



IEC 61508 Functional Safety Assessment

Project:

ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter

Customer:

ABB

Shanghai, China

Contract No.: Q14/02-077

Report No.: ABB 08-03-49 R001

Version V3, Revision R1, August 25, 2017

Desmond Lee, Ted Stewart

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

© All rights reserved.



Management Summary

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

ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter

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

- *exida* assessed the development process used by ABB through an audit and creation of a detailed safety case against the requirements of IEC 61508.
- *exida* 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. A full IEC 61508 Safety Case was prepared, using the *exida* SafetyCaseDB™ tool, and used as the primary audit tool. 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 ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter was found to meet the requirements of SIL 2, single use (HFT = 0) and SIL 3, redundant use (HFT = 1).

The manufacturer will be entitled to use the Functional Safety Logo.

Manufacturing Facilities are located in Warminster, PA and Shanghai, China.

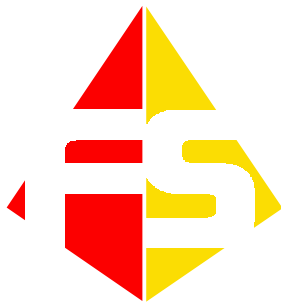


Table of Contents

Management Summary	2
1 Purpose and Scope	4
2 Project management.....	5
2.1 exida.....	5
2.2 Roles of the parties involved.....	5
2.3 Standards / Literature used	5
2.4 Reference documents	5
2.4.1 Documentation provided by ABB	5
2.4.2 Documentation generated by exida.....	10
3 Product Description.....	11
3.1 Scope of Analysis.....	12
4 IEC 61508 Functional Safety Assessment.....	13
4.1 Methodology.....	13
4.2 Assessment level	13
5 Results of the IEC 61508 Functional Safety Assessment	15
5.1 Lifecycle Activities and Fault Avoidance Measures.....	15
5.1.1 Functional Safety Management	15
5.1.2 Safety Requirements Specification and Architecture Design.....	16
5.1.3 Hardware Design	16
5.1.4 Software Design	16
5.1.5 Validation.....	17
5.1.6 Verification.....	17
5.1.7 Modifications.....	17
5.1.8 User documentation.....	17
5.2 Hardware Assessment	19
6 Terms and Definitions	20
7 Status of the document.....	21
7.1 Liability	21
7.2 Releases	21
7.3 Future Enhancements	21
7.4 Release Signatures	21

1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter. The results of this assessment provide 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 report is a result of a renewal assessment review for the ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter. The assessment has been carried out based on the quality procedures and scope definitions of *exida*.

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 partnership 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.

exida is the market leader for IEC 61508 certification for currently active marketed products.

2.2 Roles of the parties involved

ABB	Manufacturer of the ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter
<i>exida</i>	Provided services to support ABB during the development of the ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter.
<i>exida</i>	Performed the IEC 61508 Functional Safety Assessment according to option 3 (see section 1)

ABB contracted *exida* with the IEC 61508 Functional Safety Assessment of the above mentioned devices.

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 ABB

[D1]	Safety Case	ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter Safety Case
[D2]	QMP-0003L	Quality Management Plan Procedure, Control of Documents
[D3]	QMP-0008D	Quality Management Plan Procedure, Design & Development
[D4]	QMP-0010D	Quality Management Plan Procedure, Supplier Selection and Evaluation
[D5]	QMP-0018C	Quality Management Plan Procedure, Control and Monitoring of Measuring Devices

