



The manufacturer  
may use the mark:



Revision 1.1 June 30, 2018  
Surveillance Audit Due  
January 1, 2021



ANSI Accredited Program  
ISO/IEC 17065  
PRODUCT CERTIFICATION BODY  
#1004

# Certificate / Certificat Zertifikat / 合格証

HCC 1702010 C001

*exida* hereby confirms that the:

**Honeywell 7800 Series Burner Controller**  
**Honeywell International Inc.**  
**Honeywell Thermal Solutions**  
**Golden Valley, MN - USA**

Has been assessed per the relevant requirements of:

**IEC 61508 : 2010 Parts 1-7**

and meets requirements providing a level of integrity to:

**Systematic Capability: SC 3 (SIL 3 Capable)**

**Random Capability: Type B Element**

**SIL 3 @ HFT = 0; Route 1<sub>H</sub>**

**PFH/PFD<sub>avg</sub> and Architecture Constraints  
must be verified for each application**

## **Safety Function:**

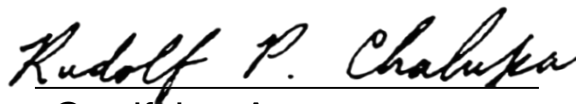
The Honeywell 7800 Series Burner Control system will control the burner according to specific pre-defined sequences. In addition the 7800 Relay Module will monitor for the presence of an acceptable flame signal or hardwired inputs with transition to Safety Shutdown (Lockout) upon loss of flame or other inputs.

## **Application Restrictions:**

The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.



  
Evaluating Assessor

  
Certifying Assessor

HCC 1702010 C001

**Systematic Capability: SC 3 (SIL 3 Capable)****Random Capability: Type B Element****SIL 3 @ HFT=0; Route 1<sub>H</sub>****PFH/PFD<sub>avg</sub> and Architecture Constraints  
must be verified for each application****Honeywell 7800 Series  
Burner Control****Systematic Capability:**

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

**Random Capability:**

The SIL limit imposed by the Architectural Constraints must be met for each element.

**IEC 61508 Failure Rates in FIT\***

Device	SD	SU	DD	DU
7800 Series Burner Control System	286	31	277	5

\* FIT = 1 failure / 10<sup>9</sup> hours

**SIL Verification:**

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH/PFD<sub>avg</sub> considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

**Assessment Report:**

HON 17-02-010 R002 V1R2 IEC 61508 Assessment Report - 7800

**Safety Manual:**

RM 7800 Burner Controller Safety Manual, V2R0



80 N Main St  
Sellersville, PA 18960



## **Results of the IEC 61508 Functional Safety Assessment**

Project:

7800 Series Burner Controller

Customer:

Honeywell Thermal Solutions  
Golden Valley, MN  
USA

Contract No.: Q17/02-010

Report No.: HON 17-02-010 R002

Version V1, Revision R2, 6/30/2018

Dave Butler



## Management Summary

The Functional Safety Assessment of the Honeywell Thermal Solutions  
7800 Series Burner Controller

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

- *exida* assessed the development process used by Honeywell Thermal Solutions 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 the manufacturing quality system in use at Honeywell Thermal Solutions.

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 Honeywell Thermal Solutions 7800 Series Burner Controller development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.**

**The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the 7800 Series Burner Controller can be used in a low demand safety related system in a manner where the  $PFD_{AVG}$  is within the allowed range for SIL 3 ( $HFT = 0$ ) according to table 2 of IEC 61508-1.**

**The assessment of the FMEDA also shows that the 7800 Series Burner Controller 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 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 3.1 of 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 / Literature used .....	6
2.4 Reference documents.....	<b>Error! Bookmark not defined.</b>
2.4.1 Documentation provided by Honeywell Thermal Solutions .....	6
2.4.2 Documentation generated by exida .....	9
2.5 Assessment Approach .....	10
3 Product Description .....	11
3.1 Hardware and Software Version Numbers .....	12
4 IEC 61508 Functional Safety Assessment Scheme.....	13
4.1 Product Modifications .....	13
5 Results of the IEC 61508 Functional Safety Assessment .....	14
5.1 Lifecycle Activities and Fault Avoidance Measures .....	14
5.1.1 Safety Lifecycle and FSM Planning .....	15
5.1.2 Documentation.....	16
5.1.3 Training and competence recording .....	16
5.1.4 Configuration Management .....	16
5.1.5 Tools (and languages) .....	17
5.2 Safety Requirement Specification.....	18
5.3 Change and modification management .....	18
5.4 System Design.....	19
5.5 Hardware Design and Verification .....	20
5.5.1 Hardware architecture design.....	20
5.5.2 Hardware Design / Probabilistic properties .....	21
5.6 Software Design.....	21
5.7 Software Verification .....	23
5.8 Safety Validation .....	24
5.9 Safety Manual .....	25
6 Terms and Definitions .....	26
7 Status of the document .....	28
7.1 Liability .....	28
7.2 Releases .....	28
7.3 Future Enhancements .....	28
7.4 Release Signatures .....	28

