Results of the IEC 61508 Functional Safety Assessment

Project:
7800 Series Burner Controller and 7823 Flame Switch

Customer:
Honeywell Combustion Controls
Houston, TX
USA

Contract No.: Q23/07-078
Report No.: HON 17-02-010 R002
Version V2, Revision R1, December 28, 2023
Rudolf Chalupa

Management Summary

The Functional Safety Assessment of the Honeywell Combustion Controls

7800 Series Burner Controller and 7823 Flame Switch

development project, performed by *exida* consisted of the following activities:

- *exida* assessed the development process used by Honeywell Combustion Controls through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The assessment 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* reviewed field failure data to verify the accuracy of the FMEDA analysis.
- *exida* reviewed the manufacturing quality system in use at Honeywell Combustion Controls.

The functional safety assessment was performed to the SIL 3 requirements of IEC 61508. 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 Honeywell Combustion Controls 7800 Series Burner Controller and 7823 Flame Switch development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.

The assessment of the FMEDA also shows that the 7800 Series Burner Controller and 7823 Flame 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).

This means that the 7800 Series Burner Controller and 7823 Flame 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 section 0 of this document.

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

Table of Contents

1 Purpose and Scope

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

- 7800 Series Burner Controller and 7823 Flame Switch

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

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

- the 7800 Series Burner Controller and 7823 Flame Switch with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

and

- the 7800 Series Burner Controller and 7823 Flame 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 7800 Series Burner Controller and 7823 Flame 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 assessment provide the safety instrumentation engineer with the required failure data 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 out 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 Honeywell Combustion Controls.

All assessment steps were continuously documented by *exida* (see [R1] to [R8]).

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, availability, and cybersecurity with over 500 person-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 350 billion hours of field failure data.

2.2 Roles of the parties involved

Honeywell Combustion Controls	Manufacturer of the 7800 Series Burner Controller and 7823 Flame Switch
exida	Performed the hardware assessment
exida	Performed the Functional Safety Assessment per the accredited *exida* scheme.

Honeywell Combustion Controls 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 61508:2010 (Parts 1 – 7)	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

Note: Documents revised after the last audit are highlighted in grey.

2.4.1 Documentation provided by Honeywell Combustion Controls

Doc. ID	Project Document Filename	Version	Date
D001	ECC Global Quality Systems Manual.pdf	Issue 7	10/3/2014
D003	ECC New Product Introduction Process Swimlane.pdf	Rev. M	2011
D003b	NPI Templates and Tools1.xlsx	Rev. C	2/20/2014
D003c	ASDP Project Audit Report - requirements.pdf		4/26/2016
D003d	711680 Kettos ASDP Tailoring - 2011 to 2015.xlsx	Rev. 8	1/6/2015
D003e	ASDP Requirements.pdf	Screenshot	
D003f	Architecture.pdf	Screenshot	
D003g	Design.pdf	Screenshot	
D003h	Implementation.pdf	Screenshot	
D003i	Test.pdf	Screenshot	

Doc. ID	Project Document Filename	Version	Date
D003j	Project Management.pdf	Screenshot	
D003k	Change Management.pdf	Screenshot	
D004	EP4.1.1_Y Eng Change Orders.pdf		8/1/2015
D004b	EP4.16.6_F Software Change Process.pdf		4/1/2013
D005	70-0568_WarrantyPolicy.pdf	Rev. 10-15	
D006	70-0568_WarrantyPolicy.pdf	Rev. 10-15	
D007	Supplier Approval Process.pdf	Rev. 5.5	
D007b	Supplier Approval Process Procedure Sheet PS-3.4.doc		3/4/2002
D008	DA3.5.2_A Conditional Qualification Testing.pdf	Rev. A	12/1/2015
D010	EP4.1.1_Y ECRO Process.pdf	Rev. Y	8/1/2015
D012	eCATS_Users_Guide.doc		(c) 2010
D012b	CHP14.pdf	Rev. P	9/25/2016
D012c	eCATS Enhancement Training Oct 2011.ppt		10/6/2011
D013	711680_Kettos ASDP Quality Plan.docx	Rev. 2	9/24/2014
D016	711680_Kettos ASDP Quality Plan.docx	Rev. 2	9/24/2014
D019	LightBlue Functional Safety Management Plan FSM.docx	Rev. 1.6	11/13/2017
D021	ASDP Software Development Lifecycle.pdf	Screenshot	
D021b	SLATE Software Tool Qualification Procedure.doc		6/28/2016
D021c	IAR Certified tools.pdf		6/28/2016
D021d	IAR Certified tools FAQ.pdf		6/28/2016
D023	EP4.1.1_Y ECRO Process.pdf	Rev. Y	8/1/2015
D023b	SIL-3 Impact Analysis Template.docx	rev. 1	8/25/2016
D023c	EP4.16.6_F Software Change Process.pdf	Rev. F	4/1/2013
D023d	EP 3.20.1_E PRODUCT SAFETY & EMC LISTING.pdf	Rev. E	4/1/2013
D023e	EP 4-3_D_1_D Form Fit or Function.pdf	Rev. D	12/1/2008
D026	LightBlue Functional Safety Management Plan FSM.docx	Rev. 1.6	11/13/2017
D026b	Light Blue Project Plan.docx	Rev. 5	10/25/2017
D027	Light Blue Configuration Management Plan.doc	Rev. 2	3/23/2017
D029	40013_LightBlue_quality_assurance_plan.xlsx	Rev. .01	10/13/2017
D029b	LightBlue-CodeReviewChecklist.docx	Rev. 0.06	
D032	D032_Job Descriptions and Competency Levels	Many	
D034	Light Blue SkillsMatrix.xlsx		10/23/2017
D034b	Unity_ Light Blue (728207).pdf		10/15/2017
D036	ISO9001 - 014501_QMS_ENG nov 2015.pdf		9/14/2018
D038	LightBlue Design Tools.docx	Rev. 0.3	11/16/2017
D040	Safety+Requirements.doc		10/20/2017
D040c	LightBlue+Requirements-2017-06-11.docx		11/6/2017
D041	SafetyArch_Review.PNG	Screenshot	

