement of diagnostic functions and interfaces. Each modification was subject to testing [11, 12].

3.5 Reliability analysis (FMEDA)

Siemens has carried out a qualitative and quantitative reliability study in line with the requirements of the IEC 61508 [1] standard. The reliability study consists of a failure modes and effects analyses (FMEDA) [6]. Table 2 presents a summary of the reliability data derived

from the FMEDA and the failure rates calculated from the field data taking a confidence interval of 90% into account.

Figure 2 shows the PFD and PFDavg curve (20 years).

The FMEDA analysis, which represents design expectations, corresponds with the data from the proven in use data, which represents operational experience.

Table 2 – Functional safety data for SITRANS P500

Properties	FMEDA	Proven In Use	90% Confidence (upper limit)
Type	B		
Safe failure rate	430.9	815.7	1867
Safe detected failure rate	24.2	n.a.	n.a
Safe undetected failure rate	406.7	n.a.	n.a
Dangerous failure rate	631	0	610.9
Dangerous detected failure rate	529	n.a.	n.a
Dangerous undetected failure rate	102	n.a.	n.a
DC	83.8%	n.a.	n.a
Safe failure fraction	90.4%	n.a.	n.a

Notes:

- Failure rates in FIT [10^{-9} 1/h]
- Confidence interval according to IEC 61508 route 2_H

Table 3 – PFDavg calculation results (1oo1)

Years	1	5	10
PFDavg	4.44E-4	2.21E-3	4.4E-3
% SIL 2	4.44%	22.1%	44%
PFSavg	1.88E-3	---	---