## 1 Purpose and Scope

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

7800 Series Burner Controller

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

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

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

and

- the 7800 Series Burner Controller 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 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 *exida*'s quality procedures and scope definitions.

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 build 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 the assessment tool, and are summarized within this report.

The assessment was planned by *exida* and agreed with Honeywell Thermal Solutions (see [R2]).

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



## 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

Honeywell Thermal Solutions                      Manufacturer of the 7800 Series Burner Controller

*exida*    Performed the hardware assessment [R3]

*exida*    Performed the Functional Safety Assessment [R1] per the accredited *exida* scheme.

Honeywell Thermal Solutions 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.

Doc. ID	Standard	Title
[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 2014 audit are listed in Section 6 2018 Update to add EC model project documents.

#### 2.4.1 Documentation provided by Honeywell Thermal Solutions

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	
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		Exp.: 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	
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	LightBlueAllList_MechanicalDesign.xlsx		11/7/2017
D056	Downstream+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
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

## 2.4.2 Documentation generated by *exida*

Doc. ID	<i>exida</i> Document Filename	Description
[R1]	HON 17-02-010 V1R1 61508 SafetyCaseWB - 7800.xlsm	Safety Case Workbook
[R2]	Q1702010r1 Light Blue Certification Proposal.pdf	Assessment Plan
[R3]	FMEDAx Honeywell Light Blue Project.nefm	FMEDA

## 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 Thermal Solutions.

The following IEC 61508 objectives were subject to detailed auditing at Honeywell Thermal Solutions:

- 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

The certification audit was done in Golden Valley, MN on 10/24/2017.

### 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 Series Burner Controllers are used for UL/CSA On/Off, UL/CSA Modulating, and FM/IRI Modulating burner applications. The 7800 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 Series include automatic burner sequencing, flame supervision, axillary burner management safety functions, system status indication, system or self-diagnostics and troubleshooting.

