Certification Report of the SmartLine ST 700 HART Pressure Transmitter

Revision No.:	2.0
Date:	2013-Feb-22
Report Number:	SEBS-A.153337/12TB
Product:	SmartLine ST 700 HART Pressure Transmitter
Customer:	Honeywell International Inc. Honeywell Field Products 512 Virginia, Dr. Fort Washington, PA 19034, USA
Order Number:	G.SEB.BS.02.006.08.031
Authority:	TÜV NORD Systems GmbH & Co. KG Functional Safety Halderstr. 27 86150 Augsburg / Germany
Author:	Josef Neumann
Review:	Bianca Pfuff

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

Content **Page**

History:

Version	Date	Author	Changes
V0.1	2013-01-10	J. Neumann	Draft1
V1.0	2013-01-21	J. Neumann	First Issue
V2.0	2013-02-22	J. Neumann	Optional Remote Diaphragm Seals / Flange Mounts added

1 Subject of certification

This report compiles the results of the assessment of the SmartLine ST 700 HART Pressure Transmitter (thereafter known as SmartLine ST 700) of Honeywell International Inc. The services of TÜV NORD Systems GmbH & Co. KG (thereafter known has TÜV NORD Systems) has been ordered by Honeywell International Inc. to certify the SmartLine ST 700 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 SmartLine ST 700 in the framework of the certification of safety-components.

The SmartLine ST 700 is to be certified in accordance with IEC 61508 for single use in Safety Integrity Level 2 (SIL 2) applications. The development and software process is to be certified in accordance with SIL 3 requirements allowing the use of the dual redundant SmartLine ST 700 in SIL 3 applications.

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

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:

- Functional Safety Management (FSM)
- Development process
- Architecture
- Safety system structure
- Hardware design
- Software design and implementation
- Verification and Validation
- Test specification

Including the following principal functional safety considerations:

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

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

3 Standards

Because of the application area of the SmartLine ST 700, the following standard is relevant:

Functional Safety	
IEC 61508:2010 Ed. 2	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61508-1	Part 1: General Requirements General definitions: Type B, Low Demand
IEC 61508-2	Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems, Required SIL 2
IEC 61508-3	Part 3: Software requirements Required SIL 3

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

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]

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

5 Overview about the system configuration

The SmartLine ST 700 is a smart device with two-wire 4-20mA HART interface. It contains self diagnostic and can be programmed to send its output to a specific failure state, either high or low upon internal detection of a failure. The product has a modular design with a common sensor board, a HART Communication board and a Termination board. The SmartLine ST 700 supports an optional local display which is considered to be non-interfering.

For safety instrumented systems using the HART version it is assumed that the 4-20mA output is used as the primary safety variable. Although the SmartLine ST 700 series is available with several different output options, no other output variants are covered by this report.