Doc. ID	Project Document Filename	Version	Date
D043	Safety+Architecture.doc		10/20/2017
D045	LightBlueHWBlocks20170206.docx		2/6/2017
D045b	LightBlueHWDescr2.docx	Rev. 0.03	9/28/2017
D045c	sio00L_2009_12_18.pdf		12/18/2009
D049	Burner Control Software Architecture.docx	Rev. 4	9/7/2017
D050	Honeywell Light Blue HAZOP Report V0R0 - tn notes.pdf	V0R0	7/27/2017
D050b	RE 20170725 Minutes of LightBlue SIL3 - Architecture Audit Review - Few SW Questions.msg		7/25/2017
D051	_Software Detailed Design (Contour).docx	Generated	10/19/2017
D051b	CSM SDD.doc	Generated	10/16/2017
D051c	EEPROM SDD.doc		6/21/2017
D051d	ngpl.txt		7/22/2004
D051e	OS SDD.doc		5/16/2016
D051f	RAMcheck module SDD.doc		9/5/2017
D051g	Safety Vars SDD.doc		9/5/2017
D053	FlameSenseConceptReview.docx		5/10/2016
D053b	Light Blue Concept Review.docx		2/22/2016
D053c	Light Blue Design Review.docx		6/27/2016
D053d	SWArchReview.png	Screenshot	
D054b	LightBlueAIList_MechanicalDesign.xlsx		11/7/2017
D056	Donwstream+Traceability+Report.pdf		10/20/2017
D056b	Upstream+Traceability+Report.pdf		10/20/2017
D056c	RE Exida - Dave - Meeting notes 20171013.msg		11/6/2017
D057	JUMPERS_FULL_REPORT.html		10/4/2017
D057b	OPTO_SAMPLING_full_report.html		9/11/2017
D058	CR-3 Screenshot.PNG	Screenshot	
D058b	CR-26 Screenshot.PNG	Screenshot	
D059	Light Blue Fault Injection List.xls		10/13/2017
D060	Kettos Coding Standard ver 1.15 31Oct2016.docx	Rev. 1.15	10/31/2016
D061	Klockwork Settings - TimN 28Mar2016.pdf		3/28/2016
D062	sprint18_end-RemainingIssues.pdf		10/12/2017
D062b	KlocworkScreenshot.PNG		10/12/2017
D064	JUMPERS.tst		10//3/2016
D064b	OPTO_SAMPLING.tst		10/31/2016
D066	OPTO_SAMPLING_full_report.html		9/11/2017
D067	Anti-Bootlegging+PIN.doc		10/13/2017
D067b	BC+State+Machine.doc		10/13/2017
D067c	VP+State+Machine.doc		10/13/2017

Doc. ID	Project Document Filename	Version	Date
D069	Safety+architecture+tests.doc		10/13/2017
D069b	Validation and Integration Test Fixtures and set up.docx		10/12/2017
D069c	sio00L_2009_12_18.pdf	Marked up	12/9/20090
D069d	ILK+in+Initiate.doc	Generated	11/13/2017
D069e	LFS+in+Initiate.doc	Generated	11/13/2017
D070	REV-15000.png		10/20/2017
D071	D071_Environmental Test Plan	Many	
D072	D072_EMC Test Plan	Many	
D074	D074_Validation Test Results	Many	
D075	D075_Environmental Test Results	Many	
D076	D076_EMC Test Results	Many	
D077	Light Blue Fault Injection List.xls		10/13/2017
D078	66-1162_B.pdf	Rev. 5	
D079	RM 7800 Burner Controller Safety Manual	V2 R0	11/14/2017
D080	ECLGBHL-CR-44.png	Screenshot	
D084	HON 17-02-010 V1R0 61508 SafetyCaseWB - 7800.xlsm	V1R0	
D086	LightBlue Design Tools.docx	Rev. 0.3	11/16/2017
D086b	IAR Compiler - Validation Of Compliance-EWAVR32-4.21.pdf	Rev. 4.21.1	3/21/2016
D089	_201710124 HON 17-02-010 V1R0 Onsite Audit Light Blue.docx		10/12/2017
D090	LightBluePlatformDifferences.xlsx		5/7/2018
D091	40013 LightBlue SW REV 5015 Test Summary.docx		6/15/2018
D092	SVNReport_BC.txt		5/7/2018
D093	Safety+architecture+tests.doc	Rev. 1	10/13/2017
D100	ISO 9001 2015 North Corregido.pdf	n/a	Dec.2018
D101	Flex-Manufacturing ISO.pdf	n/a	Jan.2019
D102	7800 Series Warranty Returns	n/a	2023
D103	RM-EC7800 Units sales.xlsx	n/a	Nov.2020
D104	7800 FW and HW changes.xls.xlsx	n/a	Nov.2020
D105	LTB-1036_ImpactAnalysis.docx	n/a	May.2018
D106	LB_low_volt_detect02 _MatchCad.pdf	2	Apr.2018
D107	LTB-903 Folder	n/a	Feb.2018
D108	LTB-1049_ImpactAnalysis.docx	n/a	May.2018
D109	LTB-1049.doc	n/a	May.2018
D110	AClineErrorRelease_5029.xls	5029	Feb.2020
D111	SoftwareDetailedDesign.doc	1	May.2021
D112	Safety+architecture+tests.xls	export	Jul.2018
D113	Safety+Requirements.xls	export	Sep.2019
D114	LTB-5030.docx	Export	Jan.2021