[D6]	QMP-0023G	Quality Management Plan Procedure, Control of Nonconforming Products
[D7]	QMP-0026B	Quality Management Plan Procedure, Corrective and Preventive Action
[D8]	PRC0077A	Quality Procedure, Software Coding & Style Guidelines
[D9]	PRC0078A	Quality Procedure, Software Design & Development Procedure
[D10]	PRC0079C	Quality Procedure, Functional Safety Management Plan
[D11]	PRC0080A	Quality Procedure, Safety Requirements Review Checklist
[D12]	PRC0081	Quality Procedure, Safety Critical Tools Qualification
[D13]	PRC0082C	Quality Procedure, R&D Group Qualification Record
[D14]	FRM-0708	Design Project Records
[D15]	PNP-0000-1PL	Template for Top Level Parts List & Construction Table
[D16]	PNP-0000-1	Template for General Arrangement Drawings
[D17]	PNP-0320-1	Template for Safety Requirements Specifications
[D18]	PNP-0330-1	Template for Integration & Validation Test Plan
[D19]	PNP-0350-1	Template for Functional Safety Documentation Checklists
[D20]	PNP-0362-1	Template for Impact Analysis
[D21]	PNP-0364-1	Template for Modification & Change of Design Project Records
[D22]	PNP-0370-1A	Template for Architecture Design Overview High Level UML & Sub Assemblies
[D23]	PNP-0372-1	Template for Hardware Design
[D24]	PNP-0376-1	Template for Software Configuration Record
[D25]	PNP-0378-1	Template for Software Design Review
[D26]	PNP-0380-1	Template for Software & Critical Code Review
[D27]	PNP-0382-1	Template for Architecture Design & SW HW Interface Review
[D28]	PNP-0384-1	Template for Safety Requirements Review per PRC0080 Checklist
[D29]	PNP-0388-1	Template for Safety Integration & Validation Test Plan Review
[D30]	PNP-0389-1	Template for Safety Manual Review
[D31]	PNP-0390-1	Template for Integration & Validation Testing
[D32]	GWI-0001H	General Work Instruction, General Documentation Numbering System
[D33]	GWI-0002F	General Work Instruction, Product Specific Numbering System

[D34]	FRM-0708b_08-001	AT Accutrak SIL 2 Design Project Records EF 05-20-2008
[D35]	AT100-0202-1j	AT100 datasheet
[D36]	AT100S-0202-1h	AT100S datasheet
[D37]	AT200-0202-1j	AT200 datasheet
[D38]	AT100-0200-1 Rev J	Draft (Safety) Manual AT100, AT100S
[D39]	AT200-0200-1 Rev I	Draft (Safety) Manual AT200
[D40]	AT100-0320-1a	R&D Document, AT100 Series Safety Requirements Specifications
[D41]	AT100-0330-1b	R&D Document, Accutrak AT100 AT100S AT200 Validation Test Plan
[D42]	AT100-0332-1a	R&D Document, AT100 Series Project & Configuration Management Plan
[D43]	AT100-0360-1	R&D Document, Software Criticality Analysis & HAZOP
[D44]	AT100-0362-1	R&D Document, Impact Analysis
[D45]	AT100-0370-1	R&D Document, Architecture Design Overview AT H070515 Software Interface
[D46]	AT100-0370-2	R&D Document, Architecture Design Overview AT100 AT100S AT200 SIL Certification
[D47]	AT100-0372-2	R&D Document, Hardware Design
[D48]	AT100-0374-2	R&D Document, Detailed module Design 05-20-2008
[D49]	AT100-0376-1	R&D Document, AT100 AT100S & AT200 Software Configuration Record
[D50]	AT100-0376-2	R&D Document, AT100 AT100S & AT200 Software Configuration Record
[D51]	AT100-0378-1	R&D Document, Software Design Review
[D52]	AT100-0380-1	R&D Document, Software & Critical Code Review
[D53]	AT100-0382-1a	R&D Document, Architecture Design & SW HW Interface Review
[D54]	AT100-0384-1	R&D Document, AT100 Series Safety Requirements Review
[D55]	AT100-0386-1	R&D Document, Software Safety Design Component Diagram UML
[D56]	AT100-0386-2a	R&D Document, Software Safety Design Diagram UML
[D57]	AT100-0388-1	R&D Document, Safety Integration & Validation Test Plan Review
[D58]	AT100-0389-1	R&D Document, Safety Manual Review
[D59]	AT100-0390-1	R&D Document, Accutrak AT100 AT100S AT200 Validation Testing