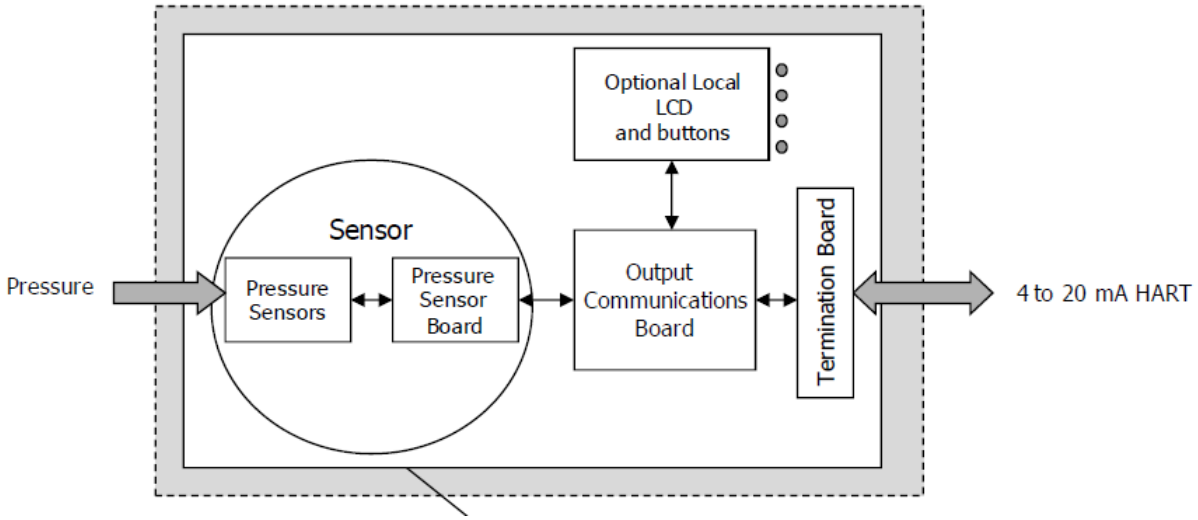

Figure 1: SmartLine ST 700 Block Diagram

The transmitter can be connected to the process using impulses lines, depending on the application.

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

5.1 Primary Safety Functions

The HONEYWELL SmartLine ST 700 measures the (pressure gauge, differential, absolute) of a process and reports the measurement within a safety accuracy of 2%.

5.2 Secondary Safety Functions

The HONEYWELL SmartLine ST 700 performs automatic diagnostics to detect internal failures and reports these failures via out of band signals on the 4 – 20 mA output. The transmitter needs a power cycle for recovery from this condition.

5.3 Logic Solver Inputs

The logic solver must be configured so that the engineering range in the transmitter matches the expected range of the logic solver.

To take advantage of the internal diagnostics in the SmartLine ST 700, the logic solver must be configured to annunciate an out of band current reading (greater than 20.8mA. or less than 3.8mA.) in standard instrument or (greater than 21.0mA. or less than 3.6 mA.) with Namur option as a diagnostic fault. The logic solver configuration must consider the slew time of the current signal and ensure that filtering is used to prevent a false diagnostic failure annunciation.

5.4 Optional Remote Diaphragm Seals / Flange Mounts

The SmartLine ST 700 Pressure Transmitter series is available with several configurations of optional Remote Seals and Flange Mounts that can be used to protect the device against potentially harmful process fluids or conditions, or for direct mounting to a vessel. These factory installed Remote Seals and Flange Mounts are covered in this assessment.

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

6 Hardware and software identification

The following versions are considered for the certification:

Hardware:

- Sensor Assy 50053143 – Rev C
- HART/DE Comm Assy 50050919 – Rev C
- HART/DE TB Assy 500055716 – Rev C

Software/Firmware:

- Sensor board: v1.000000
- Comm board: v1.020000

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

7 Documentation

The evaluation is based on the following documents of the SmartLine ST 700:

