IEC 61508 Functional Safety Assessment

Project:

STT25T Temperature Transmitter
With HART 6

Customer:

Honeywell International Inc.
Honeywell Field Products
512 Virginia Drive
Fort Washington, PA 19034
USA

Contract No.: Q10/02-43
Report No.: HON 10/02-43 R002
Version V2, Revision R3, 18 June 2012
Griff Francis

Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the:

STT25T Temperature Transmitter with HART 6

The functional safety assessment performed by *exida-certification* consisted of the following activities:

- *exida-certification* assessed the development process used by Honeywell Field Products through an audit against the requirements of IEC 61508.
- *exida-certification* reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.

The functional safety assessment was performed to the requirements of IEC 61508, SIL 3. Hardware and software process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. Also the user documentation (safety manual) was reviewed.

The results of the Functional Safety Assessment can be summarized by the following statements:

The STT25T Temperature Transmitter with HART 6 was found to meet the requirements of SIL 2 for random integrity @HFT=0, SIL 3 for random integrity @ HFT=1 and SIL 3 for systematic integrity. The manufacturer will be entitled to use the Functional Safety Logo.

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 provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option 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 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per IEC 61511 for sensors, final elements and other PE field devices.

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 option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

This assessment shall be done according to option 3.

This document shall describe the results of the IEC 61508 functional safety assessment of the STT25T Temperature Transmitter with HART 6.

2 Project Management

2.1 *exida*

exida is one of the world's leading product certification and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global corporation with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detailed product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Honeywell Field Products	Manufacturer of the STT25T Temperature Transmitter with HART 6
exida-consulting	Provided services to support Honeywell Field Products during the development of the STT25T Temperature Transmitter with HART 6.
exida-certification	Performed the IEC 61508 Functional Safety Assessment according to option 3 (see section 1)

Honeywell Field Products contracted *exida-certification* in February 2010 with the IEC 61508 Functional Safety Assessment of the above mentioned device.

2.3 Standards / Literature used

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

[N1]	IEC 61508 (Parts 1 - 7): 2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by Honeywell Field Products

[D1]	[D01]; NA; 12/10/2009	Integrated Project Schedule
[D2]	[D02]; 1.0; 9/28/2007	Coding Standards for Embedded C
[D3]	[D03]; A5; 12/1/2008	STT250 PROC OBSO REDESIGN SCHEMATIC
[D4]	[D04]; 3.3.3; 7/10/2008	Procedure: Change Management (Framework Practice 041-3U011)
[D5]	[D05]; 3.3.3; 7/8/2008	General: Holding Peer Reviews (Framework Practice 041-3U030)
[D6]	[D06]; NA; 7/10/2008	Procedure: Inspections (Framework Practice 041-3U031)
[D7]	[D07]; NA; 8/31/2007	Procedure: e-Inspection: (Framework Practice 041-3U032)
[D8]	[D08]; 3.3.3; 7/8/2008	Procedure: Creating and Distributing Software Builds (Framework Practice 041-3U080)
[D9]	[D09]; 0.2; 2/3/2009	HFS Field Instruments Firmware Development Process STT250 Platform Re-design Upgrade Project
[D10]	[D10]; NA; 8/9/2010	STT250 Obsolescence Re-design Weekly Status Meeting Minutes Example
[D11]	[D11]; 0.1; 4/12/2009	Smart Temperature Transmitters – STT250 Higher Level Design (Firmware)
[D12]	[D12]; 0; 5/15/2009	Corrective Action Process (G-PRO-QA.3.1)
[D13]	[D13]; NA; 8/14/2010	HFS Escalation Process Flow
[D14]	[D14]; NA; 9/17/2009	Supplier Selection and Qualification (Practice 061-13003)
[D15]	[D15]; NA; 8/18/2010	PC LINT Configuration Description
[D16]	[D16]; NA; 8/18/2010	LINT Error Resolution
[D17]	[D17]; NA; 7/20/2010	PC LINT Results
[D18]	[D18]; V1R1.0; 7/28/2002	exida Coding Standard
[D19]	[D19]; 2.1; 10/1/2009	STT250S SIL Unit Test Results
[D20]	[D20]; NA; 3/26/2002	Unit Test Framework Matrix
[D21]	[D21]; NA; 6/4/2009	Inspection Report: Main Board Schematic
[D22]	[D22]; NA; 3/5/2009	Inspection Report: High Level Design
[D23]	[D23]; 0.5; 6/13/2010	STT250 Smart Temperature Transmitter HART 5 System Test Plan
[D24]	[D24]; 0.3; 4/9/2010	STT250 Smart Temperature Transmitter DE System Test Results
[D25]	[D25]; 12/20/2010	PC LINT Results STT25S_H6

