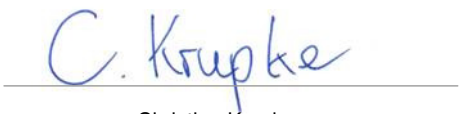
TECHNICAL REPORT ON THE TYPE APPROVAL OF THE ULTRASONIC FLOW MEASUREMENT SYSTEM "PANAFLOW HT" ACCORDING TO IEC 61508, SIL 2, SIL 3 RESPECTIVELY

Version No.:	1.0
Date of Issue:	2012-09-20
Test Report-No.:	SLA-0167/2009TB-3
Product:	Flow Measurement System PanaFlow HT
Client:	GE Sensing & Inspection Technologies 1100 Technology Park Drive Billerica MA 01821-4111, USA
Order No.:	G.SEB.BS.02.019.01.031
Inspecting authority:	TÜV NORD Systems GmbH & Co. KG Branch South Functional Safety Halderstr. 27 86150 Augsburg, Germany
Author	 Christian Krupke
Review	 Robert Korte

Document version history:

Version	Date	Author	Description of change
0.1	2011-10-12	Ch. Krupke	Initialisation
0.2	2011-10-12	R. Korte	Review
0.3	2011-10-13	Ch. Krupke	Update after Review
0.4	2011-10-24	Ch. Krupke	Update after Review GE – Chris Brolin
0.5	2011-11-28	H. Kränzle	Update after Review
0.6	2012-09-13	Ch. Krupke	Initialisation of the final assessment report
0.7	2012-09-18	R. Korte	Review
0.8	2012-09-18	Ch. Krupke	Update after Review
1.0	2012-09-20	Ch. Krupke	Update after Review GE

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

Table of Contents Page

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

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

Tables **Page**

Figures **Page**

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

1 Subject of assessment

The company GE Sensing & Inspection Technologies (hereinafter known as GE) develops, among other items, safety related Measurement Process Units (MPU) and transmitters, whose failure could have an effect on the safety of people and/or the safety of their environment. GE intends to develop a state of the art safety related ultrasonic flow measurement system called PanaFlow HT (in the following known as PanaFlow HT) based on the international standard IEC 61508. The internal project name of the PanaFlow HT is Genesis. The assessment will take place in two phases:

Phase A - Concept-Phase: In this phase TÜV NORD Systems GmbH & Co. KG (in the following named TÜV NORD) approves the general safety concept.

Phase B - Realisation of the safety function: In this phase the designed safety function should be assessed and certified.

The objective of the project encloses the assessment of the existing **F**unctional **S**afety **M**anagement, in accordance with IEC 61508 (part 1) along with the necessary development processes, techniques and measures and technical aspects.

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

2 Purpose of this report

This report is based on the concept approval report [81] and contains all results of the assessment according to IEC 61508.

It shall be shown, that the relevant requirements for management, planning and design are correct, complete and have been fulfilled sufficiently and that the required safety related measurements for avoidance, detection and control of systematic failures in soft- and hardware and random failures in HW have been fulfilled sufficiently.

Further it was assessed that the verification, the overall validation, the FSM Plan and user documentation with its relevant requirements, activities and their results have been done sufficiently from the point of view of the independent assessment of functional safety.

3 Basis of certification

Because of the application area of the PanaFlow HT, the following standards are relevant.

3.1 Generic standards for functional safety

Standards	
IEC 61508-1: 2010 SIL 2,	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements
IEC 61508-2: 2010 SIL 2,	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
IEC 61508-3: 2010 SIL 3,	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 3: Software Requirements

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

4 Documents for inspection and testing

The evaluation of the development of the PanaFlow HT is based on the following documents and assessment-/ review-protocols.

A list of valid documents significant for assessment and certification is included in the corresponding V&V Plan.

On the base of the documents reviews were documented by TÜV and measures were derived with GE (see [78]).

Customer documents:

[1] System Requirements Specification UMPU:
UMPU_SRS_v10049.pdf

[2] V&V-Plan UMPU:
UMPU_VV_v4_8.xls

[3] UMPU measure principles:
Genesis Safety Chain concept 2010-06-14.doc

[4] FMEA UMPU:
UFM_FMEA_v1_8_approved.xls

[5] FMEA OPTION BOARD:
PLTM_FMEA_v1_7_approved.xls

[6] Safety Plan:
Genesis_FSM_Plan_v4.2_approved.pdf

[7] Change Management Process:
Genesis_REF(ChangeRequestProcess)_v1_2_approved.pd

[8] Product Change list for Impact analysis:
Genesis_REF(ProductChangeChecklist)_v1_1_approved.docx

[9] Engineering Change Order:
Engineering Change Order (ECO) TCP-001-7.3.7 Rev D.doc

[10] Engineering Change Review Form:
Engineering Change Review Form 951-005 Rev C.xlsx

[11] Continuous Improvement Process:
Continuous Improvement (GEEQMS 8.5).pdf

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

[12] Process Customer Issue Resolution:
Customer Issue Resolution (CIR) (GEE-006).pdf

[13] Process Document Control:
Document Control (GEEQMS 4.2.3)_v3.2.pdf

[14] Process Record Control:
Record Control (GEEQMS 4.2.4)_v4.0.pdf

[15] Documentation Structure within the PanaFlow HT project:
Genesis_REF(DocStructureandIndex)_v1_0.xlsx

[16] PanaFlow HT documentation guide:
PLTM_REF_GenesisDocGuide_v1_5_approved.pdf

[17] Process Internal Audits:
GEE QMS 8.2.2 Internal Audit.pdf

[18] New product introduction (NPI) procedure:
MCS New Product Introduction Procedure (GEMCS_TP 7.3-010)_v1.0.pdf

[19] NPI process graphic:
npi dev process graphic for tuv.vsd

[20] Process handling of customer complaints:
Processing Customer Complaints BCP-002-8.5.2 Rev B.doc

[21] Position descriptions:
PLTM_REF(PositionDescription--Functional Safety Manager)_v1_1.pdf
PLTM_REF(PositionDescription--FW developer and tester)_v1_2.pdf
PLTM_REF(PositionDescription--FW Lead_v1_2.pdf
PLTM_REF(PositionDescription--Production)_v1_0.pdf
PLTM_REF(PositionDescription--Program Manager)_v1_0.pdf
PLTM_REF(PositionDescription--Program Technical Lead)_v1_0.pdf
PLTM_REF(PositionDescription--Functional Safety Assessor)_v1_0.pdf
PLTM_REF(PositionDescription--HW Developers and Testers)_v1_1.pdf
PLTM_REF(PositionDescription--Technical Writers)_v1_1.pdf
PLTM_REF(PositionDescription--Technology Lead)_v1_1.pdf
PLTM_REF(PositionDescription--Quality Assurance)_v1_1.pdf

[22] Purchasing process:
Supplier_Surveillance_SQE-005-7_4_1_Rev_E.pdf

[23] Meeting presentation:
Ultrasonic flowmeter TUV audit 02102012 final.pptx

[24] UMPU HWRQ Specification:
UMPU_HWRQ_v10175.pdf

[25] FWRQ Specification
UMPU_FWRQ_v10914.pdf

[26] HW Design Specification
UMPU-HWDS-v10065.pdf

[27] FW Development Life Cycle:
Firmware Development Life Cycle Rev011 approved.pdf

[28] Programming Style and Coding Standard:
Programming Style and Coding Standard for C and CPP software v1_2_approved.docx

[29] System Verification and Validation Plan:
UMPU_SVT-v10929_approved.pdf

[30] Linklist UFM to SVT:
UFM_SRS_SVT_links.xlsx

[31] Test case EDN 801 and report:
EDN801GenesisUFMAnalogOutputTestCase.docx;
EDN801.PDF;

[32] Test case EDN 802 and report:
EDN802GenesisUFMDigitalOutputTestCase.doc;
EDN802 Digital.PDF;

[33] Test case EDN 804:
EDN804GenesisUFMModbusTestCase.docx

[34] Test case EDN 808 and report:
EDN808GenesisUFMCodeLoadingTestCase.docx;
EDN808.PDF;