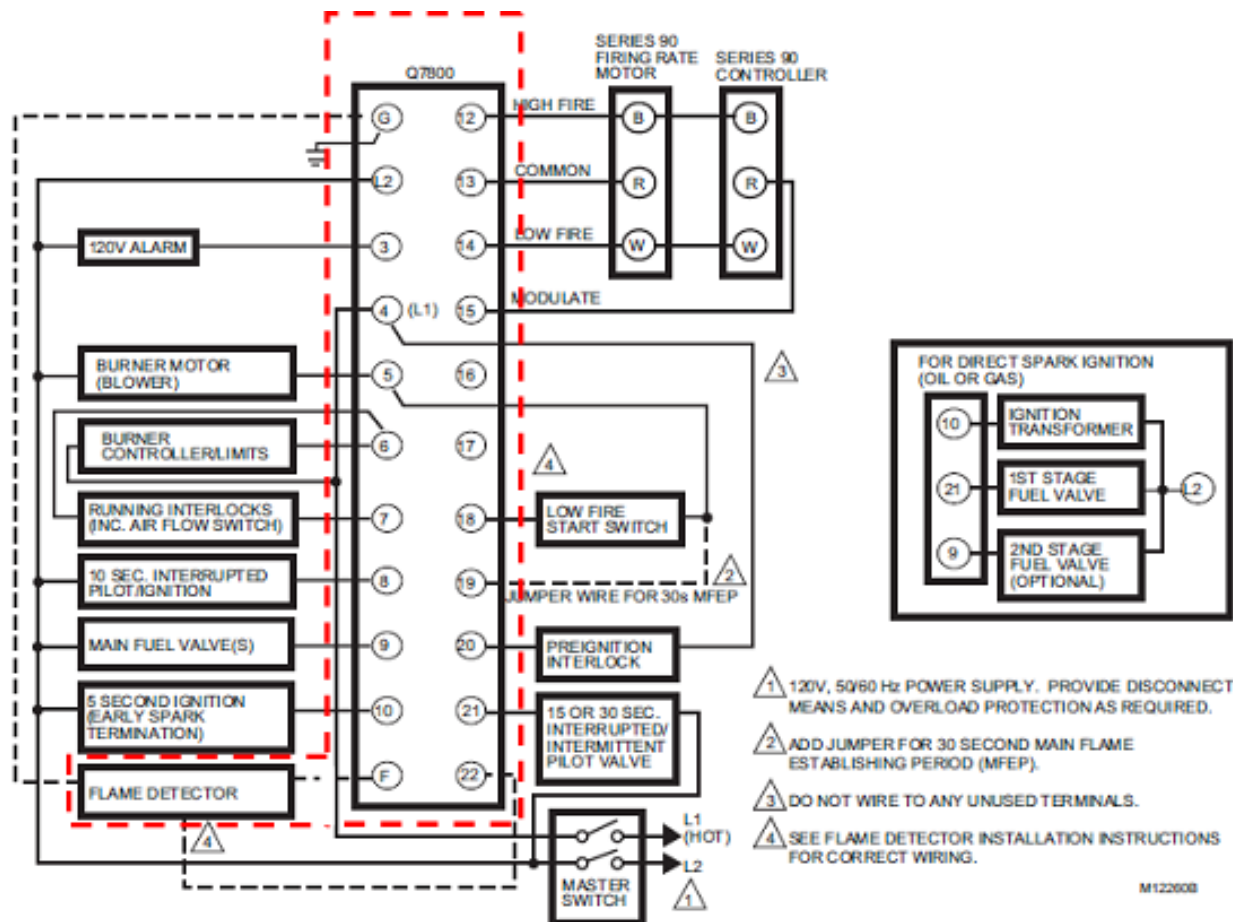


Figure 1: Controller and Sensor/Flame Detector



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	4
RM7824	4	RM7896	6	C7009A	1		
RM7830	5	RM7897	6				
RM7838	9	RM7898	6	C7915A	1	R7852B	1
RM7840*	8						
RM7845	3	EC7820	7	C7012E	1		
RM7850	5	EC7830	6	C7012F	1		
RM7865	4	EC7840	5	C7024E	7	R7824C	2
RM7885	5	EC7850	6	C7024F	5	R7847C	4
RM7888	5	EC7890	5	C7061A	1	R7851C	1
RM7890	9	EC7895	5	C7061F	1	R7861A	1
				C7076A	1	R7886A	2
				C7076D	1		
				C7961E	1		
				C7961F	1		

\*NOTE: RM7840E1016, RM7840L1018 and RM7840L1026 are Series 5

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

The 7800 Series Burner Controller is classified as a Type B<sup>1</sup> 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 - Hardware and Software Versions**

Variant/Model	Hardware Version	Software Version
RM78xx models listed in <b>Table 1</b>	Rev. -003	5015
EC78xx models listed in <b>Table 1</b>	Rev. -001	5015

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

## 4 IEC 61508 Functional Safety Assessment Scheme

*exida* assessed the development process used by Honeywell Thermal Solutions for this development project against the objectives of the *exida* certification scheme. The results of the assessment are documented in [R1]. All relevant objectives of the standard have been met by the Honeywell Thermal Solutions development processes during this development project.

*exida* audited and assessed project and product documentation for compliance with the functional safety requirements of IEC 61508. During an evaluation period, an assessor updated a safety case with the results of the assessment. The safety case documents the development project's compliance with the functional safety management requirements of IEC 61508, parts 1 through 3. Evaluation was followed by a certification review of the safety case, in which a review of a subset of the most important requirements, and a spot inspection of the remaining requirements, was carried out to ensure high quality of the safety case.

The detailed development audit (see [R1]) evaluated the compliance of the processes, procedures and techniques, as implemented for the Honeywell Thermal Solutions 7800 Series Burner Controller, with IEC 61508.

The assessment, executed using the *exida* certification scheme, tailors the IEC 61508 requirements to the scope of the development activities and the development team.

The results of the assessment show that the 7800 Series Burner Controller is capable for use in SIL 3 applications, when properly designed into a Safety Instrumented Function per the requirements and constraints specified in the Safety Manual.

### 4.1 Product Modifications

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

As part of the *exida* scheme, to renew the certificate, a surveillance audit must be conducted just prior to the expiration of the certification period. The surveillance audit includes a review of modifications made during the certification period, to show compliance with the assessed modification process. The modification documentation listed below is submitted and reviewed as part of the surveillance audit.