[D26]	[D26]; 12/20/2010	PC LINT Results STT25T_H5
[D27]	[D27]; 12/20/2010	PC LINT Results STT25T_H6
[D28]	[D29]; NA; 8/26/2010	STT250 Function Data Flow Diagram
[D29]	[D30]; NA; 8/26/2010	STT250 Code Base_Code Coverage Exposure
[D30]	[D33]; 0.4; 2/23/2010	STT250 Smart Temperature Transmitter HART 5 System Test Plan - older version
[D31]	[D34]; NA; 8/26/2010	Fault Injection Test Plan and Results
[D32]	[D35]; 06; 1/20/2009	Manufacturing Alert Process (HPS-MFG-GP-102)
[D33]	[D36]; NA; 11/10/2010	Example Weekly Status Meeting Minutes
[D34]	[D40]; NA; 6/11/2010	example Completed Code Review Checklist
[D35]	[D55]; 0.4; 4/6/2010	STT250 Smart Temperature Transmitter HART 5 System Test Plan with Results from 4-06-2010
[D36]	31-ST-25-32; 1.1; Jan 2011	Safety Manual: Honeywell STT250 Temperature Transmitter
[D37]	FSM; 2.3; 8/24/2007	H: STT25S Upgrade Project Plan
[D38]	FSM:H:PMP; 1.0; 8/28/2007	STT25T, H, D, M, S Processor Obsolescence Program Management Plan
[D39]	FSM:Training; 8/29/2007	FSM: Technical CV; Training plans & records of individuals (Team Competency Summary)
[D40]	Gap Analysis; V1 R1; 12/7/2005	exida: 61508 Gap Analysis
[D41]	H: NPDI; B; 3/30/2007	IM&C New Product Development Process
[D42]	H:Audit1; 8/8/2000	FM Certificate of Compliance STT25 Series
[D43]	H:Audit2; 2/14/2002	CSA Certificate of Compliance STT25 series
[D44]	H:Audit3; 6/30/2003	LCIE ATEX Certificate for series STT250
[D45]	H:Autotest; 3.0; 6/10/1999	Automated Test System Design - HART Implementation
[D46]	H:CS1; 0.7; 7/11/2006	IM&C Field Instruments Firmware Development Process
[D47]	H:CS2; 6/7/2006	Code Review Checklist
[D48]	H:DD1; 0.3; 7/21/2010	STT25S Smart Temp Transmitter Firmware Maintenance Document
[D49]	H:DD2; 2.1; 7/16/2007	High Level Software Design for HART 6.2 to STT25S
[D50]	H:DD3; 1.9; 9/4/2007	High Level Design for SIL3 Implementation
[D51]	H:DD3 RL; 9/7/2006	HLD SIL Implementation Review
[D52]	H:DD3 RLa; 3/27/2007	HLD for SIL3 Implementation Review Log confirmation
[D53]	H:DD4; 10/9/2006	Software Modules changed list
[D54]	H:ECO Analysis; 7/21/2006	Proven-in Use Analysis of Engineering Change Orders
[D55]	H:Hw HLD; 2.4; 8/17/2007	High Level Design Hardware for HART6 and SIL2/3