[35] Test case EDN 813:
EDN813GenesisUFMUnitsConversionTestCase.doc

[36] Fault Injection Test Plan:
EDN830FaultInjectionTestPlan.xls

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

[37] Test Case EDN 816:
EDN816GenesisUFMSafetySILDVTTestCase.docx
[38] Test Case EDN 814:
EDN814GenesisUFMFlowTestCase.docx
[39] Overview EMC tests:
Genesis EMC testing for EMCD & SIL, with procedures.xlsx
[40] EMC test descriptions:
714-895revA.pdf; 714-896revA.pdf; 714-897revA.pdf
[41] EDN 820 – Environmental Test cases and report:
EDN 820 Genesis Environmental Test Case.doc
EDN820 Environmental.pdf
[42] UMPU FW Design Specification:
GenesisUMPU_DS_1.7 part2.pdf
[43] PLTM 461 Test data:
PLTM-461_testdata_v2.doc
[44] Persistent parameter configuration steps:
PersistentParameterConfigSteps.pdf
[45] Genesis Modbus Map:
GenesisModbusMap_2_8_5_final.xlsx
[46] Test procedure Voltage dips, interruption and variation for DC power port:
714-898revA.pdf
[47] Configuration Control Plan:
Genesis_REF(Configuration Control Plan)_v1_0_approved.docx
[48] SW Decommissioning Plan:
Genesis UMPU Software Decommissioning Plan v1_0
[49] Genesis FW Code – Links to modules:
GenesisFWCode-v10792.pdf
[50] Genesis HW – Links to BOM/Schematics/Layout:
UMPU_Prototype_v10931.pdf
[51] Firmware Qualification Test Specification and Report:
UMPU_FWTS_v10832.pdf
[52] Verification link list – FW Modules and FW Tests:

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

FWTS_FWTR_linked_workitems_2012-08-10.xlsx

[53] Schematics:

Main and receiver board: 700-1565revA.pdf, 700-1566revA.pdf

Option board: TUV_700-1615 Rev17.pdf

[54] Review of schematics:

Response___GENESIS UMPU Schematics Review Minutes - 2010_05_18.doc

[55] EDN 817 – User Manual Test cases and report:

EDN817GenesisUFMUserManualTestCaseRev5.docx

EDN817.PDF

[56] BOM Main board, receiver and option board:

703-1565-03UMPUMainBoard.xlsx; 703-1566-00BOMUMPUReceiverBoard.xls

TUV_703-1615-00 Rev18.xls

[57] Layout Main board and Receiver board:

703-1565revC.pdf;

703-1566revC.pdf;

[58] HW Prototype Test Report:

Genesis-DR5actionitemsjan262012.xls

[59] Mechanical Prototype test report:

IssuefindingandPriolitylistafterGenesisCNCenclosureinspected-11-16-2011-followup.xlsx

[60] Code Review file - example:

DATAACQ.rtf

[61] Review of mechanical design:

Issue finding and Priolity list after Genesis CNC enclosure inspected -11-16-2011-follow up.xlsx;

RE Meeting minutes and follow down after review with Cheef Engineer.msg

[62] Transmitter enclosure design document:

Transmitterenclosuredesigndocument2.5-2011[1].pdf

[63] Review of layout:

IssuefindingandPriolitylistafterGenesisCNCenclosureinspected-11-16-2011-followup.xlsx

[64] EDN 812 Test report:

EDN812 Fault Injection Tests Compiled Rev B.xlsx

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

[65] FW-Code Extract:

CompositeCalc.c.txt; Correlation.c.txt; DataAcq.c.txt; ErrorLogic.c.txt; FindPeak.c.txt; Flow.c.txt; FlowLogic.c.txt; FPGAdriver.c.txt; FreqOut.c.txt; Main.c.txt; PathCalc.c.txt; PerParamBlock.c.txt; PersistParam.c.txt; SafeOutput.c.txt; Scheduler.c.txt; SignalAnalysis.c.txt; SignalDiagnostic.c.txt; SignalProcessing.c.txt; SigProc.c.txt; SilSupervisor.c.txt; TransitTime.c.txt; UnitConv.c.txt; ZeroCross.c.txt

[66] Module Tests with LDRA - Extract:

Test Manager Report safeoutput.c.pdf;

SILSUPER_Win_TestManagerReport_SVN2283.pdf;

SILSuper Module Quality Review Report.pdf;

SILSuper Module Code Reviews.pdf;

SafeOut Module Quality Review Report.pdf;

Regression Report Example safe output.pdf;

Regression Report WIN WBOX SIL Super.pdf

O -QA_Org-_QA-SYSTEM-Quality-Deck-SIL_Genesis-File.pdf

Dynamic Coverage Analysis Report Example Safe Output.pdf

CodeReviewReport_UnitConv_2560.mht

[67] Code Review – GE – Extract:

FLOW.rtf;

SAFEOUT.rtf;

SILSUPER.rtf

[68] Marketing Functional Specification:

Genesis MFS v2_3 2010-12-10 signed.pdf

[69] Fault injection testdata:

FaultInjectionTests PLTM-512_testdata_v1.pdf

[70] UMPU HW-FW Integration tests:

UMPU_HWFWIT-v10896.pdf

[71] EDN 805 – HART Testreport:

EDN805 HART.PDF

[72] User manual:

910-294UA_18_UsersManual.pdf

[73] Safety Manual:

917-025A_14_SafetyManual.pdf

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

[74] Overview LDRA Test results:
LDRA_ReportSummary_For_TUV_v1 1.xlsx

[75] UMPU Software Deviation Document:
GenesisUMPU_SDD_v1.2.docx

[76] Failed Functions:
GenesisUMPU_SDD_WorksheetForFailedFunctions_1 1.xlsx

[77] FMEDA UMPU and Option Board:
FMEDA_GENESIS_UMPU_V06_20120908_with_FaultInsertion_links.xls
FMEDA_GENESIS_Optionboard_V06_20120911_with_FaultInsertionlinks.xls

Approval authority documents:

[78] Review protocol:
Review_Mod_Genesis_v4_3.docx

[79] Assessment plan:
SLA_0167_2009PPL_V0_1_GE_UMPU.doc
SLA_0167_2009CL_IEC61508_V0_1_GE_UMPU.xlsx

[80] Assessment report ultrasonic flow sensor TÜV NORD SysTec:
SLA_0107_2009TB_2_V1_0_EN_Rheonik_UT.pdf

[81] Concept approval report:
SLA_0167_2009TB_3_V0_5_EN_Genesis_UMPU.pdf

[82] FMEDA report UMPU:
SLA_0060_2010TR01_EN_UMPU_GE_V2.pdf

[83] FMEDA report option board:
SLA_0060_2010TR04_EN_optionBoard_GE_V02.doc

[84] Assessment results IEC 61508 :
SLA_0167_2009CL_IEC61508_V0_2_GE_UMPU.xlsx

[85] Meeting protocol from Audit on 2012-02-13 in Billerica :
TUVNORD_Protokoll_Meeting_GE_BILLERICA_20120213_v0_2.doc

[86] Factory inspection:
FactoryInspection_GE_BILLERICA_Part_C_v1_0_signed_GE

[87] Calculation PFH and PFD_{avg}:
Calculation_PFH_PFD.xls

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

5 Abbreviations and glossary

In this report the following abbreviations have been used.

Term	Definition
DC	Diagnostic Coverage, Ratio of sum of failure rates of dangerous detected failures over the sum of failure rates of all dangerous failures (= dangerous detected failures + dangerous undetected failures).
EMC	Electromagnetic compatibility
E/E/PES	Electrical/Electronic/Programmable Electronic
FIT	Failure in Time = 10^{-9} h
FMEA	Failure Mode and Effects Analysis
FMEDA	Failure Mode Effects and Diagnostics Analysis
FW	Firmware = Embedded Software
FSM	Functional Safety Management
HFT	Hardware Fault Tolerance: Count of faults, which are tolerated by hardware without any dangerous failures. (HFT+1 can fail dangerous.)
HW	Hardware
MPU	Measurement Process Unit
λ_{dd}, λ_{du}, λ_{sd}, λ_{su}, λ_{d}, λ_{s}	Failure rates (Lambda) with respect to the safety function (e.g. shut down), where the first letter defines the kind of failure s=safe or d=dangerous and the second letter defines the detection d=detected or u=undetected. $\lambda_d=\lambda_{du}+\lambda_{dd}$, $\lambda_s=\lambda_{su}+\lambda_{sd}$.
PFD_{avg}	Probability of Failure on Demand Average probability of failure of a system to perform its design functions on demand.
PFH	Probability of Failure per Hour
QM	Quality Management
SF	Safety Function
SFF	Safe Failure Fraction [%] (Percentage of safe failures) = $1 - (\lambda_{[du]}/(\lambda_{[total]})$
SIL	Safety Integrity Level

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

Term	Definition
SLC	Safety Life Cycle
SRS	Safety Requirements Specification (Document)
SW	Software
UMPU	Ultrasonic Measurement Process Unit

Table 1: Abbreviations and glossary

6 System description

The PanaFlow HT is an ultrasonic flow measurement system which measures a volumetric flow rate in m^3/sec.