Doc. ID	Project Document Filename	Version	Date
D115	Kettos RMA Compilation Report, RMA Report		

2.4.2 Documentation generated by *exida*

[R1]	HON 17-02-010 IEC 61508 Safety Case, V3R0, 8-Dec-2023	Safety Case for 7800 Series Burner Controller and 7823 Flame Switch
[R2]	HCC Q20-10-162 SLATE+7800 Surveillance Proposal	Assessment Plan
[R3]	HCC 09-10-38 R001, V3R1, 30-Oct-2023	7800 Series Burner Controller FMEDA Report
[R4]	HCC 18-10-152 R001, V1R3, 1-Jul-2019	7823 Flame Switch FMEDA Report
[R5]	HON 17-02-010 R005, V1R0	IEC 61508 Change Review Report
[R6]	HCC FFA Spreadsheet 7800, 4-Dec-2023	Field Failure Analysis for 7800 Series Burner Controller
[R7]	HCC FFA Spreadsheet 7823, 21-Nov-2023	Field Failure Analysis for 7823 Flame Switch
[R8]	HCC 23-07-078, 8-Dec-2023	7800 Series Burner Controller and 7823 Flame Switch Surveillance Audit Workbook

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 with Honeywell Combustion Controls.

The following IEC 61508 objectives were subject to detailed auditing at Honeywell Combustion Controls:

- 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 Description

The 7800 Series Burner Controller is intended for use in a wide range of commercial and industrial combustion control applications including burners, boilers, furnaces, packaged rooftop units, ovens, kilns, and water heaters.

The product is designed to meet all requirements for SIL 3 according to [N1], so that it can be used as a single product with Hardware Fault Tolerance (HFT) of zero to implement SIL 3 combustion control Safety Integrity Functions (SIF).

The 7800 Series Burner Controller is a microprocessor-based integrated burner controller for automatically fired gas, oil, or combination fuel single burner applications. The 7800 is used for UL/CSA On/Off, UL/CSA Modulating, and FM/IRI Modulating burner applications. The 78700 Series system consists of a Burner Control, Dust Cover, Subbase, Amplifier, Purge Card and Optional Keyboard Display Module (standard with RM7800 and RM7838).

Functions provided by the 7800 include automatic burner sequencing, flame supervision, auxillary burner management safety functions, system status indication, system or self-diagnostics and troubleshooting.

