

420-0004-567		Sht 1 of 15	ISSUE 1
ISSUE	EDO NO	APPD	DATE
1	2-18-114	SGA	2-23-18



IEC 61508 Functional Safety Assessment

Project:
IntelliPoint RF Series Point Level Switch

Customer:
Ametek Drexelbrook
Horsham, PA
USA

Contract Number: Q16/12-046r1
Report No.: AME 16/02-046 R002
Version V1, Revision R0, October 26, 2017
Loren Stewart



Management Summary

This report summarizes the results of the functional safety assessment according to IEC 61508 carried out on the IntelliPoint RF Series Point Level Switch

Loop	Intellipoint with 4-20mA loop power and output – model SxRNTx-x0xx-xxxx
Relay	Intellipoint with 18-200VDC or 85-250VAC power and dual relay output – model SxRNLx-x1xx-xxxx or SxRNLx-x2xx-xxxx

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

- *exida* assessed the development process used by Ametek Drexelbrook through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The investigation was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team. *exida* reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* performed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed field failure data to verify the accuracy of the FMEDA analysis.

exida reviewed the manufacturing quality system in use at Ametek. The functional safety assessment was performed to the SIL 3 requirements of IEC 61508:2010. A full IEC 61508 Safety Case was created using the *exida* Safety Case tool, which also was used as the primary audit tool. Hardware and software process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. The user documentation and safety manual also were reviewed.

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

The audited development process, as tailored and implemented by the Ametek Drexelbrook IntelliPoint RF Series Point Level Switch development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.

The assessment of the FMEDA also shows that the IntelliPoint RF Series Point Level Switch meets the requirements for architectural constraints of an element such that it can be used to implement a SIL 3 safety function (with HFT = 0) or a SIL 3 safety function (with HFT = 1).

This means that the IntelliPoint RF Series Point Level Switch is capable for use in SIL 3 applications in low demand mode when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual and when using the versions specified in this document.

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





Table of Contents

Management Summary	2
1 Purpose and Scope	5
1.1 Tools and Methods used for the assessment	5
2 Project Management	6
2.1 exida	6
2.2 Roles of the parties involved	6
2.3 Standards and literature used	6
2.4 Reference documents	6
2.4.1 Documentation provided by Ametek Drexelbrook	6
2.4.2 Documentation generated by exida	8
2.5 Assessment Approach	8
3 Product Descriptions	8
4 IEC 61508 Functional Safety Assessment Scheme	9
4.1 Product Modifications	10
5 Results of the IEC 61508 Functional Safety Assessment	11
5.1 Lifecycle Activities and Fault Avoidance Measures	11
5.1.1 Functional Safety Management	11
5.1.2 Safety Lifecycle and FSM Planning	12
5.1.3 Documentation	12
5.1.4 Configuration Management	12
5.1.5 Hardware Design / Probabilistic properties	12
5.2 Safety Manual	13
6 Terms and Definitions	14
7 Status of the document	15
7.1 Liability	15
7.2 Version History	15
7.3 Future Enhancements	15
7.4 Release Signatures	15



1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the Ametek Drexelbrook:

Loop	Intellipoint with 4-20mA loop power and output – model SxRNTx-x0xx-xxxx
Relay	Intellipoint with 18-200VDC or 85-250VAC power and dual relay output – model SxRNLx-x1xx-xxxx or SxRNLx-x2xx-xxxx

by *exida* according to accredited *exida* certification scheme which includes the requirements of IEC 61508: ed2, 2010.

The purpose of the assessment was to evaluate the compliance of:

- the IntelliPoint RF Series Point Level Switch with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

and

- the IntelliPoint RF Series Point Level Switch development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial IEC 61508-1, -2 and -3 requirements for SIL 3.

and

- the IntelliPoint RF Series Point Level Switch hardware analysis represented by the Failure Mode, Effects and Diagnostic Analysis with the relevant requirements of IEC 61508-2.

The assessment has been carried out based on the quality procedures and scope definitions of *exida*.

The results of this 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.