[D1] ST 700 AP, GP, DP Transmitter R170 Project Requirements

[D2] PAR Tracking User Guide

[D3] Management Review Process

[D4] Program Management Plan

[D5] HPS Global Quality Manual

[D6] ISO 9000 Certificate

[D7] Customer Notification Process

[D8] Quality Link proactive field action message

[D9] Return Goods Authorization (RGA) Procedure

[D10] Coding Standards for Embedded C

[D11] HPS GTS Escalation Process

[D12] Part Qualification Procedure

[D13] Manufacturing Qualification Procedure

[D14] Non-Conforming Reporting Procedure

[D15] Corrective Action Procedure

[D16] Corrective Action Procedure Aux

[D17] Test Equipment Master Cal List

[D18] GTS Escalation Flow

[D19] ST6000 r100 Functional Safety Management Plan

[D20] SIL Overview slides

[D21] exida Configuration Management Checklist

[D22] exida Documentation Checklist

[D23] exida Software Tool Checklist

[D24] exida Tool Validation Checklists

[D25] Configuration and Change Management Plan

[D26] HPS Technology Backup Policy

[D27] HFS New Product Development & Introduction Process

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

[D28] New Product Development Functional Process map

[D29] PWA Design Process Map

[D30] Team Competency Summary

[D31] HIP process overview

[D32] NPI Stage Gate Review Checklist

[D33] Solutions Council Review example

[D34] NPI Stage Gate Review Support

[D35] IEC 61508 Assessment Action Item List

[D36] PROGRAMMABLE DEVICE (PD) PROCESS Flowchart

[D37] exida FSM Planning Phase Verification Checklist

[D38] ST 800 SIL Requirements

[D39] exida SRS Document Checklist

[D40] Marketing Requirements Document

[D41] Product Requirements Specification Document

[D42] ST800 Solution Requirements Spec

[D43] Safety Validation Test Plan

[D44] SIL Requirements Traceability

[D45] System Test plan review

[D46] exida Safety Validation Test Plan Checklist

[D47] HART SW System Test Plan

[D48] HART SW System Test Cases

[D49] Typhoon Test plan- high level definition phase

[D50] ST 6000 Foundation Fieldbus/PROFIBUS-PA Communication Board Hardware Maintenance Document

[D51] ST6000 HART-DE Communication Board Hardware Maintenance Doc.

[D52] Typhoon protocol to exchange data between the various Typhoon PWAs

[D53] TYPHOON TERMINAL BLOCK MODULE DESIGN REVIEW

[D54] InterProcessor Communication Protocol Review

[D55] exida Integration Test Plan Checklist

[D56] Architecture and Development Process Review

[D57] TYPHOON Pressure Transmitter SIL Review

[D58] ST 6000 CM360 Pressure Sensor Board Hardware Maintenance Document

[D59] Schematics - combined files

[D60] exida Fault Injection Checklist

[D61] exida HW Fault Injection Test Verification Checklist

[D62] BOM - combined files

[D63] De-rating Analysis

[D64] QA Reliability Plan

[D65] Fault Injection Test Plan

[D66] ST6000 Terminal Block Hardware Maintenance Document

[D67] ST800 HART Terminal Board test results

[D68] ST800 HART HW test plan and results

[D69] ST800 Sensor HW unit test plan

[D70] ST800 HART HW architecture

[D71] ST800 Sensor HW architecture

[D72] ST800 Terminal Board HW architecture

[D73] ST800 Term Bd test plan

[D74] exida Hardware Development Phase Verification Checklist

[D75] ST 6000 Sensor Firmware Maintenance Document

[D76] Typhoon ST6000 (Foundation Fieldbus) Comm SW Maint Doc

[D77] ST6000 Smart Meter Software Maintenance Document

[D78] ST 6000 HART-DE Communication Board SW Maint Doc

[D79] ST800 Sensor SW Criticality Analysis

[D80] ST800 HART SW Criticality Analysis

[D81] ST800 HART stack and interrupt design

[D82] ST800 HART design review

[D83] ST800 SW architecture for HART board- HLD

[D84] ST800 Software architecture for sensor board- HLD

[D85] exida Software Architecture and Design Phase Checklist

[D86] IEC 61508 SIL3 Tables not covered in FSM Plan

[D87] Tools Evaluation and Justification

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

[D88] ClearCase Issue Resolutions

[D89] Tool Justification Report

[D90] Test Witnessing - HART board

[D91] Test Witnessing - Sensor board

[D92] Example of Field Issues for testing

[D93] Sensor Complexity Metric and Criticality Analysis

[D94] PC Lint Support - sensor

[D95] PC Lint Support - HART board

[D96] Unit Test Records - sensor

[D97] ST800 automated sensor regression test script results

[D98] ST800 sensor automated system testsets

[D99] boundary & equivalence class test examples

[D100] Module ST6KMeasure.c test support for D92b

[D101] Automated test design for HART

[D102] Automated test scripts for HART

[D103] Automated test results for HART

[D104] Code Review example - HART

[D105] Code Review example - Sensor

[D106] Code Review example - data hiding

[D107] ST800 Sensor Unit Test Plan (big file)

[D108] ST800 Sensor Unit Test Plan (part 2)

[D109] ST800 HART board Unit Test Plan for SIL

[D110] ST800 HART board Unit Test Cases and Results for SIL

[D111] ST800 HART unit test, non-SIL, pt1

[D112] ST800 HART unit test, non-SIL, pt2

[D113] ST800 HART unit test results

[D114] exida SW Implementation Phase Verification Checklist

[D115] exida Integration Test Execution Phase Checklist

[D116] EMC Test Results

[D117] Smart Pressure Transmitter Environmental Test Plan.