[D56]	H:Hw MD; 1.1; 8/29/2007	STT25S Hardware Maintainence Document
[D57]	H:Hw Req; 2.6; 8/17/2007	STT25S Hardware Requirements Specification
[D58]	H:ISO9001; 12/26/2004	ISO 9001 Certificate
[D59]	H:LP-204605-002; A; 6/3/2004	PAC & Sub-PAC Phase Gate Reviews
[D60]	H:PAR;	Siebel Tool for Tracking PAR's (Problem Anomaly Reports)
[D61]	H:PTP; 0.6; 6/12/2010	STT250 Smart Temperature Transmitter HART 6 System Test Plan
[D62]	H:PTP2; .04; 3/22/2007	Environmental Product Test Plan
[D63]	H:PTP3; 1.5; 3/22/2007	EMC Test Plan STT25S
[D64]	H:PTP3 R; 1.4.2; 8/24/2007	EMC Test Plan STT25S - w/Results
[D65]	H:PTP4 R; 10/22/2010	EMC Test Report STT 25S TEMPERATURE TRANSMITTER
[D66]	H:PTP5 R; 10/22/2010	EMC Test Report STT 25T TEMPERATURE TRANSMITTER
[D67]	H:Regression; 3.0; 8/19/1998	Automated Test System - Regression Test
[D68]	H:RMP; 1.1; 8/28/2007	Risk Management Plan
[D69]	H:SIL Overview; 12/16/2005	SIL Enhancement Project Overview
[D70]	H:SRS1; 1.0; 8/15/2007	STT25S Upgrades Product Abstract
[D71]	H:SRS2 HAIL; 2.2; 9/21/2010	STT250 Marketing Requirements Document
[D72]	H:SWRS; 0.8; 4/10/2010	STT250 Smart Temperature Transmitter Software Requirements Specification (SRS)
[D73]	H:Traceability Matrix; 0.8; 10/8/2010	Traceability Matrix with Tags
[D74]	H:UTP1; 2.2; 8/23/2007	HAIL Unit Test Plan for HART
[D75]	H:UTP2; 2.1; 10/1/2009	HAIL Unit Test Plan for SIL3 Implementation (same as [D19])
[D76]	H:UTP2 RL; 7/13/2006	Review Comments for Test Plans
[D77]	H:VER:FITR; .3; 9/14/2007	STT25S HART6/SIL Fault Injection Testing Report
[D78]	H:VER:FITRa; 8/31/2007	STT25S Fault Injection Testing of Watchdog Timer
[D79]	H:VER:TIMING; 1/24/2011	STT25S/T Timing Test Plan & Results
[D80]	H:VP R; 7/24/2007	STT25S System Test Plans - Results
[D81]	H:VP1; 1.2; 3/22/2007	AMS Integration Test Plan
[D82]	H:VP2; 1.2; 3/22/2007	Experion Test Plan for STT25S
[D83]	H:VP4; 0.4; 4/28/2010	STT25S, D, M System Test Plan

[D84]	HART 6;	HART 6 Features Summary
[D85]	Impact; 6/5/2007	Impact Analysis for updating STT25H
[D86]	OM1; 10/31/2009	STT25x Operator Manual Manual
[D87]	OM2; 0.3; 11/7/2006	Users Guide for HART6.x
[D88]	PIU; V1 R1; 8/20/2007	exida: Proven In Use Assessment: STT25S Transmitter
[D89]	PM:OD1; E; 11/27/1997	STT25H Product Overview
[D90]	PM:OD2; 6; 7/2/1997	STTx50 Functional Software Specification
[D91]	SW TCR; V1 R1; 2/6/2007	exida: SW Test Coverage Report
[D92]	SW TCRa; 2/2/2007	exida: SW Test Coverage Analysis
[D93]	SW TCRb; 8/30/2007	exida: SW Test Coverage Analysis w/Responses
[D94]	TÜV:RQ; 0.2; 10/20/2000	TÜV Report: Requirements Database Review
[D95]	V&V:Tables 2; 2; 8/28/2007	Part 2 Tables
[D96]	V&V:Tables 3; 2; 8/28/2007	Part 3 Tables
[D97]	VER:FMEDA; V1 R1; 2/8/2009	exida: FMEDA : STT25S Temperature Transmitter
[D98]	VER1; .96; 8/24/2007	STT25S Phase Completion Status
[D99]	VER2; 10/20/2006	Code Review Meeting Doc
[D100]	VER3; 11/2/2006	Completed SIL3 Coding Standard Checklist
[D101]	[D47]; 0.6; 3/10/2010	STT250 Smart Temperature Transmitter HART 6 Unit Test Plan
[D102]	D49; 1/6/2011	STT250 Unit Test Plan Sample Review
[D103]	[D48]; 0.7; 12/15/2010	STT250 Smart Temperature Transmitter HART 6 System Test Plan
[D104]	[D57]; 0.4; 12/15/2010	STTT250 Smart Temperature Transmitter Experion System Test Plan
[D105]	20 Dec 2011	Impact Anaysis,ECR 60606 and 63118
[D106]	9 Jan 2012	Impact Anaysis, ECR 59773
[D107]	50035832-706; Iss B;	Software Release Drawing, including checksum and change description