- List of all anomalies reported
- List of all modifications completed
- Safety impact analysis which documents, with respect to each 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 Thermal Solutions 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 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 Thermal Solutions 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 of the processes, procedures and techniques as implemented for the product development with the requirements of IEC 61508. 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.**

#### Objectives

- Structure, in a systematic manner, the phases in the overall safety lifecycle that shall be considered to achieve the required functional safety of the safety-related systems.
- Structure, in a systematic manner, the phases in the safety lifecycle that shall be considered to achieve the required functional safety of the safety-related systems.
- Specify the management and technical activities during the safety lifecycle phases which are necessary for the achievement of the required functional safety of the safety-related systems.
- Specify the responsibilities of the persons, departments and organizations responsible for each 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 safety-related systems throughout the safety lifecycle.
- Document key information relevant to the functional safety of the safety-related systems throughout the overall safety lifecycle.
- Specify the necessary information to be documented in order that all phases of the safety lifecycle 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.



### 5.1.1 Safety Lifecycle and FSM Planning

#### Assessment

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.

Manufacturer has a quality management system (QMS) in place. The Manufacturer has been ISO 9001 certified. All sub-suppliers have been qualified through the Manufacturer Qualification procedure.

All phases of the safety lifecycle have verification steps described in the FSM plan, the ASDP Tailoring Plan for the development phases.

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.

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

- (1) which software modules are impacted and
- (2) which earlier safety lifecycle activities shall be repeated.

Lifecycle Phase Verification results are documented according to the verification plan and available for assessment.

#### Conclusion:

The Safety Lifecycle and FSM Planning objectives of the standard are fulfilled by the Honeywell Thermal Solutions functional safety management system and product development processes.

### 5.1.2 Documentation

#### Assessment

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.

All safety related documents are required to meet the following requirements:

- Have titles or names indicating scope of the contents
- Contain a table of contents
- Have a revision index which lists versions of the document along with a description of what changed in each version
- Documents must be searchable electronically

Several documents were sampled and found to meet these requirements.

A Documentation Management System is used to contain documentation.

There are many templates provided online for documents that require the above properties.

#### Conclusion

The Documentation objectives of the standard are fulfilled by the Honeywell Thermal Solutions functional safety management system.

### 5.1.3 Training and competence recording

#### Assessment

The FSM Plan lists the key people working on the project along with their roles. See the FSM Plan for list of project personnel. Also, there is an online list of personnel and the roles they fill.

A competency matrix has been created and includes the following:

- a) Competency requirements for each role on project.
- b) List of people who fulfill each role
- c) List of competencies for each individual matched up to required competencies based on roles that they fill.
- d) Training planned to fill any competency gaps.

#### Conclusion

The objectives of the standard are fulfilled by the Honeywell Thermal Solutions functional safety management system and internal organizational procedures.

### 5.1.4 Configuration Management

#### Assessment

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.

## **Conclusion**

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

### **5.1.5 Tools (and languages)**

#### **Assessment**

All tools which support a phase of the software development lifecycle, and cannot directly influence the safety-related system during its run time (Off-line support tools) are documented, including tool name, manufacturer name, version number, use of the tool on this project. This includes validation test tools.

All off-line support tools have been classified as either T3 (safety critical), T2 (safety-related), or T1 (interference free).

All off-line support tools in classes T2 and T3 have a specification or product manual which clearly defines the behavior of the tool and any instructions or constraints on its use.

An assessment has been carried out for T2 and T3 offline support tools, to determine the level of reliance placed on the tools, and the potential failure mechanisms of the tools that may affect the executable software. Where such failure mechanisms are identified, appropriate mitigation measures have been taken.

The following information is documented for all off-line support tools classified as either T2 or T3:

- All configuration baseline items for which  
the tool is used.

- The tool configuration (compiler options,  
batch files, scripts, etc. for each different  
use of the tool.)

See section 6.2 of the functional safety management plan (FSMP).

For each tool in class T3, evidence is available that the tool conforms to its specification or manual through a combination of confidence from use and tool validation. If evidence is not available for a given tool, measures to control faults introduced by the tool are implemented to control a failure caused by the fault.

For each tool in class T3, if tool validation was performed, the results of the validation were documented and the tool validation checklist was completed.

A Software Tool Upgrade Procedure exists and discusses the procedure to requalify an offline software tool.