The safety part of the Flow Measurement System consists basically of the following parts (see also Figure 1):

- Ultrasonic sensors: sensor arrangement mounted on a pipe to measure the acoustic transit times in the medium to determine the flow rate of the medium. The ultrasonic flow sensors have been analyzed in a proven in use assessment according to IEC 61508 SIL 2 from TÜV NORD SysTec. See therefore the technical report of the assessment [80]. The ultrasonic sensors can fulfill the requirements for SIL 2. The assessment results in the report [80] are accepted by TÜV NORD Systems.
- Co-ax – Cabling: connects the US-Transducer to the UMPU by means of matched cables and terminal blocks.
- UMPU: the ultrasonic measurement processing unit generates and processes the transducer signals, calculate and determine the measurement values. The UMPU has capacity for 3 transducer pairs (only two pairs are used in the safety variant of the measurement system) as input channels and the safety relevant output is the SPI Interface to the option board.
- Option board: The Option board converts the measurement values from the UMPU FPGA and gives a 4-20mA current signal. This signal will be read back

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

by the UMPU, in case of differences between nominal and actual value the output goes under 4mA (fire low).

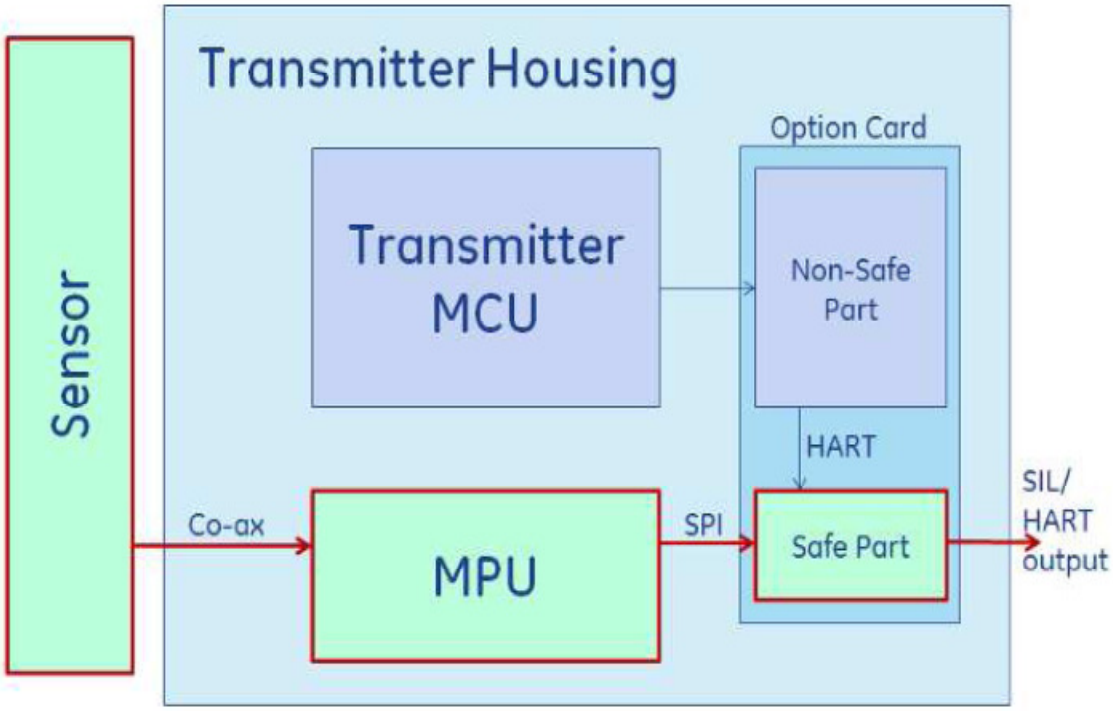


Figure 1: UMPU Safety Chain

6.1 UMPU measurement principle

The measurement system with UMPU measures a volumetric flow rate in m^3/sec (cubic meters per second).

The function of the UMPU is to convert the flow measurement signals from the ultrasonic sensor to a 4 to 20 mA output. A value between 4 and 20 mA is proportional to the volumetric flow rate and indicates normal operation. A value less than or equal 3.6mA indicates the Safe State for "Fire Low". A value greater than or equal 21.0mA indicates the Safe State for "Fire High". Safety function and safe state are described in chapter 7.1.

The UMPU measurement system determines the safe output in three steps:

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

- **Acoustic Measurement.** The MPU uses the sensor to measure the acoustic transit time through the fluid. This transit time is proportional to the flow rate of the fluid in the pipe. Details of acoustic measurement are given in safety chain concept [3].

- **Calculating Flow Rate**. The Measurement Process Unit uses this transit time and the known path length of the acoustic signal to determine the velocity of the fluid in m/s. The MPU then multiplies this by the known cross-sectional area of the pipe to determine volumetric flow rate in m^3/sec. Finally, the MPU uses this flow rate and the scaling of the safe output to determine what mA value to put out and gives this digital value over the SPI interface to the option board. In the following figure the block schematic of the UMPU is pictured.

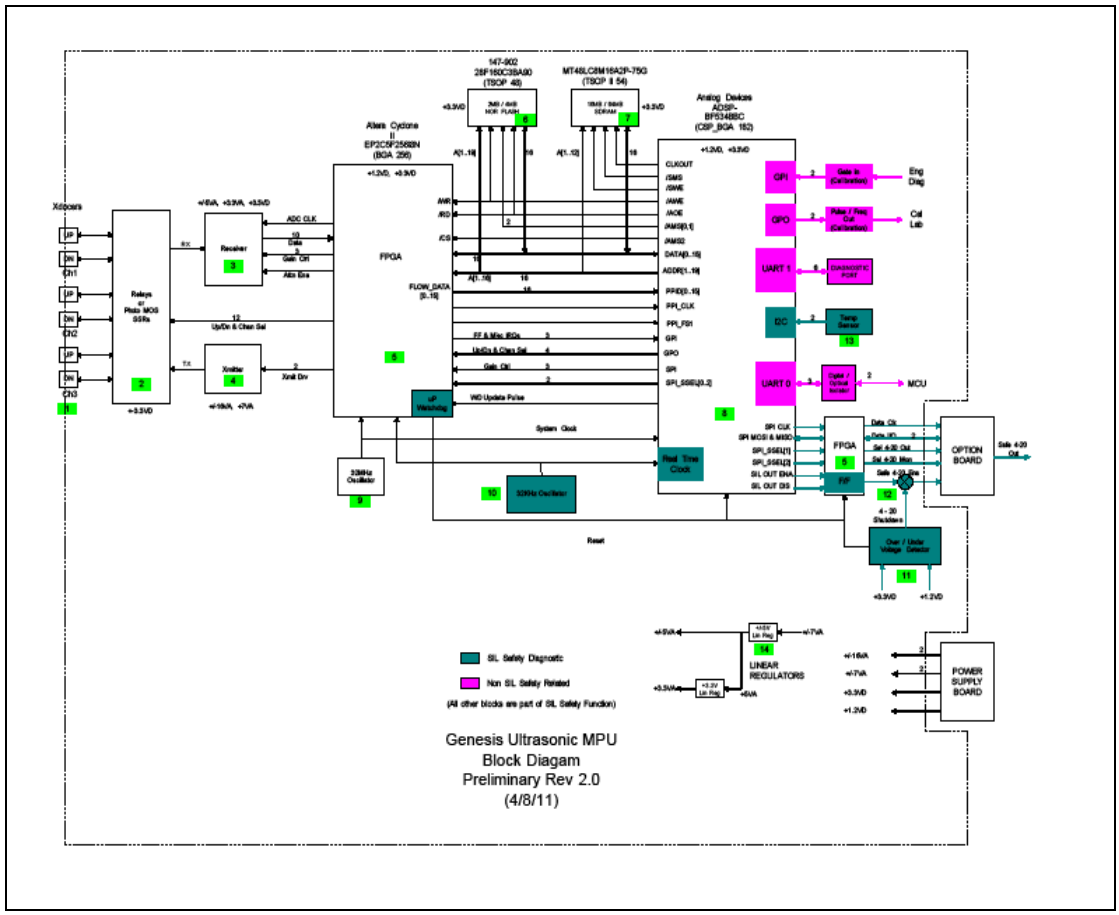


Figure 2: Block schematic UMPU

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

- **Converting the Digital Signal** The Option board converts the measurement values from the UMPU FPGA and gives a 4-20mA current signal. This signal will be read back by the UMPU, in case of differences between nominal and actual value the output goes under 4mA (fire low). In the following picture the block schematic of the option board is pictured.