[D118] Validation Test Results (Performance)

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

[D119] Performance Validation Test Results (meterbody file)

[D120] Fault Injection Test Results

[D121] FIT witnessing

[D122] ST800 HART sw system test results

[D123] ST800 HART HW Phys Layer test results

[D124] HART system test results (updated)

[D125] HART system test evaluation

[D126] Sensor system test set summary

[D127] exida Functional Safety Assessment Phase Verification Checklist

[D128] Functional Safety Assessment Plan - FSA Plan

[D129] ST800 Safety Manual

[D130] Safety Manual review

[D131] Proof test verification

[D132] ST800 HART SW Release Construction

[D133] ST800 User Manual

[D134] SHA-1 Hash Signature- Sensor

[D135] SHA-1 Hash Signature- HART

[D136] Failure Modes, Effects and Diagnostics Analysis (FMEDA) Report

[D137] exida FMEDA Document Checklist

[D138] Change Control Process

[D139] HW/Elec Change Process Map

[D140] PAR Change Report summary

[D141] HON Safety Impact Analysis Form

[D142] exida Modification Phase Verification Checklist

Documentation from the Auditor:

[D143] SEBS-A 20120518.091351_V1 0Quot_Honeywell_ST800.pdf

[D144] Fault Injection Tests ST800 Pressure Transmitter V1.0

[D145] TUVNORD_review_FMEDA_ST800_V3.0.doc

[D146] TUVNORD_Review_Honeywell_ST800_v0.1.doc

[D147] CL_IEC61508_V1_0_Honeywell_ST800_V1.0

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

8 Assessment activities and results

8.1 Development Process

General aspects and scope:

In this step of assessment, a safety management audit has been performed to cover the relevant requirements of the IEC 61508, in respect of the fulfillment of the requirements to the safety quality procedures.

The scope of the Functional Safety Management Audit covers the specified Safety Lifecycle Phases of the IEC 61508. The scope for Honeywell International Inc. is as follows:

For design, developing, manufacturing and integration of microprocessor based 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 SmartLine ST 700 system in a SIL 3 environment. The FSM procedures are used to reduce the systematic failure rate. Honeywell International Inc. has created the following documents to define the FSM activities:

- HPS Global Quality Manual [D5]
- Program Management Plan [D4]
- Functional Safety Management Plan [D19]
- PWA Design Process Map [D29]
- HFS New Product Development & Introduction Process [D27]
- Configuration and Change Management Plan [D25]
- HIP process overview [D31]

Within the project all safety relevant definitions are defined by the Functional Safety Management and the normative requirements.

Structuring of the development process

The documents [D1] to [D37] describe the Honeywell International Inc. development processes, procedures and work-instructions. TÜV NORD Systems visited the Honeywell International Inc. development site as an external assessment department, toured the facilities and interviewed the Safety Design Team in order to understand all the relevant corporate procedures. They then extracted the most important functional safety management requirements from the standards and prepared documents indicating needed enhancements of the standard processes. TÜV NORD Systems has reviewed this document to discuss the overall FSM requirement activities for the project with Honeywell International Inc. TÜV NORD Systems has than discussed the relevant items with Honeywell International Inc. and reviewed the documents for the safety aspects of the system. Honeywell International Inc. is covering the following areas:

- Functional Safety Management
- Quality Management System
- Development of Safety Sub-Systems (Realization)
- Verification & Validation activities (Testing)

The focus of the interview with Honeywell International Inc. was to demonstrate compliance with the appropriate sections of the IEC 61508 standard. The following sections were considered:

- Specific Objectives for Functional Safety
- Change Management (Modification Process)
- Maintenance

The reviews with Honeywell International Inc. were related to the following areas:

- Safety Requirement specification
- Safety Architectural Constrains

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

- Safety Hardware Requirements
- Safety Software Requirements
- Verification & Validation of Safety Products
- Safety Manual

It was essential for the audit to discuss the safety aspects of the project with the participants and to ask for the relevant documents and to access all relevant information. Actual documentation from the SmartLine ST 700 project was partly reviewed and the statements of the participants were compared with the relevant parts of the documents.