MTTR 8h

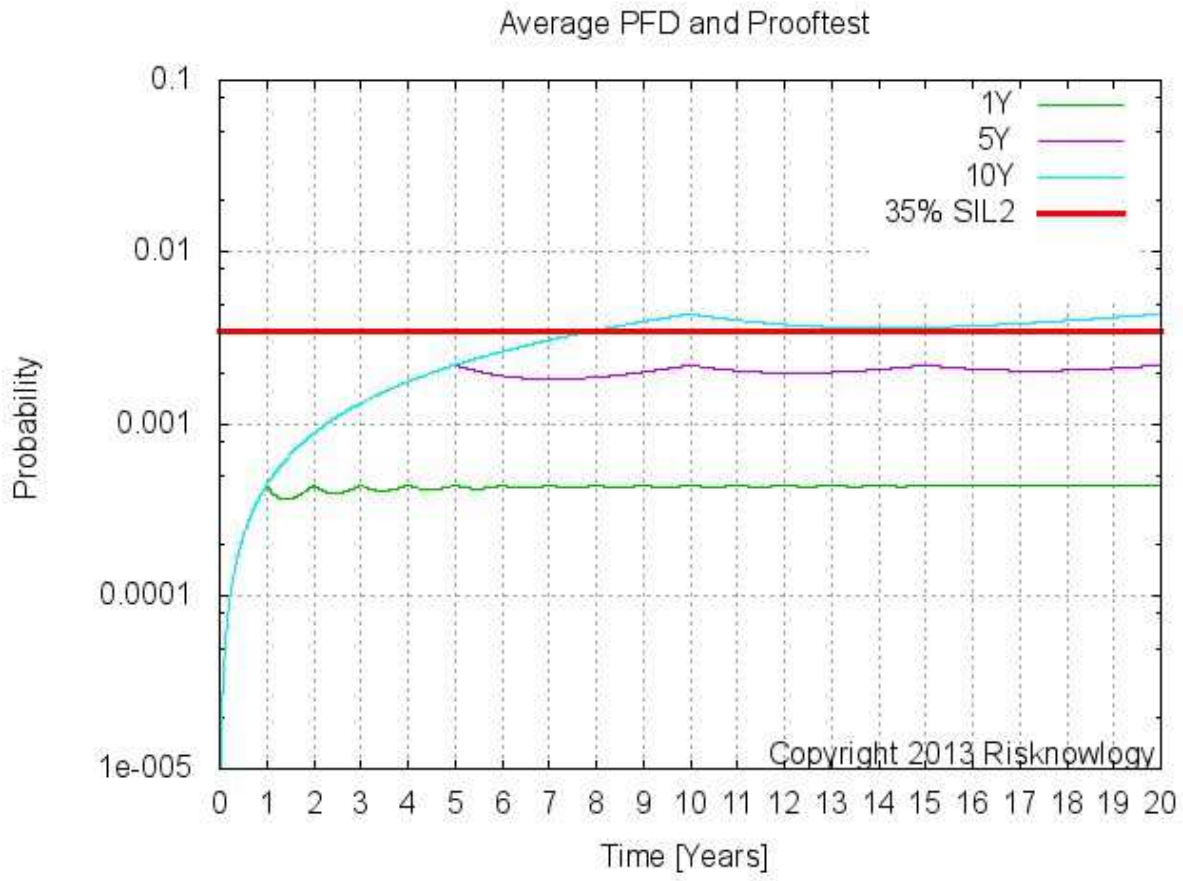

Figure 2 – PFDavg results

3.6 EMC, Basic safety and environmental testing

The product complies [9] to

- EMC directive 2004/108/EC
- ATEX directive 94/9/EC

4 User Documentation

The safety manual [8] provided by Siemens provides all necessary information for use of the product. The manual was reviewed without any objections.

5 Conclusions

The proven in use analysis demonstrates that the specified safety function of SITRANS P500 is suitable for SIL 2 safety properties according to IEC 61508, route $2_{H,}$ 2_S and IEC 61511.

6 References

The following references have been used during the project:

1. IEC 61508: 2010
   Functional Safety of Electrical, Electronic, Programmable Electronic Safety Related Systems
2. IEC 61511: 2003
   Functional safety: Safety instrumented systems for the process industry sector
3. SN 29000, Failure Rates of Components, 2004
4. 001_SITRANS_P500_2013_08_15
5. 102_Stückzahl_P500_201300422
   103_SITRANS_P500_Einsatzgebiete_V1_0
   105_Praesentation Pilotkunden
6. 301_P500_Gerät_akt_2013_08_27
7. Schematics, Drawings
   302_Anschlusselekt_a5e01360466b-02.pdf
   303_Applikation_A5E01359820B-09.pdf
   304_Messzelle_A5E01360457B-06.pdf
   305_FMEDA_Darstellung_2008_10_22.ppt
   306_Messzelle_TechZeich_A5E02189134d-01.pdf
   307_Application_BOM_A5E01359820-09.pdf
   308_Messzelle_BOM_A5E01360457-06.pdf
   309_Anschlusselekt_BOM_A5E01360466-02.pdf
8. Manual, Safetymanual: 501_A5E02344527-07de_P500HART_Ex_OI
9. EMC, Environmental and basic safety
   402_TYPPRÜFPROGRAMM DRUCKMESSUMFORMER Version 10_2010.pdf
   407_cert_Sitr_P500_EC_EMC_ATEX_7MF5xx_de_en_A5E02607915_02.pdf
10. Impact Analyses
    601_Changelog_neue_Messbereiche.doc
    602_Impact_Analysis_neue_Messbereiche.xls
    605_Changelog_P500_SIL_Measure.doc
    606_Impactanalyse FW-Änderung Messzellen uC.doc
    Impactanalyse FW-Änderung ADC_Ready, 2014-06-25
11. P500_FW35.02.02_Integrationtest_Plan_Spec_Report, 2014-07-14
    TestReport_FW_P500_HART_V35.02.02, A5E34584328/001, 2014-07-09
12. Änderung_Beschreibung_FW35_03_00
    PIA-Impactanalysis FW35.03.00
    PIA-Impactanalysis FW-Änderung COM-µC
    Certificate_FW_P500_HART_V35.03.00
    TestReport_FW_P500_HART_V35.03.00