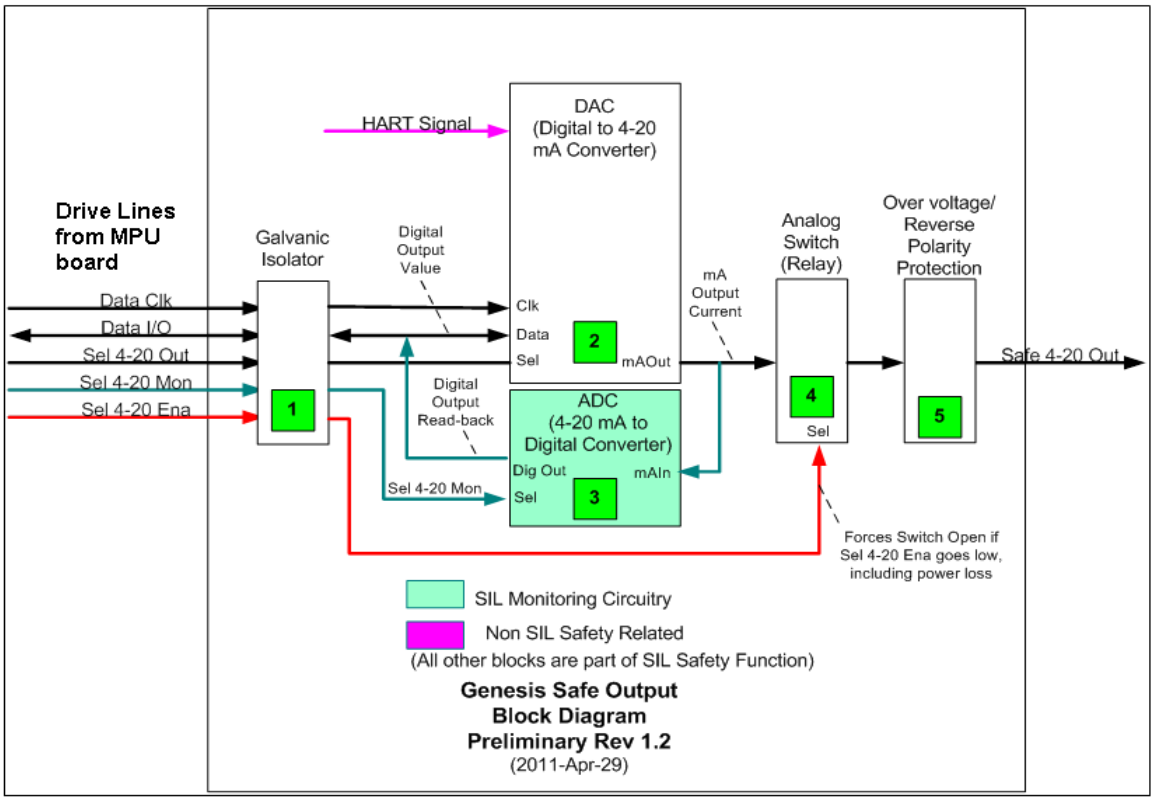


Figure 3: Block schematics option board

A detailed description of the UMPU functionality is given in [1].

6.2 Field of Application

The platform will serve a variety of process systems, e.g. in industrial automation, the process industry and custody transfer applications. The platform is to be used world-wide with a focus on North America, Europe, China, Korea and Japan. In the following an example application is given to illustrate how the PanaFlow HT is utilized.

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

Delayed Coker Application

The residue from an oil refining process is heated to 600 degrees C which allows it to flow in liquid form to a delayed coker process. Here the oil residual is further processed to extract another 10% of energy products. If the flow of the liquefied product slows below a certain rate the material will harden into a solid mass called “coke” that will block the pipeline. This coke can only be cleared by dismantling the pipeline, at great cost and risk of human injury.

The material is toxic and an environmental hazard. A high flow rate is an indication of a leak in the pipeline, which is also hazardous. The requirement of the flow meter is to provide a reliable flow measurement of a very hot liquid. The ultrasonic flow meter, which causes no restriction to the flowing fluid, provides volumetric flow rate data to the customer control system via 4-20 mA output. Any indication that the flow measurement is not trustworthy must be reported to the system by forcing the 4-20 mA output value to the Dangerous Detected state.

7 Overview of the safety loop

7.1 Safety Function, safe and dangerous state

For the UMPU, the 4-20 mA current output reflects the volumetric flow rate or the mass flow rate.

The safe state of the UMPU is either Fire Low or Fire High, depending on which dangerous detected state has been selected by the authorized user for the 4 – 20mA output.

The term “Fire Low” corresponds to a current output below or equal to 3.6mA and the term “Fire High” corresponds to a current output above or equal to 21.0 mA compliant with NAMUR NE 43.

The dangerous sate is when the abbreviation of the measurement is greater than 2%.

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

7.2 Timings

The timings are shown in the SRS [1] and are listed in the following table.

Name	Time	Description/Comment
Reaction Time	<= 1min	The reaction time is the time taken after threshold violation for the current output to be in safe state (Fire Low)
Fault detection time	< 1min	The Fault Detection Time is the time needed to detect an internal fault.
Proof Test Interval	1 year	The proof test is to be executed according to procedures described in the safety manual.
MTTR	24h	Mean Time to Restoration
MRT	24h	Mean Repair Time
Life time	20 years	Life time of the system

Table 2: Timing requirements

In the following figure the timing constraints are pictured:

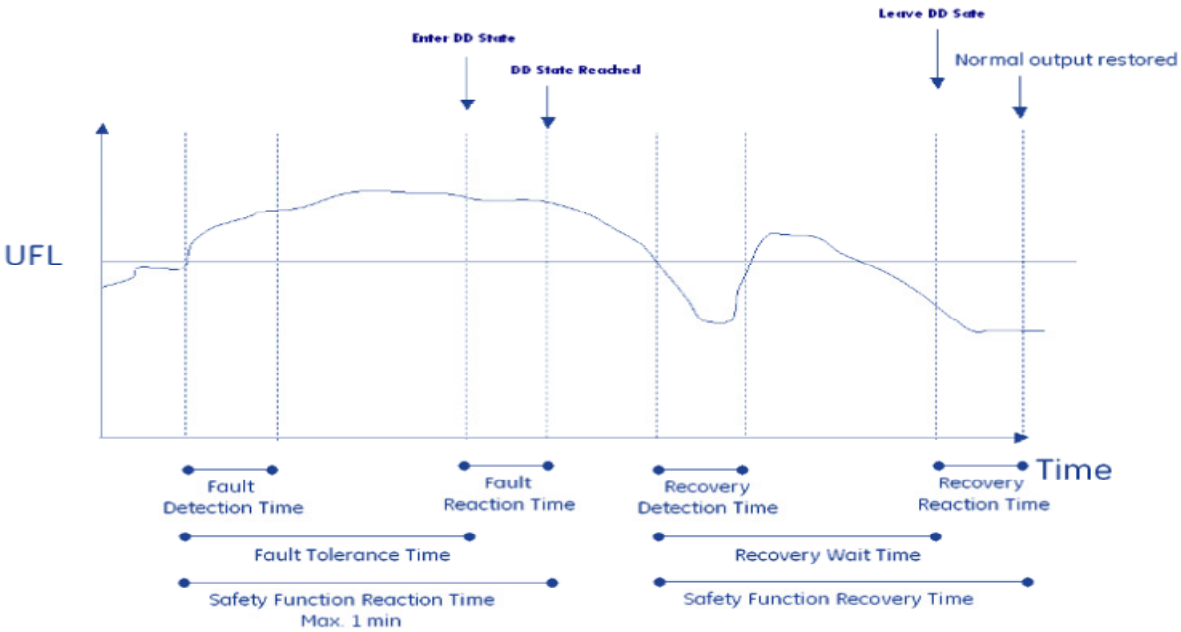


Figure 4: Timing constraints

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

The sum of fault detection time and fault reaction time of the PanaFlow shall be shorter than the Safety Function Reaction Time.