[D60]	AT100-0510-1	R&D Document,08-001 Software Records Static Analysis
[D61]	AT100-0512-1	R&D Document,08-001 Software Documentation Files Differences
[D62]	AT100-0514-1	R&D Document,08-001 Software Documentation DIAGS.C Software Checkout
[D63]	FRM-0709	Design / Development Review Minutes
[D64]	PWI-0054a	AT Series Sensor Assembly
[D65]	SPM201-5000-1PIC	Photos of SPM201-5000-1 Rev G Assembly
[D66]	KTK 08-03-49 R001	<i>Exida</i> Proven In Use Assessment, AT100, AT100S, and AT200 Magnetostrictive Level Transmitter
[D67]	KTK 08/01-09 R001, V1 R2	ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter FMEDA Report
[D68]	SPM201-4001-1A.EFM	ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter FMEDA 4001 board Spreadsheet
[D69]	SPM201-5001-1A.EFM	ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter FMEDA 5001 board Spreadsheet
[D70]	SPM201-4000-2faulttest	Fault Injection Test report for SPM201-4000-2
[D71]	SPM201-5000-1faulttest	Fault Injection Test report for SPM201-5000-1
[D72]	SPM201-6000-2faulttest	Fault Injection Test report for SPM201-6000-2
[D73]	SPM201-7000-2faulttest	Fault Injection Test report for SPM201-7000-2
[D74]	IEC 61508 tables ABB	IEC 61508 Tables, document shows all tables from IEC 61508 Annex A and B from part 2 and part 3 along with a description as to how ABB meets each of the requirements
[D75]	PMU 10, Rev G, March 5, 2013	Supply Management Procedure
[D76]	ITP 201211002, Rev 0	Inspection Test Plan, Magnetic Level Gauge
[D77]	Production Doc Package, Rev01	Production Document Package Form
[D78]	AT100-0362-5_AT100_H_&_AT100_H_TS	Impact Analysis for changes in Sept 2013
[D79]	AT100-0391-3_Accutrak_AT100_Series	Software Release Notes for changes in Sept 2013
[D80]	AT100-0362-4_AT100_H_&_AT100_H_TS	Impact Analysis for changes in May 2012

[D81]	AT100-0391- 2_Accutrak_AT100_Series	Software Release Notes for changes in May 2012
[D82]	AT100-0362- 3_AT100_H_&_AT100_H_ TS	Impact Analysis for changes in July 2011
[D83]	AT100-0391- 1_Accutrak_AT100_Series	Software Release Notes for changes in July 2011

2.4.2 Documentation generated by *exida*

[R1]	ABB 08-03-49 R001 V2R1 IEC 61508 Assessment AT100 100s 200.doc, July 30, 2014	IEC 61508 Functional Safety Assessment for ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter (This document)
[R2]	Ktek 08-01-09 R001 V1 R2 FMEDA review AT100	FMEDA Report
[R3]	ABB 17-04-002 R002 V1R1	ABB Shanghai Manufacturing Audit Report

3 Product Description

The ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter is a two-wire 4 – 20 mA smart device. It contains self-diagnostics and is programmed to send its output to a specified failure state, either high or low, upon internal detection of a failure. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable.

Figure 1 shows an overview of the main parts of the ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter and the boundary for the Failure Modes, Effects, and Diagnostic Analysis.