2.4.2 Documentation generated by *exida certification*

[R1]	HON 10-02-43 R002 V2R3 IEC 61508 Assessment	IEC 61508 Functional Safety Assessment for STT25T Temperature Transmitter with HART 6 (This document)
[R2]	Honeywell_STT25S-T_ SafetyCaseDB24Jan11.esc	Safety Case Database

3 Product Description

An example of the system and application environment in which the transmitter will be embedded once delivered is shown in the following drawing. Figure 1 shows an example Safety Instrumented Function in which the STT25T Temperature Transmitter with HART 6 can be used.

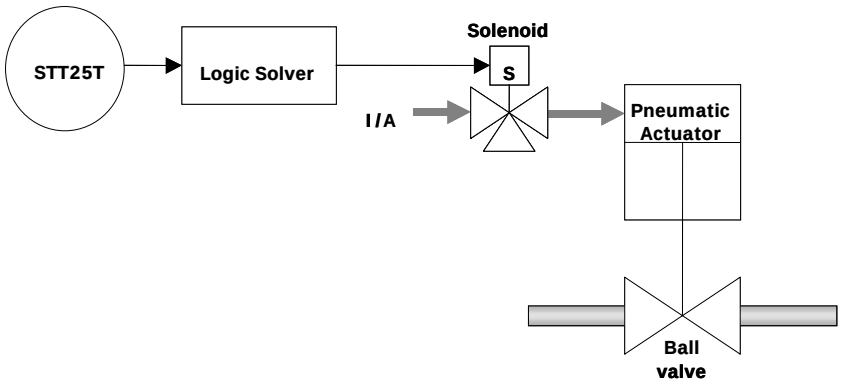


Figure 1 Example Safety Instrumented Function

Revisions covered:

Hardware 50035832-006 Rev A; Software Rev 1.0, checksum 0x0145783D

Hardware 50035832-006 Rev B; Software Rev 2.0, checksum 0x01438D1E

4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from Honeywell Field Products as documented in section 2.4.1. A visit to the Honeywell's Fort Washington, PA facility on 25, 26 August 2010 was included as part of the assessment.

4.1 Methodology

The full functional safety assessment includes an assessment of all fault avoidance and fault control measures during hardware and software development and demonstrates full compliance with IEC 61508 to the end-user. The assessment considers all requirements of IEC 61508.

As part of the IEC 61508 functional safety assessment the following aspects have been reviewed:

- Development process, including:
    - Functional Safety Management, including training and competence recording, FSM planning, and configuration management
    - Specification process, techniques and documentation
    - Design process, techniques and documentation, including tools used

    - Validation activities, including development test procedures, test plans and reports, production test procedures and documentation
    - Verification activities and documentation
    - Modification process and documentation
    - Installation, operation, and maintenance requirements, including user documentation
- Product design
    - Hardware architecture and failure behavior, documented in a FMEDA
    - Software architecture and failure behavior

The review of the development procedures is described in section 5.1. The review of the product design is described in section 5.2.

4.2 Assessment level

The STT25T Temperature Transmitter with HART 6 has been assessed per IEC 61508 to the following levels:

- SIL 2 random integrity for a single device (Hardware Fault Tolerance = 0)
- SIL 3 random integrity for multiple devices (Hardware Fault Tolerance = 1)

The development procedures were assessed as suitable for use in applications with a maximum Safety Integrity Level of 3 (SIL 3 capability) according to IEC 61508.