## **Conclusion**

The objectives of the standard are fulfilled by the Honeywell Thermal Solutions functional safety management system.

## 5.2 Safety Requirement Specification

### Objectives

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, to achieve the required functional safety.

### Assessment

All element safety functions necessary to achieve the required functional safety are specified, including, as appropriate:

- functions that enable the EUC to achieve or maintain a safe state;
- functions related to the detection, annunciation and management of sensor and actuator faults;
- functions that allow the PE system to be safely modified;
- safety-related communications (see 7.4.11 of IEC 61508-2);
- safety accuracy and stability for measurement and control (if required).

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 the SRS has enough detail such that the required SIL can be achieved during design and implementation, and can be assessed. 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.

All safety related constraints between the software and hardware have been documented in the Software Safety Requirements or other suitable requirements document.

### Conclusion

The objectives of the standard are fulfilled by the Honeywell Thermal Solutions functional safety management system and use of requirements management tools.

## 5.3 Change and modification management

### Assessment

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.



A 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.

The Software Modification Procedure 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.

## **Conclusion**

The objectives of the standard are fulfilled by the Honeywell Thermal Solutions functional safety management system, change management procedures, and sustaining product procedures.

## **5.4 System Design**

### **Assessment**

System or subsystem design has been partitioned into subsystems, and interfaces between subsystems are clearly defined and documented.

The System Architecture Design clearly identifies that all components are developed to the target SIL.

The System Architecture Design 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 expresses the design in terms of:

- functionality
- information flow between elements
- sequencing and time relationships
- timing constraints
- concurrency/synchronization
- data structures
- design assumptions
- exception handling
- structural views
- behavioral views

The Software Design is well understood by the developers, and is documented in a way that can be easily verified.

## **Conclusion**

The objectives of the standard are fulfilled by the Honeywell Thermal Solutions functional safety management system and new product development processes.

## **5.5 Hardware Design and Verification**

### **Objectives**

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

- Create 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 meet 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.

### **5.5.1 Hardware architecture design**

#### **Assessment**

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.

## **Conclusion**

The objectives of the standard are fulfilled by the Honeywell Thermal Solutions functional safety management system and new product development processes.

### **5.5.2 Hardware Design / Probabilistic properties**

#### **Assessment**

To evaluate the hardware design of the 7800 Series Burner Controller, a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida* for each component in the system. This is documented in [R3]. Assumptions taken in the FMEDA were verified using Fault Injection Testing as part of the development (see the Fault Injection Test Plan [D77]) and as part of the IEC 61508 assessment.

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration. An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with 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 failure rates must be considered in combination with those of other devices, and the calculation of a  $PFD_{AVG}$  for a Safety Instrumented Function (SIF) to determine suitability for a specific Safety Integrity Level (SIL).

#### **Conclusion**

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

### **5.6 Software Design**

#### **Objectives**

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.

## **Assessment**

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 software criticality analysis (SCA) / SW HAZOP was performed and criticalities have been documented.

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. For example, the Burner Controller module implements:

- Periodic Galloping pattern test
- Redundant Memory with comparison
- CRC of ROM
- Address Bus Test
- Check for key bit processing errors in safety key exchange with safety micro
- many others

The Software Design describes the design features that maintain the safety integrity of data.

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.

Restarts are done when faults are detected.

The Software Design does not dynamically allocate memory.

An SCA / SW HAZOP analysis has been completed on the software, however, no SIL reduction is claimed for software components.

## **Conclusion**

The objectives of the standard are fulfilled by the Honeywell Thermal Solutions functional safety management system.



## 5.7 Software Verification

### Objectives

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.

### Assessment

The Software Architecture Design was reviewed. This review would confirm that the architecture fulfills the safety requirements. In addition, if the notation was ambiguous, it would be pointed out by the reviewers. All action items required to be addressed were submitted to the action item tracking system and have been resolved.

Modular approach: 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.

Structural test coverage (entry points) of 100% is documented by a tool or a manual trace of test coverage.

Structural test coverage (statements) 100% is documented by a tool or a manual trace of test coverage.

Structural test coverage (branches) 100% is 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.

The product has no safety critical floating-point calculations.

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.

#### **Conclusion:**

The objectives of the standard are fulfilled by the Honeywell Thermal Solutions functional safety management system, software development process, and new product development processes.

## **5.8 Safety Validation**

### **Objectives**

- Ensure that the design and implementation of the safety-related systems meets the specified safety functions and safety integrity requirements.
- Plan the validation of the safety of the safety-related systems.
- Validate that the 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.