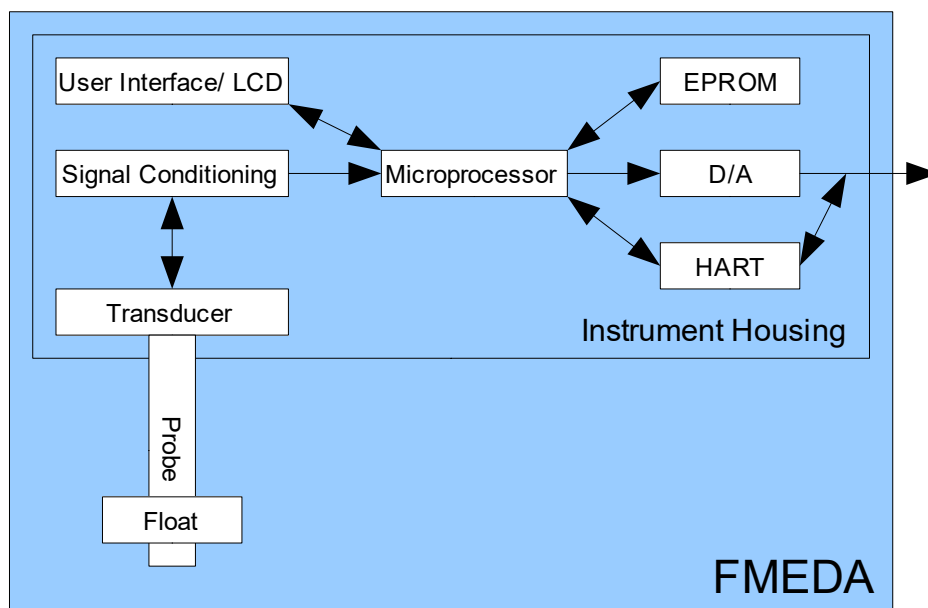


Figure 1 AT100, AT100S, AT200 SIS Assembly

Table 1 gives an overview of the different versions that were considered in the FMEDA of the ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter.

Table 1 Version Overview

AT100	Magnetostrictive Level Transmitter
AT100S	Magnetostrictive Level Transmitter, Sanitary Application
AT200	Magnetostrictive Level Transmitter, External Mounted

The ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter is classified as a Type B¹ device according to IEC 61508, having a hardware fault tolerance of 0.

¹ Type B device: “Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

3.1 Scope of Analysis

The following were considered in this analysis:

Product: AT100 Magnetostrictive Level Transmitter

Models: AT100, AT100S, AT200

Options: 4-20mA output, single output

The change history for the following versions were reviewed:

Firmware version:

AT_H_01_s002_110725; AT_H_TS_01_s002_110725

AT_H_01_s002_120501; AT_H_TS_01_s002_120501

AT_H_01_s002_130912; AT_H_TS_01_s002_130912

Hardware version:

Processor board #: SPM201-5001-1 Revision Level: A

Signal conditioning board #: SPM201-4001-1 / SPM201-4001-2 Revision Level: NC

Display board #: SPM201-7000-2 Revision Level: B

Connector board #: SPM201-3000-1 Revision Level: D

Hart Board #: SPM201-6000-1 Revision Level: D

Hardware version:

Processor board #: SPM201-5000-1 Revision Level: A

Signal conditioning board #: SPM201-4000-2 Revision Level: NC

Display board #: SPM201-7000-2 Revision Level: B

Connector board #: SPM201-3000-1 Revision Level: D

Hart Board #: SPM201-6000-1 Revision Level: D

4 IEC 61508 Functional Safety Assessment

The IEC 61508 Functional Safety Assessment was performed based on the information received from ABB and is documented in [D1].

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. Any requirements that have been deemed not applicable have been marked as such in the full Safety Case report, e.g. software development requirements for a product with no software.

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, documented in a Software Criticality and Software HAZOP report

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 ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter has been assessed per IEC 61508 to the following levels:

- SIL 2 capability, single use (Hardware Fault Tolerance = 0)
- SIL 3 capability, redundant use (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) according to IEC 61508. The review of changes and design functionality were assessed and continue to fulfill the objectives of the standard to meet SIL 3.

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by ABB during the product development against the objectives of IEC 61508 parts 1, 2, and 3, see [D1]. The development of the ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter was done prior to establishing of this IEC 61508 SIL 3 compliant development process. Consequently, for the evaluation of systematic fault avoidance measures, proven in use claims were considered in addition to documented artifacts identifying potential systematic weaknesses in the current design. The Safety Case was updated with project specific design documents. Future modifications to the ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter must be made per the IEC 61508 SIL 3 compliant development process.

5.1 Lifecycle Activities and Fault Avoidance Measures

ABB has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented in [D1]. Most of the ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter functionality was developed before this IEC 61508 compliant development process was in place, consequently proven in use arguments were considered for some of the systematic fault avoidance measures.

This functional safety assessment investigated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the Magnetostrictive Level Transmitter development. 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 ABB development process complies with the relevant managerial requirements of IEC 61508 SIL 3. The objectives of the standard continue to be fulfilled by the ABB functional safety management system for the safety lifecycle and overall documentation control. The relevant processes have been followed in making product changes.