5 Results of the IEC 61508 Functional Safety Assessment

exida-certification assessed the development process used by Honeywell Field Products during the product development against the objectives of IEC 61508 parts 1, 2, and 3. The development of the STT25T Temperature Transmitter with HART 6 was done per a development process that was close to a IEC 61508 SIL 3 compliant development process. Supplemental activities were performed.

5.1 Lifecycle Activities and Fault Avoidance Measures

Honeywell Field Products used a development process during the STT25S/T development that met most requirements of IEC 61508. This functional safety assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the transmitter development. Additional analysis and documentation activities were performed to complete the requirements of IEC 61508. The investigation was executed using subsets of the IEC 61508 requirements tailored to the SIL 3 work scope of the development team. The result of the assessment can be summarized by the following observations:

The audited Honeywell development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1.1 Functional Safety Management

FSM Planning

The functional safety management of any functional safety product development is governed by the Honeywell Program Management Plan [D38]. For this development project Honeywell Field Products created a Project Plan which includes plans for Functional Safety Management (FSM). The Project Plan including FSM planning for the STT25T, [D37] was reviewed. This plan includes the following sections: Project Definition, Project Organization, Scope of Services (development process), and Configuration Management.

Version Control

As documented in [D38] and [D9], the following documents are stored under version control:

- Software source code modules
- Test plans and results
- Safety analysis and requirements
- Justification for, details of, impact analysis for, and approval for all modifications
- Software/hardware specification and design documents
- Verification results
- Evaluation of and impact analysis for pre-existing software/hardware components/packages.
- All tools and development environments.

Training, Competency recording

The Team Competency Summary, [D39] documents the qualifications of the independent V&V and functional safety assessment team.

5.1.2 Safety Requirements Specification and Architecture Design

As defined in, a safety requirements specification (SRS) is done for all products that must meet IEC 61508 requirements. The safety requirements are contained in the Marketing Requirements Document (MRD) for the STT25T, [D71]. This document was reviewed as part of the assessment. The requirements include Operating Modes, Safety Functional Requirements and Safety Integrity Requirements.

[D38] also states that an Architecture Design document be created. For the STT25T, an architecture design is included in the High Level Hardware Deisgn Specification, [D55] which was reviewed as part of the assessment. This document includes a block diagram of the overall architecture and a description of all components and interfaces. This document has been reviewed in terms of completeness and correctness against the safety requirements.

5.1.3 Hardware Design

Hardware design, including both electrical and mechanical design, is done according to [D38]. The hardware design process includes the creation of a hardware specification, hardware design, design verification testing, a failure modes, effects and diagnostic analysis (FMEDA), a design review, the creation of manufacturing drawings, manufacturing test, and then a final design review.

5.1.4 Validation

All safety requirements documented in [D71] are validated by test or inspection. A validation test specification and plan [D61] and [D75] were created for the STT25T Temperature Transmitter with HART 6 and reviewed as part of the assessment. Each validation test includes an explicit test to the requirement being validated. As part of the assessment, it was verified that all safety requirements were covered by one or more validation tests.

5.1.5 Verification

The development and verification activities are defined in [D38]. Verification activities include the following: Design Review Meetings, Hardware Verification Testing via Fault Injection, FMEDA, Module Testing, Module Integration Test, and Software Inspection.

5.1.6 Modifications

Modifications are done per the Honeywell process as documented in [D12].

5.1.7 User documentation

Honeywell Field Products created a Safety Manual for the STT25T, see [D36]. This safety manual was assessed by *exida-certification*. The final version is considered to be in compliance with the requirements of IEC 61508. The document includes all required reliability data and operations, maintenance, and proof test procedures.

5.2 Hardware Assessment

To evaluate the hardware design of the STT25T, a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida-certification* for each component in the system. This is documented in [D97]. The FMEDA was verified using Fault Injection Testing as part of the development, see [D77], and as part of the IEC 61508 assessment.

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 extensions to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design.

From the FMEDA failure rates are derived for each important failure category. Table 1 lists these failure rates as reported in the FMEDA reports. The failure rates are valid for the useful life of the devices.