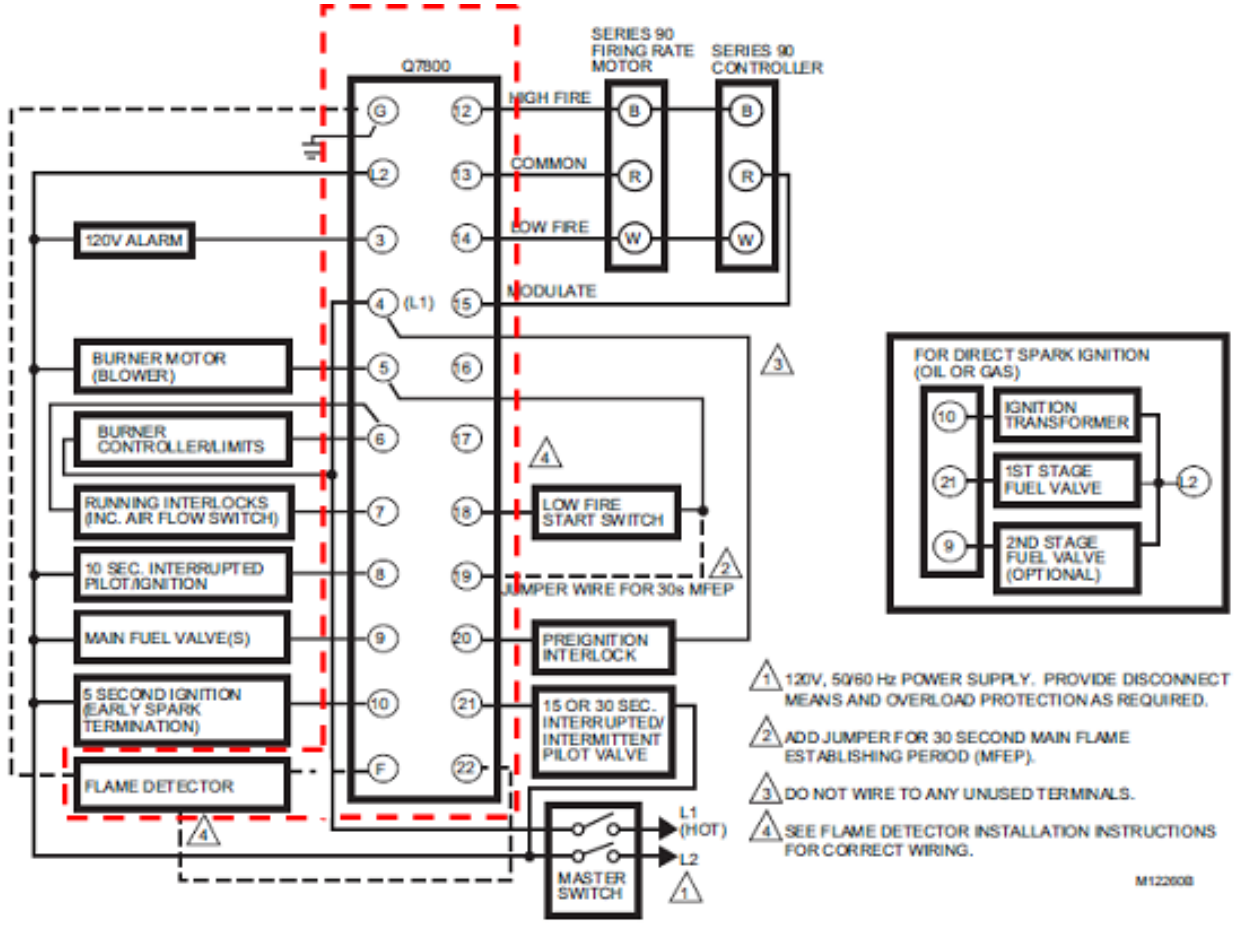

Figure 1: Controller and Sensor/Flame Detector

This assessment applies to the following model numbers in Table 1. The product versions are referred to as series numbers below. The combinations of modules, sensors and flame amplifiers are specified in Honeywell documentation.

Table 1: 7800 Series Burner Controller Model and Series

RELAY MODULES				FLAME SENSORS		FLAME AMPLIFIERS	
MODEL	**SERIES**	**MODEL**	**SERIES**	**MODEL**	**SERIES**	**MODEL**	**SERIES**
RM7800	9	RM7895	6	C7008A	1	R7847B	5
RM7824	4	RM7896	6	C7009A	1		
RM7830	5	RM7897	6				
RM7838	9	RM7898	6	C7915A	1	R7852B	2
RM7840*	8						
RM7845	3	EC7820	7	C7012E	7		
RM7850	5	EC7830	6	C7012F	5		
RM7865	4	EC7840	5	C7024E	obsolete	R7824C	2
RM7885	5	EC7850	6	C7024F	obsolete	R7847C	5
RM7888	5	EC7890	5	C7061A	1	R7851C	2
RM7890	9	EC7895	5	C7061F	1	R7861A	2
				C7076A	1	R7886A	2
				C7076D	1		
				C7961E	1		
				C7961F	1		

*NOTE: RM7840E1016 and RM7840L1026 are Series 5; RM7840L1018 is Series 6.

Model S7830 has been assessed to be interference free and may be used with the above products without impacting safety.

The Honeywell 7800 Series Burner Controller and 7823 Flame Switch is a microprocessor-based element that can be fitted with any 7800 SERIES amplifier to provide relay action from one relay with 2 single pole, double throw (SPDT) circuits when flame is present or not present. The EC7823/RM7823 Relay Module, Q7800 Wiring Subbase and Amplifier, are required to complete the system.

Functions provided by the 7800 Series Burner Controller and 7823 Flame Switch include flame monitoring, system status indication, system or self-diagnostics and troubleshooting.

The 7800 Series Burner Controller and 7823 Flame Switch safety function is a flame detector relay only. Suitable primary control must be used to provide safe-start check, safety lockout, load switching and other required outputs in flame safeguard systems.

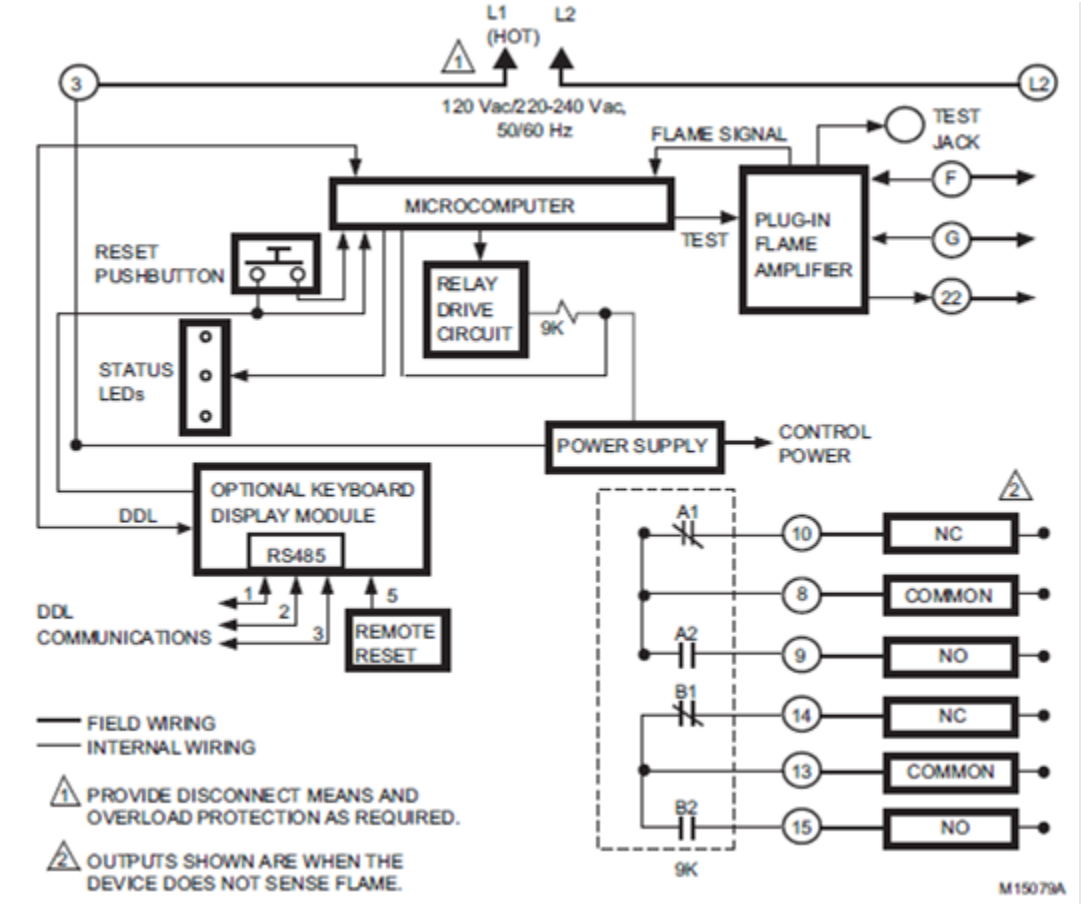

Figure 2: Flame Switch Overview

The 7800 Series Burner Controller and 7823 Flame Switch is classified as a Type B[1] device according to IEC 61508, having a hardware fault tolerance of 0.