5.1.1 Functional Safety Management

FSM Planning

The functional safety management of any ABB Safety Instrumented Systems Product development is governed by QMP-0008B Quality Management Plan Procedure, Design & Development [D3]. ABB has a Functional Safety Management Plan Quality Procedure, PRC0079A [D10] which is fixed but requires the creation of Design Project Records per FRM-0708 [D14] for each development which defines all of the tasks that must be done to ensure functional safety as well as the person(s) responsible for each task. These processes and the procedures referenced herein fulfill the requirements of IEC 61508 with respect to functional safety management.

Version Control

All documents are under version control as documented in [D1] and required by the Control of Documents Quality Management Plan Procedure [D2]. Design drawings and documents are also under version control. ABB uses Microsoft Source Safe for its version control.

Training, Competency recording

Personnel training records are kept in accordance with IEC 61508 requirements as documented in [D1] and PRC0082 the R&D Group Qualification Record Quality Procedure [D13]. ABB hired *exida* to be the independent assessor per IEC 61508.

5.1.2 Safety Requirements Specification and Architecture Design

As defined in [D10] and [D14], a safety requirements specification (SRS) is done for all products that must meet IEC 61508 requirements. The requirements specification contains a scope and safety requirements section. For the ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter, the SRS [D40], has been reviewed by *exida*. During the assessment, *exida* reviewed the content of the specification for completeness per the requirements of IEC 61508.

Requirements are tracked throughout the development process by the creation of derived requirements, which map the requirements to the design, and by mapping requirements to appropriate validation tests in the validation test plan [D57].

Requirements from **IEC 61508-2, Table B.1** that have been met by ABB include project management, documentation, separation of safety requirements from non-safety requirements, structured specification, inspection of the specification, semi-formal methods and checklists. [D74][D71] documents more details on how each of these requirements has been met. This meets the requirements of SIL 3.

5.1.3 Hardware Design

Hardware design, including both electrical and mechanical design, is done according to [D3], [D10] and [D14][D32]. The hardware design process includes component selection, detailed drawings and schematics, safety case documents for agency justification, a failure mode, effects and diagnostic analysis (FMEDA), an architecture design review, the creating of prototypes, and hardware verification tests.

Requirements from **IEC 61508-2, Table B.2** that have been met by ABB include observance of guidelines and standards, project management, documentation, structured design, modularization, use of well-tried components, checklists, semi-formal methods, computer aided design tools, simulation, and inspection of the specification. This meets the requirements of SIL 3.

5.1.4 Software Design

Software design is done according to [D3], [D10], [D14], [D8], and [D9][D32]. The software design process includes software interface specification [D45], detailed module design [D48], specification of configuration records [D49] and [D50], design and critical code reviews [D51] and [D52], and UML specifications [D55] and [D56].

Requirements from **IEC 61508-3, Table A.1 through A.5** that have been met by ABB include observance of guidelines and standards, project management, documentation, structured design, modularization, use of well-tried components, checklists, semi-formal methods, computer aided design tools, simulation, and inspection of the specification, selection of suitable programming language, use of a defined subset of the language, and others. This meets the requirements of SIL 3.

5.1.5 Validation

Validation Testing is done via a set of documented tests (see [D10] and [D14]). The validation tests are traceable to the Safety Requirements Specification [D40] in the validation test plan [D41]. In addition to standard Test Specification Documents, third party testing may be included as part of agency approvals. As the ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter consists of simple electrical devices with a straightforward safety function, integration testing has been limited to verifying that all diagnostics take the appropriate action when they find a problem (See [D59][D2] for more details on this testing).

Procedures are in place for corrective actions to be taken when tests fail as documented in [D1] and [D7].

Requirements from IEC **61508-2, Table B.3** that have been met by ABB include functional testing, project management, documentation, and black-box testing. Field experience and statistical testing via regression testing are not applicable. [D74] documents more details on how each of these requirements has been met. This meets the requirements of SIL 3.