7.3 Safety architecture

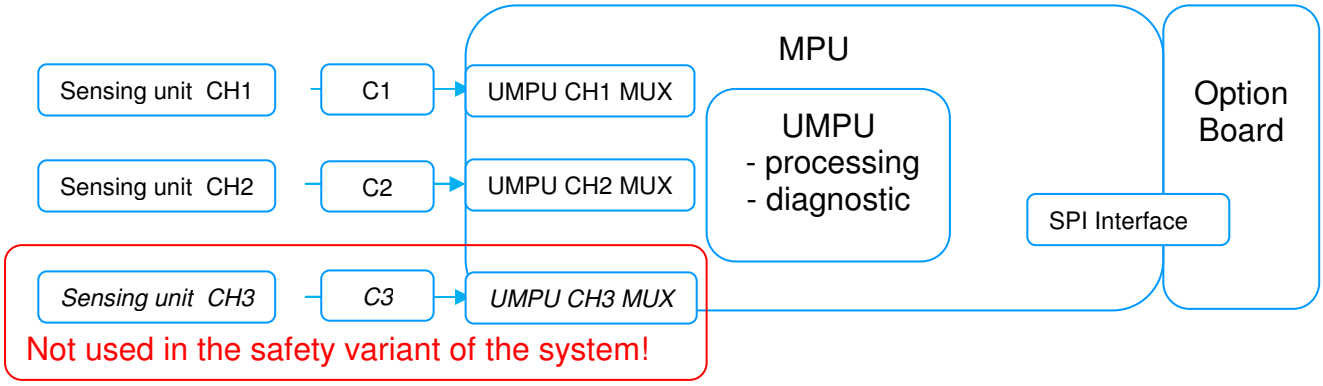


Figure 5: UMPU physical structure

The physical structure of the UMPU is shown in Figure 5 consisting of three ultrasonic transducer channels (only UMPU CH1 MUX and UMPU CH2 MUX are used in the safety variant of the system), the measurement processing unit and the option board. The channel multiplexers of the UMPU system can be considered as part of sensor channel chain. One ultrasonic sensing unit consists of two transducers.

The UMPU-system to be assessed as either one or two safety relevant channels.

In the following the different possibility of sensor voting are mentioned.

7.3.1 Sensor 1oo1 – MPU and Option Board 1oo1 – Configuration #1

Sensing unit 1 – C1 – UMPU CH1 MUX Sensing unit 2 – C2 – UMPU CH2 MUX	UMPU - processing - diagnostic	Option Board

Figure 6: 1oo1 architecture two sensors, MPU and Option Board

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

The safety architecture (Figure 6) considers the UMPU measurement system with two input channels including the sensor elements and the processing logic and the option board as a 1oo1 structure.

7.3.2 Sensor 1oo1 – MPU and Option Board 1oo1 - Configuration #2

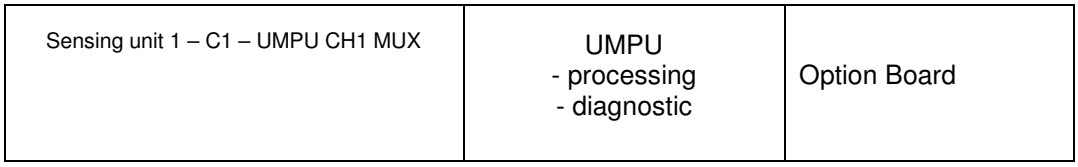


Figure 7: 1oo1 architecture one sensor, MPU and Option Board

The safety architecture (Figure 6) considers the UMPU measurement system with one input channels including the sensor elements and the processing logic and the option board as a 1oo1 structure.

7.3.3 Further configuration possibilities – Reaching SIL 3

If more PanaFlow HT flow measurement systems (including transducers, UMPU and option board) are used in a configuration where the Hardware Fault Tolerance is greater then 1, SIL 3 can be reached because the SW has been developed according to SIL 3. This is based on IEC 61508 part 2, section 7.4.4.2.4.

That means if e.g. two PanaFlow HT flow measurement systems are used in a 1oo2 architecture SIL 3 can be reached. Please note that also the PFH and/or PFD_{avg} have to be calculated to show that SIL 3 can be reached in the used architecture.

7.4 Safety Integrity

The relevant safety requirements of PanaFlow HT are documented in the corresponding SRS [1].

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

The applied techniques and measures to preserve safety integrity in HW and SW development are documented in the V&V plan [2].

7.4.1 Safety properties

The safety properties (SP) for the safety functions are defined in [1].

No.	Safety Property	Description
1.	Mode of operation related to safety function	Depends on the application where the PanaFlow HT is used. For certification High and Low Demand Mode are considered.
2.	Safety Integrity Level HW	SIL 2
3.	Safety Integrity Level SW	SIL 3
4.	Safety critical input (UMPU)	Analogue signal - acoustic transit time
5.	Safety critical output	4-20mA output
6.	Type	The system shall be considered a Type B = Complex System with software
7.	Safe failure fraction	SFF >= 90%
8.	PFH for SIL 2 PFD_{avg} for SIL 2	$\geq 10^{-7}$ to $< 10^{-6}$ $\geq 10^{-3}$ to $< 10^{-2}$
9.	Architecture and HFT	1oo1D; HFT = 0
10.	Life time	20 years

Table 3: Safety properties (SP)

7.4.2 Maximum tolerable PFH and PFD_{avg} values for the PanaFlow HT

PFH/PFD_{avg} needs to be distributed to all parts of a whole safety loop according to their corresponding proportion within the application (sensor, logic unit, actuator – see the following figure).

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

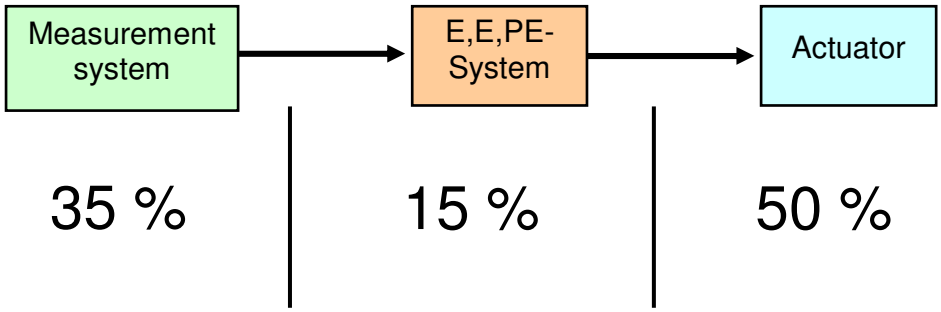


Figure 8: Failure distribution for a safety loop

The PanaFlow HT is the measurement part in a safety loop. Therefore 35% of the failure rate is available for the PanaFlow HT.

35 % failure from total SIL2 limit:

$$PFH_{Gen,total} \leq 350 \text{ FIT}.$$

$$PFD_{avg\_Gen\_total} \leq 3{,}5\ 10^{-3}$$

For the PanaFlow HT GE has specified the following distribution of the failure rate.

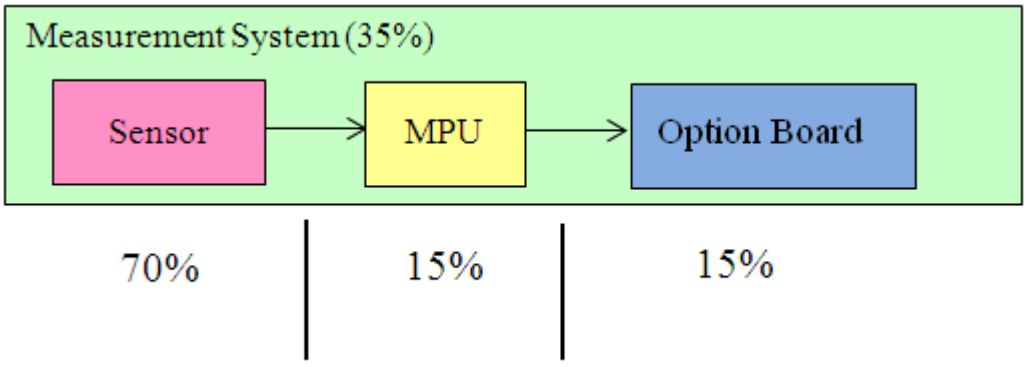


Figure 9: Failure distribution of the PanaFlow HT

So 15% of the measurement system are for the MPU and 15% for the option board

Therefore these threshold values must be reached.