1.1 Tools and Methods used for the assessment

This assessment was carried by using the *exida* Safety Case tool. The Safety Case tool contains the *exida* scheme which includes all the relevant requirements of IEC 61508.

For the fulfillment of the objectives, expectations are defined which builds the acceptance level for the assessment. The expectations are reviewed to verify that each single requirement is covered. Because of this methodology, comparable assessments in multiple projects with different assessors are achieved. The arguments for the positive judgment of the assessor are documented within this tool and summarized within this report.

The assessment was planned by *exida* agreed with Ametek Drexelbrook.

All assessment steps were continuously documented by *exida* (see [R1] to [R2]).



2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies, specializing in automation system safety and availability with over 400 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 company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment based on 250 billion hours of field failure data.

2.2 Roles of the parties involved

Ametek Drexelbrook	Manufacturer of the IntelliPoint RF Series Point Level Switch
<i>exida</i>	Performed the hardware assessment
<i>exida</i>	Performed the IEC 61508 Functional Safety Assessment per the accredited <i>exida</i> scheme.

Ametek contracted *exida* in December 2016 for the IEC 61508 Functional Safety Assessment of the above-mentioned devices.

2.3 Standards and literature used

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

[N1]	IEC 61508 (Parts 1 - 7): 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
------	-------------------------------	---

2.4 Reference documents

2.4.1 Documentation provided by Ametek Drexelbrook

[D1]	Overall Development Process	440-0010-007 New Product Development Procedure - SIL.pdf
[D2]	Overall Development Process	440-0115-146 NPD Product Stage Gate Sign-off Form - SIL.pdf
[D3]	Overall Development Process	440-0115-234 NPD Project Release Checklist - SIL.pdf
[D4]	Software Development Process	440-0015-069 Software Documentation Procedure XXX.pdf
[D5]	Modification Procedure	440-0015-003 EDO Procedure - SIL.pdf
[D6]	Modification Procedure	440-0015-138 Engineering EDO Processing Procedure.pdf



[D7]	Modification Procedure	440-0115-001 EDO Form - SIL.pdf
[D8]	Modification Procedure	440-0011-120 Vault Tracking Drawing Library Procedure.pdf
[D9]	Modification Procedure	440-0015-122 Permanent Paper System Index Numerical.pdf
[D10]	Impact Analysis Template	440-0115-234 NPD Project Release Checklist - SIL.pdf
[D11]	High Level Software Design Specification	UIV CM DC SDD.doc.crdownload
[D12]	Coding Standard	440-0015-123 Engineering Software Development Guidelines XXX.pdf
[D13]	Validation Test Plan	440-0015-098 Guideline for Test Plan and Fixture Generation.pdf
[D14]	Name of Change Request Tracking System	440-0011-120 Vault Tracking Drawing Library Procedure.pdf
[D15]	Validation Test Results	2016-05-25 - DVT Testing - Rev_4.docx
[D16]	IOM	manual-intellipoint-line-powered-level-switch-rnl-series_english.pdf
[D17]	Engineering Change Documentation	440-0011-038 Maintaining the Document Control Drawing Number.pdf
[D18]	Doc # RNLXX1-LM, Issue #21	Installation and Operating Instructions, IntelliPoint RF Series Line Powered Point Level Switch
[D19]	Doc # RNTXX-LM, Issue #17	Installation and Operating Instructions, IntelliPoint RF Series Two-Wire Point Level Switch
[D20]	Doc # 385-0048-003, Issue 16, 2010-04-10	Assembly Drawing, Bill of Material, and Schematic Drawing, RF Point Level Micro Board
[D21]	Doc # 385-0048-007, Issue 10, 2011-01-10	Assembly Drawing, Bill of Material, and Schematic Drawing, 2-Wire Point Level Power Supply, Xfmr Bd
[D22]	Doc # 385-0048-021, Issue 4, 2002-05-21	Assembly Drawing, Bill of Material, and Schematic Drawing, Universal Power Supply Amendment Relay Board
[D23]	Doc # 385-0048-022, Issue 12, 2016-07-07	Assembly Drawing, Bill of Material, and Schematic Drawing,
[D24]	Doc # 385-0048-030, Issue 4, 2015-11-13	Assembly Drawing, Bill of Material, and Schematic Drawing, Intellipoint 2-Wire Input Board
[D25]	General Circuit Description Intellipoint Transmitter - Updated 06-01-17.doc	General Circuit Description, Intellipoint Transmitter 100 kHz
[D26]	Safety Manual V1R1	SIL Intellipoint Safety Manual