Requirements from IEC **61508-2, Table B.5** that have been met by ABB include functional testing and functional testing under environmental conditions, Interference surge immunity testing, fault insertion testing, project management, documentation, static analysis, dynamic analysis, and failure analysis, expanded functional testing and black-box testing. [D74] documents more details on how each of these requirements has been met. This meets SIL 3.

5.1.6 Verification

The development and verification activities are defined in [D10] and [D14]. Verification activities include the following: Fault Injection Testing [D70], [D71], [D72], and [D73], Code Review [D52] per [D26], Checklists embedded in [D14], FMEDA [D67], and Software Criticality Analysis and HAZOP [D43]. Further verification activities are documented in [D10] and [D14] for new product development projects.

5.1.7 Modifications

Modifications are done per the ABB' IEC 61508 SIL 3 compliant development process as documented in [D5] and [D7][D9], and governed by [D14]. This meets the requirements of IEC 61508 SIL 3. The objectives of the standard continue to be fulfilled by the ABB functional safety management system for modifications. The relevant processes have been followed in making product changes.

5.1.8 User documentation

ABB updated the user manual for the ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter and incorporated the requirements for the Safety Manual, see [D38] and [D39][D46]. This (safety) manual was assessed by *exida*. 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.

Requirements from IEC **61508-2, Table B.4** that have been met by ABB include operation and maintenance instructions, user friendliness, maintenance friendliness, project management, documentation, limited operation possibilities, protection against operator mistakes, and operation only by skilled operators. [D74] documents more details on how each of these requirements has been met. This meets the requirements for SIL 3.

5.2 Hardware Assessment

To evaluate the hardware design of the ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter, a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida* for each component in the system. This is documented in [D67][D7]. The FMEDA was verified using Fault Injection Testing as part of the development, see [D70], [D71], [D72], and [D73][D41], 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 extension 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 2 lists these failure rates as reported in the FMEDA reports. The failure rates are valid for the useful life of the devices.

Table 2 Failure rates according to IEC 61508

Device	λ_{sd}	λ_{su}^2	λ_{dd}	λ_{du}	SFF ³
ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter	0 FIT	99 FIT	377 FIT	45 FIT	91.3%

For low demand SIL 2 applications the PFD_{AVG} value of the Safety Instrumented Function needs to be $\geq 10^{-3}$ and $< 10^{-2}$. The FMEDA report [D67] lists the percentage that the ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter uses of this budget for a one year proof test interval. 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 ABB AT100, AT100S, AT200 Magnetostrictive Level Transmitter meets the hardware requirements of IEC 61508 SIL 2, single use (HFT = 0) and IEC 61508 SIL 3, redundant use (HFT = 1).

² 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

³ The Safe Failure Fraction (SFF) is not displayed as this parameter needs to be evaluated for the complete final element subsystem

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 (1×10^{-9} failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HART	Highway Addressable Remote Transducer
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 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).
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: V3

Revision: R1

Version History: V3, R1: Recertification. Updated after site audit. Product remained certified to IEC 61508; 2000, DL/TES, August 25, 2017

V2, R1: Recertification. Updated documents received. Product remained certified to IEC 61508; 2000. TES, Aug 04, 2014

V1, R1: Added manufacturing locations, S. Close, March 11, 2013

V1, R0: First release; June 16, 2008

V0, R1: Internal Draft; June 04, 2008

Original Author: Iwan van Beurden

Current Author: Ted Stewart / Desmond Lee

Review: John Yozallinas

Release status: released

7.3 Future Enhancements

At request of client.

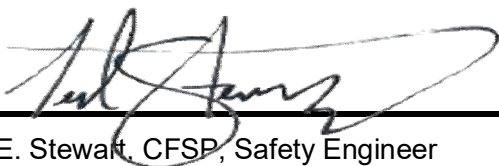
7.4 Release Signatures



Iwan van Beurden, Director of Engineering



William M. Goble, Principal Partner



Ted E. Stewart, CFSP, Safety Engineer

Desmond Lee

Desmond Lee, CFSE, Senior Safety Engineer

John C Yozallinas

John Yozallinas, CFSE, Senior Safety Engineer