3.1 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions of 7800 Series Burner Controller:

Table 2 - <Enter short product name as product1 under custom properties> Hardware and Software Versions

Variant/Model	Hardware Version	Software Version
RM78xx models listed in Table 1	Rev. -003	5030
EC78xx models listed in Table 1	Rev. -001	5030

The versions in Table 1 and Table 2 were current when this report was released. For updated versions covered under this certification, refer to the <Enter short product name as product1 under

[1] Type B element: "Non-Complex" element (using discrete components); for details see 7.4.4.1.3 of IEC 61508-2, ed2, 2010.

custom properties> Safety Manual which includes the company webpage where the certified versions and compatibility can be checked.

The 7823 assessment is applicable to the hardware and software versions shown in Table 3. Flame detectors and amplifiers from Table 4 which use Ampli-Check™ or Self-Check™ have been previously certified by *exida* and are incorporated into this analysis. The combinations of modules, sensors and flame amplifiers are specified in Honeywell installation and safety manual documents. The component versions listed were certified and current at the time of this certification. Contact Honeywell Combustion Controls for information on version updates or compatibility issues.

Table 3 Version Overview

7800 Series Burner Controller and 7823 Flame Switch using Detectors/Amplifiers with Ampli-Check modules (see Table 4)	Hardware: Doc # 32329382, Rev 5 or higher, Jan.2019 Firmware: Build 5028 or higher, Aug.2019
7800 Series Burner Controller and 7823 Flame Switch using Detectors/Amplifiers with Self-Check modules (see Table 4)	

Table 4 Flame Detectors and Amplifiers

FLAME SENSORS		**FLAME AMPLIFIERS**	
MODEL	**SERIES**	**MODEL**	**SERIES**
C7008A	1	R7847B	4
C7009A	1		
C7915A	1	R7852B	1
C7012E	1	R7847C	4
C7012F	1	R7851C	1
C7061A	1	R7861A	1
C7061F	1	R7886A	2
C7076A	1		
C7076D	1		
C7961E	1		
C7961F	1		

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by Honeywell Combustion Controls for this development project against the objectives of the exida certification scheme. The results of the assessment are documented in [R1].

All objectives have been successfully considered in the Honeywell Combustion Controls development processes for the development.

exida assessed the set of documents against the functional safety management requirements of IEC 61508. An evaluating assessor created a safety case, to argue that the relevant requirements of IEC 61508-1 to -3 have been met, based on documented evidence provided. An independent certifying assessor then reviewed the safety case to ensure coverage of the relevant requirements and the validity of the arguments. Additionally, an audit is performed to witness development and manufacturing environments and techniques to ensure procedures are being followed and that certain testing is carried out successfully.
The safety case demonstrated the fulfillment of the functional safety management requirements of IEC 61508-1 to 3.

The detailed development audit (see [R1]) evaluated the compliance of the processes, procedures and techniques, as implemented for the Honeywell Combustion Controls 7800 Series Burner Controller and 7823 Flame 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 7800 Series Burner Controller and 7823 Flame Switch is capable for use in SIL 3 applications, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

4.1 Product Modifications

The modification process has been successfully assessed and audited, so Honeywell Combustion Controls may make modifications to this product as needed.

As part of the *exida* scheme a surveillance audit is conducted prior to renewal of the certificate. The modification documentation listed below is submitted as part of the surveillance audit. *exida* will review the decisions made by the competent person in respect to the modifications made.

- List of all anomalies reported
- List of all modifications completed
- Safety impact analysis which shall indicate with respect to the modification:
  - The initiating problem (e.g. results of root cause analysis)
  - The effect on the product / system
  - The elements/components that are subject to the modification
  - The extent of any re-testing
- List of modified documentation
- Regression test plans

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Honeywell Combustion Controls 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 7800 Series Burner Controller and 7823 Flame 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

Honeywell Combustion Controls has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented in [D003].

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 Honeywell Combustion Controls design and development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1.1 Functional Safety Management

The objective of functional safety management are to:

- 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.

Honeywell Combustion Controls has documented their development and manufacturing processes in overall safety lifecycle procedures. They specify the required management and technical activities, as well as the responsibilities of the persons, departments, and organizations involved in each product and software safety lifecycle phase. This meets the requirements of SIL 3.

5.1.2 Safety Lifecycle and FSM Planning

The functional safety management plan defines the safety lifecycle for this project. This includes a definition of the safety activities and documents to be created for this project. This information is communicated via these documents to the entire development team so that everyone understands the safety plan. The Software Development Procedure identifies the phases of the software development lifecycle and the inputs/outputs associated with each phase. All phases of the safety lifecycle have verification steps described in the FSM plan, the ASDP, the plan for the development phases.

Software development procedure states that if, at any phase of the software safety lifecycle, a modification is required pertaining to an earlier lifecycle phase, then an impact analysis shall determine which software modules are impacted and which earlier safety lifecycle activities shall be repeated. Lifecycle Phase Verification results are documented according to the verification plan and available for assessment.