### **Assessment**

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.

The following information is documented in the test results:

- a) a record of validation activities, permitting validation results to be reproduced and/or retraced.
- b) The version of the validation plan used to execute the test.
- c) The safety function associated with each test case.
- d) The tools and equipment and calibration data.
- e) The Configuration Identification of the Item Under Test.

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.

## **Conclusion**

The objectives of the standard are fulfilled by the Honeywell Thermal Solutions functional safety management system, software development process, and new product development processes.

## **5.9 Safety Manual**

### **Objectives**

- Develop procedures to ensure that the required functional safety of the safety-related system 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.

The Safety Manual gives guidance on recommended periodic (offline) proof test activities for the product, including listing any tools necessary for proof testing. Procedures for maintaining tools and test equipment are listed.

All routine maintenance tools and activities required to maintain safety are identified and described in the Safety Manual.

The Safety Manual identifies all security measures that are implemented against potential threats or vulnerabilities.

The user manual defines what configuration options and methods exist for the product. The safety manual documents any recommended configurations and any features that may not be used.

### **Conclusion**

The objectives of the standard are fulfilled by the Honeywell Thermal Solutions functional safety management system and the safety manual.



## 6 2018 Update to add EC model project documents

### 6.1 Update Methodology

As part of the update to the certificate the following aspects have been reviewed:

- 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.
- Impact Analysis – If changes were made to the product design, the impact analysis associated with the change is reviewed to see that the functional safety requirements for an impact analysis have been met.
- Safety Manual – The latest version of the safety manual is reviewed to determine that it meets the IEC 61508 requirements for a safety manual.

#### 6.1.1 Documentation provided by Honeywell Thermal Solutions

File	Vers.	Date
ChangeLog-5004to5013.xlsx		
JIRA_Report.pdf		Snapshot
LTB-802_ImpactAnalysis.docx	Rev. 1	12/19/2017
LTB-821_LTB-823_ImpactAnalysis.docx	Rev. 1	1/4/2018
LTB-858_LTB-837_ImpactAnalysis.docx	Rev. 1	1/18/2018
LTB-871_ImpactAnalysis.docx	Rev. 1	2/26/2018
LTB-873_ImpactAnalysis.docx	Rev. 1	2/26/2018
LTB-903_ImpactAnalysis.docx	Rev. 1	2/26/2018
LTB-984_ImpactAnalysis.docx	Rev. 1	2/27/2018
LTB-985_ImpactAnalysis.docx	Rev. 1	2/27/2018
LTB-989_LTB-995_ImpactAnalysis.docx	Rev. 1	2/27/2018
LTB-991_ImpactAnalysis.docx	Rev. 1	2/27/2018
LTB-1012_LTB-1021_ImpactAnalysis.docx	Rev. 1	2/27/2018
LTB-1036_ImpactAnalysis.docx	Rev. 1	2/27/2018
LightBluePlatformDifferences.xlsx		5/7/2018
SVNReport_BC.txt		5/7/2018
40013 LightBlue SW REV 5015 Test Summary.docx		6/15/2018
Safety+architecture+tests.doc	Rev. 1	10/13/2017

### 6.1.2 Surveillance Documentation generated by *exida*

[R4]	17-02-010 R005 V1R0 7800 Light Blue (EC models) Update Assessment.docx	IEC 61508 SafetyCaseWB for 7800 Series Burner Controller
------	--	--

## 6.2 Update Results

### 6.2.1 Engineering Changes

All engineering changes were for the purposes of creating variant products by adapting the core product. All engineering changes were performed per the assessed modification process, including impact analysis, and development procedures. Engineering artifacts were assessed and found to be adequate.

### 6.2.2 Safety Manual

The updated safety manual was reviewed and found to be compliant with IEC 61508:2010.

## 7 Terms and Definitions

Term	Definition
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 <sup>-9</sup> 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 <sub>AVG</sub>	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.
SIL	Safety Integrity Level



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

## 8 Status of the document

### 8.1 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.

### 8.2 Releases

Contract Number	Report Number	Revision Notes
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

Authors: Dave Butler

Review: Rudy Chalupa, 6/29/2018

Release status: Released

### 8.3 Future Enhancements

At request of client.

### 8.4 Release Signatures

Dave Butler, Senior Safety Engineer

Rudy Chalupa, Senior Safety Engineer