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

Measurement part	Threshold PFH value	Threshold PFD_{avg} value
MPU	$PFH_{MPU} \leq 52,5$ FIT	$PFD_{avg\_MPU} \leq 5,25\ 10^{-4}$
Option Board	$PFH_{OB} \leq 52,5$ FIT	$PFD_{avg\_OB} \leq 5,25\ 10^{-4}$
Ultrasonic Sensors	$PFH_{ultra} \leq 245$ FIT	$PFD_{avg\_ultra} \leq 2,45\ 10^{-3}$

Table 4: Maximum tolerable PFH and PFD_{avg} values

7.4.3 Measures for avoidance and control of (systematic) software failures

The requirements and principles for avoidance of systematic failures for the development of safety relevant SW are documented in the V&V-Plan (see [2]).

Such requirements and measures are e.g.

- Usage of relevant definitions of QM-System of GE
- Definition of requirements and specification and implementation of traceability, tool based (Polarion),
- Verification- and validation planning
- Safety development SW life cycle defined
- Usage of tool based SW design methods incl. reviews and documentation (Artisan Studio)
- Usage of version- and configuration management (OpenGE)
- Usage of programming- and documentation guidelines incl. defensive and safety related programming (coding standard)
- The software is written in C and will be analysed by static test tools.
- Software self monitoring, means protection of safety critical data by plausibility checks and checksum encoding,

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

7.4.4 Measures for avoidance and detection of random hardware failures

The requirements and measurements for avoidance of random HW failures as follows are documented in the V&V Plan [2]:

- Usage of components with low failure rates,
- De-rating of all HW elements,
- Safety related design: failure of components lead preponderantly to a safe state,
- Safety trained developers,
- ROM-Tests
- Reading back the 4..20mA output
- RAM Failure detection by complete sequential RAM tests (periodical and at start-up)
- periodically trigger the external WDT,

7.4.5 Measures to avoid and control systematic HW-failures

Planned and used measurements in the V&V Plan [2] for avoidance of systematic failures in HW are e.g.:

- Usage of relevant definitions of QM-System of GE
- Measurements for avoidance of failures as well as techniques and measurements to control systematic faults caused by environmental stress or influences,
- Tool based definitions of requirements and specifications of high quality and implementation of traceability, (Polarion)
- Hardware development life cycle defined
- Usage of version- and configuration management (OpenGE)
- Verification- and validation planning
- Usage of tool based HW design methods incl. reviews and documentation

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

7.5 HW and FW Version

The assessment is valid for the HW and FW Versions listed in the following table:

HW Transducer	XD-170 Rev. D XD-173 Rev. D
HW UMPU board	710-1565 Rev. A 710-1566 Rev. A
HW option board	710-1615 Rev. B
FW Version (UMPU)	2830

Table 5: Version of HW and FW

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

8 Assessment activities

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

1. Functional safety
    - 1.1 Quality-Management und Management of functional safety
    - 1.2 system and concept
    - 1.3 Development of HW
    - 1.4 Failure Mode and Effect Analysis (FMEDA) with calculation of λ-values, SFF and PFH-value
    - 1.5 Development of FW
    - 1.6 Factory inspection
    - 1.7 Safety related information in Installation- and operating manual
2. Environmental influences
    - a. Climatic and temperature influence
    - b. Mechanical influence
3. EMC
    - a. Electromagnetic influence
    - b. Electromagnetic radiation

The documentation of the safety related development of GE includes documents from the areas QM-system, system-level, HW and FW.

The documents provided by the manufacturer in its valid version will be listed in a summarizing document list included in the V&V Plan [2].

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

9 Assessment

The safety related development of the GE PanaFlow HT flow measurement system was assessed on the base of the documents listed in chapter 4.

The assessment of PanaFlow HT has been carried out with the main focus, how far the traceable documented results are able to fulfil the requirements according to functional safety and their management and that the relevant phases of the safety life cycle have been performed sufficiently.

The base for the assessment is the standard IEC 61508 SIL 2 for HW and IEC 61508 SIL 3 for SW. The following documentation of the assessment and its results is structured in two parts:

- Management of functional safety and
- Technical specifications.

The basic management of functional safety for this product is documented in the safety plan [6]. The related processes ([7] - [14], [17] - [20] and [22]) are implemented within GE and have been applied during development of the PanaFlow HT. The technical specifications are described in the documents [1] - [5], [24] - [24], [26] and [42].

GE uses the Requirement Tool Polarion. Therefore the safety related requirements are marked clearly and unique and the derived measurements are sufficiently traceable. Forward- and backward traceability is used / supported respectively by using Polarion.

9.1 Quality-Management and Functional Safety Management

The quality management system applied for the development of the PanaFlow HT is process oriented.

Policy and strategy for achieving functional safety and the means for a culture of safe working are visible.

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

In the safety plan [6] the processes for achieving functional safety are described or referenced. The referenced processes ([7] - [14], [17] - [20] and [22]) have also been assessed (see [78]). In combination with the V&V Plan [2] the safety plan include all management and technical activities of the safety related system, that are necessary to achieve, assess and maintain the required functional safety.

Functional Safety Management Audits in the context of ISO 9001:2008 internal audits will be done periodically to consolidate Functional safety management and to secure the usage and application of the relevant related documents. These are the basis to achieve functional safety during the whole safety life cycle.

Result of assessment:

Policy and strategy for achieving functional safety and the means for a culture of safe working are visible and supported by FSM audits.

In the safety plan [6] the definition of functional safety management are carried out. The safety plan and the related processes ([7] - [14], [17] - [20] and [22]) as wells as the V&V Plan [2] include all management and technical activities of the safety related system, that are necessary to achieve, assess and maintain the required functional safety.

9.1.1 Functional Safety Management Plan und Safety Development Life Cycle

All management and technical activities within the safety life cycle and its phases to be applied are defined by the manufacturer in the safety plan [6] and V&V plan [2] to achieve and maintain the required functional safety according to SIL 2 for HW and SIL 3 for SW for the safety function.

In the V&V plan in table “Human Resources” the roles and responsibilities of the persons working in the project are outlined.

Persons concerned with the safety related life cycle are competent on the base of their education and experience, especially from activities in the context of safety engineering, to carry out the requested works with responsibility.

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

The adequate documentations of the techniques and measurements to control random and systematic failures are listed in two sheets of the V&V plan (the HW Measures and the SW Measures).

Selected tools are documented with a rating of the criticality of safety impact and qualified in accordance with IEC 61508-3 chapter 7.4.4. E.g. for the compiler (a tool that has been voted as “high critical”) a list of projects, where the compiler was successfully used is available. Some tools are “proven in use” according to their application in different projects.

The process of agreement and authorisation of changes and requirements for management of faults is applied.

The requirements for operation and maintenance as well as the requirements for installation and commissioning are integrated in the SRS [1].

The usage and the evidence of the system for the management of functional safety (incl. measurements to control changes, identification of products, control of documents) the process of development with its results of the single steps are described in the safety plan and will be developed further.

The validation and verification activities are documented.

The safety life cycle of the IEC 61508 with its activities and definitions is the base of the phases of the safety lifecycle for the development of the PanaFlow HT. The safety life cycle is structured systematically. The safety plan and V&V plan contains in addition to the planned activities the references on the results (output). The relevant results are documented according to the different phases and levels (system, HW and FW) of development. Milestones for verification and validation of the relevant results are defined for all phases of the SLC. The application was assessed by a review of QM-documents (see [78]) and an audit on 2012-02-03 in Billerica (see [85]).

The structure of the documentation of the project and for the management of functional safety is documented.

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

Selected measurements, techniques and tools are documented or referenced. The main principle techniques (methods and measurements) used are the “classical” methods of test, review and inspection.