Honeywell Combustion Controls has a quality management system (QMS) in place and has been ISO 9001 certified. All sub-suppliers have been qualified through the Manufacturer Qualification procedure. Reported dangerous failures that occur in the field are captured and analyzed and recommendations are made to minimize the chance for a repeat occurrence of the failure.

This meets the requirements of SIL 3.

5.1.3 Documentation

There are two document management systems in place. One is used for quality system documentation and some hardware documentation, and the other system is used for the other engineering artifacts, including firmware. The systems control how all safety relevant documents are changed, reviewed, and approved.

The Functional Safety Management Plan also identifies the structure of the project-specific documentation as well as the specific versions of procedures and standards to be used on the project. The procedures to manage project documentation are also specified. This meets the requirements of SIL 3.

5.1.4 Training and competence recording

The Functional Safety Management Plan addresses competency requirements by providing documented evidence that personnel are evaluated for the project roles they serve. Evaluation is performed by management and project leadership and training is provided and documented when gaps are identified. This meets the requirements of SIL 3.

5.1.5 Configuration Management

The configuration of the product to be certified is documented including all hardware and software versions that make up the product. For software, this includes source code. Subversion is used for source code version control and Configuration Management.

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. This meets the requirements of SIL 3.

5.1.6 Tools

A suitable set of tools are selected, qualified, and properly managed over the whole safety lifecycle, which assist in verification, validation, assessment, and modification activities. Project tools are listed and categorized, by criticality to the safety function, in the Functional Safety Management Plan. Each tool's qualification is listed or referenced. This meets the requirements of SIL 3.

5.2 Safety Requirement Specification

The main objectives of the related IEC 61508 requirements are to specify the requirements for each E/E/PE safety-related system, in terms of the required safety functions and the required safety integrity, in order to achieve the required functional safety.

Software safety requirements have been created as derived/allocated requirements (from Safety Requirements). These requirements have been made available to the software developers and have been reviewed by software developers. The results of the review are documented, and all action items are tracked through resolution.

The SRS has been reviewed to verify that it has sufficient detail so the required SIL can be achieved during design and implementation. SRS content is available and sufficient for the duties to be performed. This has been confirmed by the validation testing and assessment. Specific requirements for start-up and restart procedures are specified. All system, operator, and software interfaces necessary to achieve the required functional safety are specified and all safety related constraints between the software and hardware have been documented in the Software Safety Requirements or other suitable requirements document.

This meets the requirements of SIL 3.

5.3 Change and modification management

Objectives

The main objectives of the related IEC 61508 requirements are to ensure that the required safety integrity is maintained after corrections, enhancements or adaptations to the E/E/PE safety-related systems.

Modifications are initiated with an Engineering Design Change procedure [D023]. All changes are first reviewed and analyzed for impact before being approved. Measures to verify and validate the change are developed following the normal design process.

The Modification Procedure requires that an Impact Analysis be performed to assess the impact of the modification, including the impact of changes to the software design (which modules are impacted) and on the Functional Safety of the system. The results of an Impact Analysis are documented.

Modification Request/Records will document the reason for the change and have a detailed description of the proposed change. The impact analysis documents which tests must be run to validate the change and which tests must be re-run to validate that the change did not affect other functionality.

The Software Modification Procedure requires that the changed software module is reverified after the change has been made and requires that all affected software modules are reverified after modification. The Software Modification Procedure allows regression validation for certain modifications. The Impact Analysis indicates the plan for software verification and validation of the modification. The plan is a tailored version of the plan expected for a full verification, based on the SIL.

The modification process has been successfully assessed and audited, so Honeywell Combustion Controls may make modifications to this product as needed. This meets the requirements of SIL 3.

5.4 System Design

The objective of the related IEC 61508 requirements of this subclause are to specify the design requirements for each E/E/PE safety-related system, in terms of the subsystems and elements.

The System Architecture Design clearly identifies that all components are developed to the target SIL and describes that the behavior of the device when a fault is detected is to take the device to the Lockout State (all outputs to safe states).

The System Architecture Design clearly identifies all safety critical interfaces and a communications analysis has been done to show that these interfaces comply with 7.4.11 of IEC 61508-2. Code protection (information and/or time redundancy) is considered where needed.

All software components or subsystems listed in the Software Architecture Design have corresponding Software Designs which further partition the design into software modules. The design has a focus on simplicity. The Software Design describes the design of all diagnostics required to detect faults in software control flow and data flow. The resulting behavior of the device due to a detected fault is specified.

Formal design reviews are held and the results recorded; action items are identified, assigned, and resolved. Reviews are documented using software tools called Fisheye and Crucible. The System Architecture Design requires the use of a password to access the configuration to make changes.

Semi-formal methods are used in the design and development. The Software Design is well understood by the developers and is documented in a way that can be easily verified.

This meets the requirements of SIL 3.

5.5 Hardware Design and Verification

The main objectives of the related IEC 61508 requirements are to:

- Create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements).
- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.
- Demonstrate, for each phase of the overall, E/E/PES and software safety lifecycles (by review, analysis and/or tests), that the outputs meet in all respects the objectives and requirements specified for the phase.
- Test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase.

- Integrate and test the E/E/PE safety-related systems.

The hardware design is captured in schematics, which are under revision control and configuration management. The design is verified through review and verification testing. This meets the requirements of SIL 3.

5.5.1 Hardware architecture design

Hardware Components used on previous projects are given priority over new components. This is implemented by having a component database, and a procedure which states that approval must be given to use any hardware component not already in the component database. FMEDA analyst has reviewed the design and determined that there are measures against physical environment stresses.