Verification & Validation activities (Testing)

For verification & validation the independent test engineers are responsible for all activities within this segment. The definitions out of the tables of the standard are defined in [D86] to [D93]. They create the test specifications for specific projects used by the development engineers. The functional tests and integration and validation testing was done by independent test engineers. The test engineers must have specific knowledge about safety functions of the specific project. Internal training is therefore an important method to improve the knowledge of the test engineers. This could be proved by interviews and with reviews of examples of the corresponding documents.

Result

The document reviews have shown that the Functional Safety Management System, defined in the documents [D1] to [D37] 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 TÜV NORD Systems must be informed.

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

8.2 System Architecture

The system documents [D38] to [D49] have been reviewed to verify compliance of the system architecture with the standard listed in clause 3 "Standards".

Based on the set of requirements TÜV NORD Systems has evaluated whether the implemented fault detection and fault control measures which are defined for the SmartLine ST 700 were sufficient to meet the requirements. The system architecture was evaluated in regards to completeness and correctness against the hardware and software requirements specification [D38]. The system architecture have 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 SmartLine ST 700 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 TÜV NORD Systems has shown that the system architecture of the SmartLine ST 700 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 fulfill the Safety Integrity Level 2 with a Safe Failure Fraction of >90%.

8.3 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 assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the SmartLine ST 700:

- Only a single component failure will fail the entire SmartLine ST 700
- 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 stress levels are average for an industrial environment and can be compared to the exida Profile 2 with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the online diagnostics
- 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.
- Materials are compatible with process conditions
- The device is installed per manufacturer's instructions
- The Transmitter is generally applied in relatively clean gas or liquid, therefore no severe service has been considered in the analysis of the base Transmitter.
- External power supply failure rates are not included
- Worst-case internal fault detection time is 9 minutes

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

The following tables show the failure rates resulted from the SmartLine ST 700 FMEDA [D136].

Table 1 and Table 2 list the failure rates for the SmartLine ST 700. These failure rates do not include failure of the sensing devices.

Failure category	Failure rate (in FIT)	
Fail Safe Undetected		174.3
Fail Dangerous Detected		222.7
- Fail Detected (detected by internal diagnostics)	153.3	
- Fail High (detected by the logic solver)	26.7	
- Fail Low (detected by the logic solver)	42.8	
Fail Dangerous Undetected		43.9
No Effect		102.4
Annunciation Undetected		1.4
External Leakage		22.5

Table 1 Failure rates SmartLine ST 700

The failure rates that are derived from the FMEDA for the SmartLine ST 700 are in a format different from the IEC 61508 format. Table 2 lists the failure rates for SmartLine ST 700 according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents.

It is assumed that the probability model will correctly account for the Annunciation Undetected failures. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected according to IEC 61508 (worst-case assumption). 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.

According to IEC 61508, also the Safe Failure Fraction (SFF) of the SmartLine ST 700 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. This is reflected in the following formula for SFF:

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

Where $\lambda_{total} = \lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

Device	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
SmartLine ST 700 with 4-20mA	0 FIT	174.3 FIT	222.7 FIT	43.9 FIT	90.0%

Table 2: Failure rates and Safe Failure Fraction according to IEC 61508

The architectural constraint type for the SmartLine ST 700 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 Honeywell International Inc. SmartLine ST 700 is 50 years. The failure rates of the Honeywell International Inc. SmartLine ST 700 may increase sometime after this period. When plant experience indicates a shorter useful lifetime, the number based on plant experience should be used.

Remote Diaphragm Seals / Flange Mounts:

An analysis was performed on the various Remote Seals / Flange Mounts that Honeywell International Inc. can supply with the SmartLine ST 700. The results of that analysis are listed in Table 3 and Table 4 for the various applications. The failure rates listed would get added to the rates for the SmartLine ST 700 that are listed above.