2.4.2 Documentation generated by *exida*

[R1]	AME 16/12-046 R001 V1 R3 FMEDA IntelliPoint	FMEDA report, IntelliPoint RF Series Point Level Switch
[R2]	AME 16/12-046 R001 V1 R4 IntelliPoint Safetycase	IEC 61508 SafetyCaseWB for IntelliPoint RF Series Point Level Switch

2.5 Assessment Approach

The certification audit was closely driven by requirements of the *exida* scheme which includes subsets filtered from IEC 61508.

The assessment was planned by *exida* and agreed upon by Ametek Drexelbrook.

The following IEC 61508 objectives were subject to detailed auditing at Ametek Drexelbrook:

- FSM planning, including
 - Safety Life Cycle definition
 - Scope of the FSM activities
 - Documentation
 - Activities and Responsibilities (Training and competence)
 - Configuration management
 - Tools and languages
- Safety Requirement Specification
- Change and modification management
- Software architecture design process, techniques and documentation
- Hardware architecture design - process, techniques and documentation
- Hardware design / probabilistic modeling
- Hardware and system related V&V activities including documentation, verification
 - Integration and fault insertion test strategy
- Software and system related V&V activities including documentation, verification
- System Validation including hardware and software validation
- Hardware-related operation, installation and maintenance requirements

3 Product Descriptions

The Intellipoint is a true "no calibration" point level measurement system. It uses the technique of RF-Admittance to determine the presence or absence of process material. RF-Admittance is virtually immune to the effects of process material "build-up" or "coating" of the level sensing element. A few of the IntelliPoint's features are:

- 1) Microcontroller based electronics



- 2) A single unit that is DC or AC powered with auto detection
- 3) Dual Relay or 4-20 mA outputs
- 4) Local LED status indicators
- 5) Intrinsically Safe (IS/ia) sensing element.

Table 1 gives an overview of the different versions that were considered in the FMEDA of the IntelliPoint.

Table 1 Version Overview

Loop	Intellipoint with 4-20mA loop power and output – model SxRNTx-x0xx-xxxx
Relay	Intellipoint with 18-200VDC or 85-250VAC power and dual relay output – model SxRNLx-x1xx-xxxx or SxRNLx-x2xx-xxxx

The IntelliPoint is classified as a Type B¹ element according to IEC 61508, having a hardware fault tolerance of 0.

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by Ametek Drexelbrook for this development project against the objectives of the *exida* certification scheme. The results of the assessment are documented in Error! Reference source not found..

All objectives have been successfully considered in the Ametek Drexelbrook development processes for the development.

exida assessed the set of documents against the functional safety management requirements of IEC 61508. This was done by a pre-review of the completeness of the related requirements and then a spot inspection of certain requirements, before the development audit.

The safety case demonstrated the fulfillment of the functional safety management requirements of IEC 61508-1 to 3.

The detailed development audit (see Error! Reference source not found.) evaluated the compliance of the processes, procedures and techniques, as implemented for the Ametek Drexelbrook IntelliPoint RF Series Point Level Switch, with IEC 61508.

The assessment was executed using the *exida* certification scheme which includes subsets of the IEC 61508 requirements tailored to the work scope of the development team.

The result of the assessment shows that the IntelliPoint RF Series Point Level Switch is capable for use in SIL 3 applications, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

¹ Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2, ed2, 2010.



4.1 Product Modifications

The modification process has not yet been assessed and audited, so modifications are not currently covered by this assessment. No modifications are permitted to the certified versions of the IntelliPoint RF Series Point Level Switch without reassessment.