Hardware architecture design has been partitioned into subsystems, and interfaces between subsystems are defined and documented. Design reviews are used to discover weak design areas and make them more robust. Measures against environmental stress and over-voltage are incorporated into the design.

The FSM Plan, development process and guidelines define the required verification activities related to hardware including documentation, verification planning, test strategy and requirements tracking to validation test.

This meets the requirements of SIL 3.

5.5.2 Hardware Design / Probabilistic properties

Assessment

To evaluate the hardware design of the 7800 Series Burner Controller and 7823 Flame Switch, a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) was performed by exida for each component in the system. These are documented in [R3] and [R4]. Assumptions taken in the FMEDA were verified using Fault Injection Testing as part of the development (see the Fault Injection Test Plan [D077]) 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.

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 objectives of the standard are fulfilled by the Honeywell Combustion Controls functional safety management system, FMEDA quantitative analysis, and hardware development guidelines and practices.

5.6 Software Design

The main objectives of the related IEC 61508 requirements are to:

- Create a software architecture that fulfils the specified requirements for software safety with respect to the required safety integrity level.

- Review and evaluate the requirements placed on the software by the hardware architecture of the E/E/PE safety-related system, including the significance of E/E/PE hardware/software interactions for safety of the equipment under control.
- Design and implement software that fulfils the specified requirements for software safety with respect to the required safety integrity level, which is analyzable and verifiable, and which is capable of being safely modified.

The Software Architecture Design contains a description of the software architecture. The design is partitioned into existing components and modules, which are identified as such. All components are considered safety critical at the highest SIL as defined in the safety requirements specification for the product. However, a FMEA was performed, and criticalities have been documented and no SIL reduction is claimed for software components.

The Software Architecture Design uses a code generator that is based on a carefully specified state machine "language", developed by Honeywell, which qualifies as an unambiguous, semi-formal method. The Software Architecture Design specifies that fault detection techniques are employed to detect software faults.

The Software Design describes the design features that maintain the safety integrity of data and all diagnostics required to detect faults in software control flow and data flow. The resulting behavior of the device due to a detected fault is specified. Restarts are done when faults are detected and memory is not dynamically allocated.

This meets the requirements of SIL 3.

5.7 Software Verification

The main objectives of the related IEC 61508 requirements are to:

- To the extent required by the safety integrity level, test and evaluate the outputs from a given software safety lifecycle phase to ensure correctness and consistency with respect to the outputs and standards provided as input to that phase.
- Verify that the requirements for software safety (in terms of the required software safety functions and the software safety integrity) have been achieved.
- Integrate the software onto the target programmable electronic hardware. Combine the software and hardware in the safety-related programmable electronics to ensure their compatibility and to meet the requirements of the intended safety integrity level.

The Software Architecture Design was reviewed. This review confirms that the architecture fulfills the safety requirements and is free from ambiguity. All action items required to be addressed were submitted to the action item tracking system and have been resolved.

A modular approach has been used in the software design. Design has been broken up into classes and methods which are modular and subprograms have a single entry and a single exit. A structural test coverage of 100% for entry points, statements, and branches has been documented by a tool or a manual trace of test coverage.

The 'C' programming language is used. As shown in table C.1 of IEC 61508-7, the 'C' programming language when used with a defined language subset, a coding standard, and static analysis tools is highly recommended for all SILs. For this project, there is a coding standard which defines a language subset and static analysis tools are used to detect potential problems in the source code. Therefore, 'C' can be considered a suitable programming language.

Module Test Results for all safety related modules were produced and documented per the Module Test Verification Plan/Specification; sample results files were reviewed; unit tests are automated or manual; verification of data is included in tests; result files show the pass/fail output line. No unintended functions were performed.

The results of Static Analysis of source code are documented, controlled with project documentation and verified. The Integration Test Plan requires that Safety Functions are tested during Integration Testing using a functional testing approach. Integration Test Cases have been successfully run per the Integration Test Plan and Integration Test Results have been documented.

For each test, the Integration Test Results Record identifies the Test Case, its version, the version of the product being tested, the tools; and the equipment used, along with their calibration data. In addition, the Integration Test Results Record references the Integration Test Plan including version number. VectorCast test management tools are used to manage the module testing process.

Source code standard states that software modules interact with each other through their interfaces which are fully defined and documented, completely prototyped, including names of parameters, return values, special uses of the function and evidence is available that this was followed.

Module test results show that boundary value analysis was used to determine test cases. These test cases are applied to the interface of the module. Unit Test Checklist in Unit Test Plan states that this should be done. A review of several module tests showed that this has been done.

The Integration Test Plan was reviewed and found to be adequate regarding its coverage of the Software Safety Requirements, the Software Architecture Design, the Software System Design, the types of tests to be performed and the procedures to be followed. All action items have been resolved or deferred.

The Integration Test Plan calls for black-box testing of all integration levels. Equivalence classes and boundary values have been considered in writing all Integration Test Cases. Test case execution includes combining some critical cases at extreme operating boundaries.

This meets the requirements of SIL 3.

5.8 Safety Validation

The main objectives of safety validation are to:

- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.
- Plan the validation of the safety of the E/E/PE safety-related systems.
- Validate that the E/E/PE safety-related systems meet, in all respects, the requirements for safety in terms of the required safety functions and the safety integrity.
- Ensure that the integrated system complies with the specified requirements for software safety at the intended safety integrity level.

One or more test cases, or analysis documents, exist for each safety requirement (including software safety requirements) as shown by the requirements traceability matrix. Each test case includes a procedure for the test as well as pass/fail criteria for the test (inputs, outputs and any other acceptance criteria). The validation test plan includes the procedure used to properly judge that the validation test is successful or not.