For the processing of complaints as well as dangerous incidents caused by the product, procedures are defined or referenced in the safety plan.

Procedures for version-, configuration- and change (request-) management are described or referenced.

Result of assessment:

The requirements of IEC 61508 to avoid systematic failures by the planned measurements in the safety relevant processes for the management of functional safety and their implementation and application, the structure of documentations, as well as the structure of the applied QM-System in the context of the project are adequate for its purpose. The application was assessed by a review of QM-documents (see [78]) and an audit on 2012-02-03 in Billerica (see [85]).

9.1.2 Planning for verification and validation

In each phase of the development of a safety related system it is necessary according to IEC 61508, to carry out a verification process. The verification shall show that the result of a phase fulfils the requirements of specifications and design.

The validation shall identify problems related to the specification and the developed product. That concerns the end of development of the system or subsystem.

The verification and validation activities are described in the safety plan [6] in general. The planning and detailed specification of verification and validation activities is documented in e.g. [2], [29], [31] - [41], [51], [52] and [55]. These plans and specifications shall assure that all activities for verification and validation with its responsibilities are carried out. The methods and techniques for verification and validation are described or referenced in the safety plan [6] and overall V&V plan [2].

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

Result of assessment:

The planning and specification of verification and validation activities is sufficient and did not give rise to any safety objections.

9.1.3 Evidence of activities for verification and validation

Evidence to the activities according to the verification and validation plan is mostly documented directly in the specification documents. The documents (as e.g. [31], [32], [34], [41], [54], [55], [58], [59], [60], [61], [63], [64], [71], [70], [67] and [74]) created hereby were assessed by spot tests. A review process is used.

Result of assessment:

The evidence of activities for verification and validation are adequate for its purpose. The results did not give rise to any relevant safety objections.

9.1.4 Documentation

The documentation within the development of the PanaFlow HT is structured in

- System Safety Requirements Specification
- FMEA – Failure Mode and Effects Analysis
- Safety Plan
- Verification and validation plan
- Management processes
- HW/FW Requirement Specification
- HW/FW Design Specification
- Test specifications
- FMEDA
- Verification, Validation and Test reports
- Safety and user manual

The documents to be prepared as basis for certification will be listed/ added in the V&V Plan [2]. Backward traceability will be implemented. Forward traceability is supported.

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

Result of assessment:

The available documentation (see chapter 4) is complete and sufficient.

9.2 Functional safety

9.2.1 Safety requirements specifications

The project requirements for the PanaFlow HT are documented in the SRS [1]. The safety relevant requirements include the objective of development, standards and guidelines which have to be applied, requirements to external interfaces and system properties. All requirements are handled in the requirement management tool “Polarion”. Traceability is visible “linking” the derived requirements by unique ID numbers. The requirements are refined in the HW/FW requirement specification ([24] and [25]) and then again in the HW/FW design specification ([26] and [42]).

Result of assessment:

The SRS [1] and the resulting documents were assessed according to consistency related to the basis of certification and traced and assessed according to its comprehensibility of the derived specific requirements. With the requirement management in “Polarion” it is possible to handle the requirement traceable up to the check in the final validation phase. The results did not give rise to any relevant safety objections.

9.2.2 Analysis of the safety related system concept

Objective of the system – FMEA is the detection of weaknesses of the architecture on system level which are safety critical according to their impact on functional safety. Failures have been assumed for the several subsystems and components. The consequences for safety have been analysed and considered whether they are controlled and where necessary requirements and measurements have been derived.

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

With the System-FMEAs (Ultrasonic MPU [4] and Option Board [5]) and the derived requirements and measurements was shown, that the specifications can fulfil the requirements according to IEC 61508 SIL 2.

To evaluate the probability of a dangerous failure for the system a calculation of PFH and PFD_{avg} will be done in the context of the assessment and certification (see below).

Result of assessment:

The theoretical FMEAs on system level, carried out by GE were reviewed. The analysis of the system concept of the PanaFlow HT shows, that SIL 2 according to IEC 61508 can be fulfilled in principle. The requirements for the architecture are presented complete, consistent and comprehensive.

9.2.3 Assessment of functional safety in hardware

For the development of the HW the safety life cycle of IEC 61508 has been used.

The HW design and its implementation have been analyzed.

The measures for avoidance, detection and control of systematic and random failures of hardware are described in the V&V Plan [2] and in the chapters 7.4.4 and 7.4.5.

An analysis of the HW was done in terms of FMEDAs (see [77]). Verification and Validation activities as well as tests of HW have been planned and executed (see also chapter 9.5).

Result of assessment:

The analysis of the HW design and its implementation did not give rise to any relevant safety objections. The planned and realized measures to prevent, detect and control random and systematic HW failures are sufficient. The HW is systematic capable up to SIL 2 according to IEC 61508.

9.2.4 Assessment of functional safety in Firmware

For the development of the FW the safety lifecycle of IEC 61508 has been used.

The FW design and its implementation have been analyzed.

The measures for safety integrity in the FW are documented in the V&V plan [2]. The measures for avoidance, detection and control of systematic failures of Software are also described in chapter 7.4.3.

Tests of FW have been planned and executed with LDRA Tool.

All offline support tools have been assessed according to IEC 61508-3 (see [2]).

Result of assessment:

The analysis of the FW design and its implementation did not give rise to any relevant safety objections. The planned and realized measures to prevent, detect and control systematic FW failures are sufficient. The FW is systematic capable up to SIL 3 according to IEC 61508.

9.3 Calculation of the quantitative results

The company GE determines the quantitative parameters required by IEC 61508 with the help of a FMEDA for the HW of the PanaFlow HT UMPU board and option board. The purpose of the requirements of IEC 61508 is amongst others to prevent, detect and control failures in systems or sub systems and to limit the probability of dangerous failures to defined values. Using mathematical models and calculation methods the residual error rate (**P**robability **F**ailures per **H**our; PFH) can be determined as a function of hardware architecture and a specified useful life of an electronic system. The failure rates of the used electronic components were taken from the reliability data handbook IEC 62380 and SN 29500 entered into an Excel list and checked for plausibility.

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

9.3.1 Quantitative requirements

The quantitative requirements for the measurement system are listed in chapter 7.4.

9.3.2 Assessment results

9.3.2.1 Safety relevant sensing

The ultrasonic transducer has been assessed in a proven in use assessment according to IEC 61508 SIL 2. See therefore the technical report of the assessment [80].

In the following table the determined λ-values, SFF and DC are pictured.

Sensing Device	λ_{du} [Fit]	λ_{dd} [Fit]	SFF [%]	DC [%]
Ultrasonic 1 transducer	11,27	123,93	92	92
1 sensing unit (transducer pair)	22,54	247,86	92	92
2 sensing units (2 transducer pairs)	45,08	495,72	92	92

Table 6: Quantitative results sensors

The estimated DC is only an assumption due to the categorization of the failures in the proven in use assessment of the ultrasonic sensing device.

One sensing unit always consist of two transducers so for the further assessment the values for 2 transducers given in Table 6 are taken.

In worst case calculation four safety relevant transducers are used in 1oo1 architecture.

Tests have shown that all the failures which have been categorized as dangerous detected in the proven in use assessment in [80] could be detected by the ultrasonic measurement process unit.

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

9.3.2.2 Measurement process unit and cabling

For the UMPU Board and the cabling GE has executed a FMEDA [77] in cooperation with TÜV NORD Systems. The results are documented in the corresponding report [82] and are adopted and accepted. In the following table the λ-values, SFF and DC of the UMPU board and cabling are pictured.

Device	λ_{su} [Fit]	λ_{sd} [Fit]	λ_{du} [Fit]	λ_{dd} [Fit]	SFF [%]	DC [%]
Measurement unit	52,49	174,39	3,98	17,05	98,4	81
Cable Harness Assy	0,52	4,68	0,52	4,68	95	90

Table 7: Quantitative results MPU and Cabling

9.3.2.3 Option board

For the Option Board GE has also executed a FMEDA [77] in cooperation with TÜV NORD Systems. The results are documented in the corresponding report [83] and are adopted and accepted. In the following table the λ-values, SFF and DC of the option board are pictured.