Table 1 Failure rates according to IEC 61508

Device	λ_{SD}	λ_{SU}[1]	λ_{DD}	λ_{DU}	SFF[2]
STT25T Temperature Transmitter with HART 6 RTD Input and RMA300-ME	0 FIT	224.6 FIT	287.9 FIT	33.5 FIT	93.9%
STT25T Temperature Transmitter with HART 6 TC Input and RMA300-ME	0 FIT	211.1 FIT	279.7 FIT	30.8 FIT	94.1%
STT25T Temperature Transmitter with HART 6 RTD Input and RMA300-SM	0 FIT	224.6 FIT	286.6 FIT	42.7 FIT	92.3%
STT25T Temperature Transmitter with HART 6 TC Input and RMA300-SM	0 FIT	211.1 FIT	278.4 FIT	40.0 FIT	92.5%
STT25T Temperature Transmitter with HART 6 RTD Input and SPD	0 FIT	224.6 FIT	300.4 FIT	34.5 FIT	93.8%
STT25T Temperature Transmitter with HART 6 TC Input and SPD	0 FIT	211.1 FIT	292.2 FIT	31.8 FIT	93.8%

A user of the STT25T 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 at a particular safety integrity level (SIL).

[1] It is important to realize that the Residual failures are included in the Safe Undetected failure category according to IEC 61508. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations

[2] Safe Failure Fraction needs to be calculated on (sub)system level

For low demand SIL 2 applications the PFD_{AVG} value of the Safety Instrumented Function needs to be ≥ 10^{-3} and < 10^{-2}. The FMEDA report [D97] lists the percentage that the STT25T uses of this budget. For a SIL 2 application, the PFD_{AVG} for a 1-year Proof Test Interval of the Honeywell STT25T Transmitter with a 4-wire RTD is approximately equal to 3.5% of the range. The PFD_{AVG} for a 1-year Proof Test Interval of the Honeywell STT25T Transmitter with a Thermocouple is approximately equal to 3.2% of the range.

These results must be considered in combination with PFD_{AVG} of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL). The Safety Manual states that the application engineer should calculate the PFD_{AVG} for each defined safety instrumented function (SIF) to verify the design of that SIF.

The analysis shows that design of the STT25T meets the hardware requirements of IEC 61508, SIL 2 @HFT=0 and SIL 3 @ HFT=1.

5.3 Quality Management System

Honeywell's quality management system has been ISO 9001 certified, [D58]. exida examined the quality management system and determined that it was adequate to ensure that the functional safety characteristics of the product are maintained through the manufacturing process.

6 Terms and Definitions

Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Modes, Effects and Diagnostic Analysis
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
PFH	Probability of dangerous Failure per Hour
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).
V&V	Verification and Validation
HART	Highway Addressable Remote Transducer
AI	Analog Input
AO	Analog Output
DI	Digital Input
DO	Digital Output
Type A (sub)system	“Non-Complex” (sub)system (using discrete elements); for details see 7.4.3.1.2 of IEC 61508-2
Type B (sub)system	“Complex” (sub)system (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 prepares reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* 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.

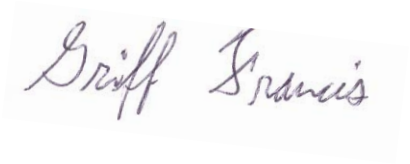
7.2 Releases

Version:	V2	
Revision:	R3	
Version History:	V2, R3:	added [D105] - [D107] to section 2.4.1, reference Q12/06-051; 18 June 2012
	V2, R2:	updated product name and customer address; 17 June 2011
	V2, R1:	created from Report No. HON 10/02-43 R001, started at V2 R1 to keep revision the same as R001; 24 Feb 2011
Author:	Griff Francis	
Review:	V2, R3:	Roger Brill (Honeywell)
	V0, R1:	Michael Medoff, William Goble as R001
Release status:	Released	

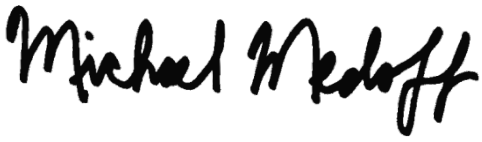
7.3 Future Enhancements

At request of client.

7.4 Release Signatures



Griff Francis, Safety Engineer



Michael Medoff, Senior Safety Engineer

Dr. William M. Goble, Principal Partner