Fault injection testing has been performed on the product as defined in the fault injection test plan. The results have been analyzed and adjustments have been made to the FMEDA based on these results. Test results are documented including reference to the test case and test plan version being executed.

The EMC/Environmental specifications tested (and passed) were the same as or more stringent than those reviewed and approved by the FMEDA analyst. Performance modeling has been performed to an extent in that timing requirements must be met.

The validation testing requires simulation of process inputs and timing between input changes (process simulation). This is done by testing the software in the product hardware and simulating the input signal(s) and other process conditions using a test fixture or test equipment.

This meets the requirements of SIL 3.

5.9 Safety Manual

The objective of the Safety Manual is to provide the information necessary for users of the certified product to develop procedures to ensure that the required functional safety of the E/E/PE safety-related systems is maintained during operation and maintenance.

A safety manual documents all safety related information needed to ensure that the required level of functional safety is maintained during operation and maintenance. This information includes safety integrity properties, specification of safety functions, technical interface specifications, configuration information, procedures to validate the integrity of the product, how to contact Honeywell to report any failures, the responsibilities of the end user in the case a fault is detected, environmental limits, competency requirements for installation/maintenance/use and procedures to install new versions of software. This meets the requirements of SIL 3.

7 2023 IEC 61508 Functional Safety Surveillance Audit

7.1 Roles of the parties involved

Honeywell Combustion Controls	Manufacturer of the 7800 Series Burner Controller and 7823 Flame Switch
exida	Performed the hardware assessment review
exida	Performed the IEC 61508 Functional Safety Surveillance Audit per the accredited *exida* scheme.

Honeywell Combustion Controls contracted *exida* in July 2023 to perform the surveillance audit for the above 7800 Series Burner Controller and 7823 Flame Switch. The surveillance audit was conducted remotely on November 3, 2023.

7.2 Surveillance Methodology

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

- Procedure Changes – Changes to relevant procedures since the last audit are reviewed to determine that the modified procedures meet the requirements of the *exida* certification scheme.
- Engineering Changes – The engineering change list is reviewed to determine if any of the changes could affect the safety function of the 7800 Series Burner Controller and 7823 Flame Switch.
- Impact Analysis – If changes were made to the product design, the impact analysis associated with the change will be reviewed to see that the functional safety requirements for an impact analysis have been met.
- Field History – Shipping and field returns during the certification period will be reviewed to determine if any systematic failures have occurred. If systematic failures have occurred during the certification period, the corrective action that was taken to eliminate the systematic failure(s) will be reviewed to determine that said action followed the approved processes and was effective.
- Safety Manual – The latest version of the safety manual will be reviewed to determine that it meets the IEC 61508 requirements for a safety manual.
- FMEDA Update – If required or requested the FMEDA will be updated. This is typically done if there are changes to the IEC 61508 standard and/or changes to the *exida* failure rate database.
- Evaluate use of the certificate and/or certification mark - Conduct a search of the applicant's web site and document any misuse of the certificate and/or certification mark. Report any misuse of the certificate and/or certification mark to the exida Managing Director.
- Recommendations from Previous Audits – If there are recommendations from the previous audit, these are reviewed to see if the recommendations have been implemented properly.
- Documents submitted for this audit are listed in section 2.4.

7.2.1 Documentation provided by Honeywell Combustion Controls

Note: See Section 2.4.1 for documents that have been revised or added since the previous audits (highlighted in grey).

7.3 Surveillance Results

7.3.1 Procedure Changes

There were no significant changes to the procedures during the previous certification period.

7.3.2 Engineering Changes

There were no significant design changes to these products during the previous certification period.

7.3.3 Impact Analysis

There were no safety-related design changes during the previous certification period.

7.3.4 Field History

The field histories of these products were analyzed and found to be acceptable.

7.3.5 Safety Manual

The updated safety manual was reviewed and found to be compliant with IEC 61508.

7.3.6 FMEDA Update

The FMEDA was not updated as part of this project.

7.3.7 Evaluate use of certificate and/or certification mark

The Honeywell Combustion Controls website was searched, and no misleading or misuse of the certification or certification marks was found.

7.3.8 Previous Recommendations

Previous recommendations for improvement were reviewed and were resolved satisfactorily to the requirements of IEC 61508.

7.4 Surveillance Audit Conclusion

The result of the Surveillance Audit Assessment can be summarized by the following observations:

The Honeywell Combustion Controls 7800 Series Burner Controller and 7823 Flame Switch continues to meet the relevant requirements of IEC 61508:2010 for safety applications up to SIL 3 based on the initial assessment and considering:

- field failure history

- permitted modifications completed on the product

- resolution of past action items

This conclusion is supported by the updated Safety Case and certification documents.

8 Terms and Definitions

Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure 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).
HART	Highway Addressable Remote Transducer
AI	Analog Input
AO	Analog Output
DI	Digital Input
DO	Digital Output
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

9 Status of the document

9.1 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.

9.2 Version History

Contract Number	Report Number	Revision Notes
Q23/07-078	HON 17-02-010 R002 V2R1	Update for surveillance audit; incorporated 7823, RPC, 28-Dec-2023
Q17/02-010	HON 17-02-010 R002 V1R2	Update to include EC models; Dave Butler, 6/30/2018
Q17/02-010	HON 17-02-010 R002 V1R1	Internal revision; Dave Butler, 6/25/2018
Q17/02-010	HON 17-02-010 R002 V1R0	Initial draft and post-review changes; Dave Butler, 12/1/2017

Review: V2R1, Chris O'Brien, 28-Dec-2023
Release status: Released

9.3 Future Enhancements

At request of client.

9.4 Release Signatures

Rudolf P. Chalupa, CFSE, Senior Safety Engineer

Chris O'Brien, CFSE, Partner