5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Ametek Drexelbrook during the product development against the objectives of the *exida* certification scheme which includes IEC 61508 parts 1, 2, & 3 [N1]. The development of the IntelliPoint RF Series Point Level Switch was done per this IEC 61508 SIL 3 compliant development process. The Safety Case was updated with project specific design documents.

5.1 Lifecycle Activities and Fault Avoidance Measures

Ametek Drexelbrook has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented in [D01].

This functional safety assessment evaluated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the product development. The assessment was executed using the *exida* certification scheme which includes subsets of 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 development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1.1 Functional Safety Management

Objectives

Structure, in a systematic manner, the phases in the overall safety lifecycle that shall be considered in order to achieve the required functional safety of the E/E/PE safety-related systems.

- Structure, in a systematic manner, the phases in the E/E/PES safety lifecycle that shall be considered in order to achieve the required functional safety of the E/E/PE safety-related systems.
- Specify the management and technical activities during the overall, E/E/PES and software safety lifecycle phases which are necessary for the achievement of the required functional safety of the E/E/PE safety-related systems.
- Specify the responsibilities of the persons, departments and organizations responsible for each overall, E/E/PES and software safety lifecycle phase or for activities within each phase.
- Specify the necessary information to be documented in order that the management of functional safety, verification and the functional safety assessment activities can be effectively performed.
- Document all information relevant to the functional safety of the E/E/PE safety-related systems throughout the E/E/PES safety lifecycle.
- Document key information relevant to the functional safety of the E/E/PE safety-related systems throughout the overall safety lifecycle.
- Specify the necessary information to be documented in order that all phases of the overall, E/E/PES and software safety lifecycles can be effectively performed.
- Select a suitable set of tools, for the required safety integrity level, over the whole safety lifecycle which assists verification, validation, assessment and modification.



5.1.2 Safety Lifecycle and FSM Planning

Assessment

Manufacturer has a QMS in place. The Manufacturer has been ISO 9001 certified.

Conclusion:

The objectives of the standard are fulfilled by the Ametek Drexelbrook functional safety management system and new product development processes.

5.1.3 Documentation

Assessment

There is a document management system in place. This system controls how all safety relevant documents are changed, reviewed and approved.

Conclusion

The objectives of the standard are fulfilled by the Ametek Drexelbrook functional safety management system.

5.1.4 Configuration Management

Assessment

Formal configuration control is defined and implemented for Change Authorization, Version Control, and Configuration Identification. A documented procedure exists to ensure that only approved items are delivered to customers. Master copies of the software and all associated documentation are kept during the operational lifetime of the released software.

Conclusion

The objectives of the standard are fulfilled by the Ametek Drexelbrook organizational release procedures, functional safety management system and new product development processes.

5.1.5 Hardware Design / Probabilistic properties

Assessment

To evaluate the hardware design of the Intellipoint, a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida* for each component in the system. This is documented in [R2].

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.



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.

Conclusion

The objectives of the standard are fulfilled by the Ametek Drexelbrook functional safety management system, FMEDA quantitative analysis, and hardware development guidelines and practices.

5.2 Safety Manual

Objectives

- Develop procedures to ensure that the required functional safety of the E/E/PE safety-related systems is maintained during operation and maintenance.

Assessment

The Safety Manual is provided and identifies and describes the functions of the product. The functions are clearly described, including a description of the input and output interfaces. When internal faults are detected, their effect on the device output is clearly described.

Conclusion

The objectives of the standard are fulfilled by the Ametek Drexelbrook functional safety management system and the safety manual.



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
HFT	Hardware Fault Tolerance
Low demand mode	Mode where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
High demand mode	Mode where the demand interval for operation made on a safety-related system is less than 100x the diagnostic detection/reaction interval, or where the safe state is part of normal operation.
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 A element	"Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	"Complex" element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 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 Version History

Contract Number	Report Number	Revision Notes
Q16/12-046	AME 16/12-046R002 V1, R0	Initial Release

Review: Steven Close, *exida*, 10/26/17

Status: Released, 10/26/17

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Handwritten signature of Loren Stewart in black ink.

Loren Stewart, CFSE, Safety Engineer

Handwritten signature of Steven Close in black ink.

Steven Close, Senior Safety Engineer