Device	λ_{su} [Fit]	λ_{sd} [Fit]	λ_{du} [Fit]	λ_{dd} [Fit]	SFF [%]	DC [%]
Output circuit	8,72	223,70	2,33	230,59	99,5	99

Table 8: Quantitative results option board

9.3.2.4 PanaFlow HT

Considering the two configuration possibilities described in the chapters 7.3.1 and 7.3.2 you reach for the complete PanaFlow HT ultrasonic measurement system (configuration 1 and 2) the following λ-values, SFF and DC:

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

Device	λ_{su} [Fit]	λ_{sd} [Fit]	λ_{du} [Fit]	λ_{dd} [Fit]	SFF [%]	DC [%]
PanaFlow HT configuration 1 with 2 sensing units	61,73	402,77	51,91	749,04	95,9	93,5
PanaFlow HT configuration 2 with 1 sensing unit	61,73	402,77	29,37	501,18	97,1	94,6

Table 9: Quantitative results PanaFlow HT

The PanaFlow HT has a 1oo1 architecture and therefore a HFT = 0.

For the calculation of the PFH and PFD_{avg} the Mean Repair Time MRT = 24h, the Mean Time to Restoration MTTR = 24h and the Life Time T_1 = 175200h. In addition it is assumed that 50% of the λ_{du} failures can be found in the Proof-Test Interval of 8760h which is described in the user documentation [72] and [73]. The calculations are documented in [87].

This will lead to the following PFH and PFD_{avg} values

Device	PFH	PFD_{avg}
PanaFlow HT configuration 1 with 2 sensing units	5,19e-8	2,41e-3
PanaFlow HT configuration 2 with 1 sensing unit	2,94e-8	1,36e-3

Table 10: PFH and PFDavg for PanaFlow HT 1oo1 architecture

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

If the PanaFlow HT is used in a 1oo2 architecture (HFT = 1) and a common cause factor of 10% is assumed. The following PFH and PFD_{avg} values can be achieved.

Device	PFH	PFD_{avg}
PanaFlow HT configuration 1 with 2 sensing units	5,29e-9	2,46e-4
PanaFlow HT configuration 2 with 1 sensing unit	2,97e-9	1,38e-4

Table 11: PFH and PFDavg for PanaFlow HT 1oo2 architecture

9.3.2.5 Overall quantitative result

The proven in use assessment of the sensing unit and the FMEDAs of the UMPU board, the cabling and the option board have been executed by TÜV NORD Systems. The results are adopted and accepted.

The PanaFlow HT fulfils in configuration 1 and 2 in 1oo1 architecture the quantitative requirements to the SFF, PFH and PFD_{avg} for SIL 2 according to IEC 61508.

In addition the PanaFlow HT fulfils in configuration 1 and 2 in 1oo2 architecture the quantitative requirements to the SFF, PFH and PFD_{avg} for SIL 3 according to IEC 61508.

9.4 Environmental Influences, EMC

The tests related to the environmental influences and EMC have been carried out to show that they have no influence on functional safety.

The test plan and test results for environmental and EMC tests are documented in [39], [40] and [41].

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

Result of assessment:

The tests carried out did not give rise to any safety objections.

9.5 Testing

The tests of SW and HW have been systematically planned ([29], [31] - [41], [51], [52] and [55]), performed and documented ([31], [32], [34], [41], [54], [55], [58], [59], [60], [61], [63], [64], [71], [70], [67] and [74]). The tested requirements are traceable by unique labels for system test purposes. Therefore traceable evidence is available that requirements are verified and validated by adequate testing activities. This is visible for the different phases of V-model with its verification and validation activities like field-, system- module- and integration tests. The coverage of module testing is considered. Testing activities are supported by commercial tools (e.g. LDRA). The test reports are also subject to approval and release.

The testing activities concern not only dynamic, but also static testing (e.g. documented reviews incl. subsequent edit activities).

Result of assessment:

For the safety relevant requirements measurements for testing activities are planned, implemented and traceable. The evidence of traceability is supported by unique labelling of the requirements. The relevant HW- and SW-Tests according to the state of the project have been done. The HW- and SW-development process is supported strongly by the performed system- and subsystem and integration tests. The test definitions are sufficient to prove compliance with the standard. The results did not give rise to any relevant safety objections and are accepted.

9.6 Checklists

The fulfillment of the requirement of IEC 61508 was assessed by using an excel based requirement checklist [84].

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

Result of assessment:

The checklist for IEC 61508 proves that all requirements are sufficiently fulfilled.

9.7 Factory Inspection

The manufacturing process of GE in Billerica, USA has been inspected at the meeting on 2012-02-03. The results are documented in the inspection report [86].

Result of assessment:

The results of the factory inspection did not give any safety objections.

9.8 Safety relevant user documentation

The safety relevant user documentation in terms of user manual [72] and safety manual [73] have been reviewed (see [78]).

Result of assessment:

The assessment did not give any safety objections. The users of the system have to follow the instructions given in the manuals.

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

10 Result Summary

The documents provided by the manufacturer have been reviewed and are accepted.

Policy and strategy for achieving functional safety and the means for a culture of safe working are visible and supported by FSM audits.

In the safety plan [6] the definition of functional safety management are carried out. The safety plan and the related processes ([7] - [14], [17] - [20] and [22]) as well as the V&V Plan [2] include all management and technical activities of the safety related system, that are necessary to achieve, assess and maintain the required functional safety.

The requirements of IEC 61508 to avoid systematic failures by the planned measurements in the safety relevant processes for the management of functional safety and their implementation and application, the structure of documentations, as well as the structure of the applied QM-System in the context of the project are adequate for its purpose. The application was assessed by a review of QM-documents (see [78]) and an audit on 2012-02-03 in Billerica (see [85]).

The planning and specification as well as the evidence of verification and validation activities are adequate for its purpose and did not give rise to any safety objections.

The available documentation (see chapter 4) is complete and sufficient.

The SRS [1] and the resulting documents were assessed according to consistency related to the basis of certification and traced and assessed according to its comprehensibility of the derived specific requirements. With the requirement management in “Polarion” it is possible to handle the requirement traceable up to the check in the final validation phase. The results did not give rise to any relevant safety objections.

The theoretical FMEAs on system level, carried out by GE were reviewed. The analysis of the system concept of the PanaFlow HT shows, that SIL 2 according to IEC 61508 can be fulfilled in principle. The requirements for the architecture are presented complete, consistent and comprehensive.

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

The analysis of the HW design and its implementation did not give rise to any relevant safety objections. The planned and realized measures to prevent, detect and control random and systematic HW failures are sufficient. The HW is systematic capable up to SIL 2 according to IEC 61508.

The analysis of the FW design and its implementation did not give rise to any relevant safety objections. The planned and realized measures to prevent, detect and control systematic FW failures are sufficient. The FW is systematic capable up to SIL 3 according to IEC 61508.

The proven in use assessment of the sensing unit and the FMEDAs of the UMPU board, the cabling and the option board have been executed by TÜV NORD Systems. The results are adopted and accepted.

The PanaFlow HT fulfils in configuration 1 and 2 in 1oo1 architecture the quantitative requirements to the SFF, PFH and PFD_{avg} for SIL 2 according to IEC 61508.

In addition the PanaFlow HT fulfils in configuration 1 and 2 in 1oo2 architecture the quantitative requirements to the SFF, PFH and PFD_{avg} for SIL 3 according to IEC 61508.

The tests related to the environmental influences and EMC have been carried out and did not give rise to any safety objections.

For the safety relevant requirements measurements for testing activities are planned, implemented and traceable. The evidence of traceability is supported by unique labelling of the requirements. The relevant HW- and SW-Tests according to the state of the project have been done. The HW- and SW-development process is supported strongly by the performed system- and subsystem and integration tests. The test definitions are sufficient to prove compliance with the standard. The results did not give rise to any relevant safety objections and are accepted.

The checklist for IEC 61508 proves that all requirements are sufficiently fulfilled.

The manufacturing process of GE in Billerica, USA has been inspected at the meeting on 2012-02-03. The results of the factory inspection did not give any safety objections.

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

The safety relevant user documentation in terms of user manual [72] and safety manual [73] have been reviewed and did not give rise to any safety objections.

The users of the system have to follow the instructions given in the manuals.

The assessment of the PanaFlow HT carried out by TÜV NORD Systems has shown that the system fulfils SIL 2 according to IEC 61508 in 1oo1 configuration and can reach SIL 3 in e.g. a 1oo2 configuration.

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