Failure Category	High Trip		Low Trip	
	Normal	Severe	Normal	Severe
	1 Seal, Gage/Absolute or Level			
Fail Safe Undetected	0	0	74	106
Fail Dangerous Undetected	76	109	2	3
No Effect	19	19	19	19
External Leakage	0	20	0	20
	2 Seals, Differential			
Fail Safe Undetected	70	101	77	111
Fail Dangerous Undetected	82	117	75	106
No Effect	37	37	37	37
External Leakage	22	63	22	63

Table 3: Additional failure rates Honeywell Remote Seals / Flange Mounts in FIT

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

External leakage failure rates do not directly contribute to the reliability of the device but should be reviewed for secondary safety and environmental issues.

Device	λ_{sd}	λ_{su} [1]	λ_{dd}	λ_{du}	SFF [2]
1 Seal, High Trip, Normal Service	-	0	0	76	-
1 Seal, High Trip, Severe Service	-	0	0	109	-
1 Seal, Low Trip, Normal Service	-	74	0	2	-
1 Seal, Low Trip, Severe Service	-	106	0	3	-
2 Seals, High Trip, Normal Service	-	70	0	82	-
2 Seals, High Trip, Severe Service	-	101	0	117	-
2 Seals, Low Trip, Normal Service	-	77	0	75	-
2 Seals, Low Trip, Severe Service	-	111	0	106	-

Table 4: Additional failure rates Honeywell Remote Seals / Flange Mounts according to IEC 61508 in FIT

Result:

With these results from the calculation it can be shown, that the SmartLine ST 700 fulfils SIL 2 for the hardware design in a single configuration.

[1] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
[2] Safe Failure Fraction needs to be calculated on an element level

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg

8.4 Software Design and Implementation

The software design is defined in the software design documents [D75] to [D85]. To provide the necessary internal testing of the hardware module to cover the IEC 61508 requirements for the Safe Failure Fraction (SFF) according SIL 2 various diagnostics has been implemented. This was done following the IEC 61508-3 SIL 3 process for software developing and implementation. These additional tests includes RAM and ROM testing and a flow control to reach a sufficient safe failure fraction > 90%. Coding standards are defined [D10] and tested in [D94] and [D95]. The corresponding documents have been reviewed by TÜV NORD Systems.

Result

The normative requirements out of the techniques and measures according to the IEC 61508-3 for software have been selected in the high level design of the software [D84] and considered for the development of the software. The software design and implementation and implemented measures are compliant to IEC 61508 part 3 according SIL 3.

8.5 Verification and Validation

The verification activities are defined by the reviews of the documentation according the specific phases of the development model (V-model). The review documentation has been discussed with responsible engineers from Honeywell International Inc. and has been reviewed by TÜV NORD Systems.

The test specification defined in the System Test Documentation [D86] to [D93] 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 [D118], the test results have been reviewed by TÜV NORD Systems. The test results are also referenced to the Design Specification.

The definition and results are documented in the Fault Injection Test Reports [D120]. In addition of the Fault Injection Tests from the manufacturer example Tests have

been performed by TÜV NORD Systems together with the test team. The results are documented in [D144]

Result

The review of the Integration Test Plan and the Test Reports from the manufacturer and the execution of the sample tests by TÜV NORD Systems 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.

8.6 Environmental Influences, EMC

The tests related to the environmental influences and EMC have been carried out through Honeywell International Inc. to show that the functional safety is not affected. The test plan and test results for the SmartLine ST 700 environmental and EMC tests are documented in [D116] and [D117].

Result

The defined requirements with respect to environmental influences and EMC are met. The tests carried out did not give rise to any safety objections.

8.7 Safety Manual

The Safety Manual [D129] has been reviewed to fulfill 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 SmartLine ST 700 has shown that 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 is in accordance with SIL 3 requirements allowing the use of dual redundant SmartLine ST 700 in SIL 3 applications.

The validation and testing activities has shown compliances between the realized transmitter implementation and the safety requirements specification.

The actual version of the Safety Manual must be considered for the use in safety relevant applications.

TÜV NORD Systems GmbH & Co. KG
Halderstr. 27
86150 Augsburg