Certificate / Certificat

Zertifikat / 合格証

HCC 1901116 C001

exida hereby confirms that the:

Honeywell 7823 Flame Switch

Honeywell Process Solutions

Honeywell Thermal Solutions (HTS)
Houston, TX 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_H

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Safety Function:

The Honeywell 7823 Flame Switch will de-energize a relay output for loss of flame and transition to the safe state.

Application Restrictions:

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

The manufacturer may use the mark:

Revision 1.0 October 10, 2019
Surveillance Audit Due
October 1, 2022

exida Certification

John C Yozallinas
Evaluating Assessor

David Smith
Certifying Assessor

ISO/IEC 17065
PRODUCT CERTIFICATION BODY
#1004

Certificate / Certificat / Zertifikat / 合格証

HCC 1901116 C001

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 3 @ HFT=0; Route 1_H

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

Honeywell 7823 Flame Switch

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*

Options	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
7823 using Ampli-Check™	246	189	117	3.1	99.4%
7823 using Self-Check™	272	189	130	3.7	99.4%

* FIT = 1 failure / 10^9 hours

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH/PFD_{avg} 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 19-01-116 R001 V1R2 and higher

Safety Manual:

RM 7800 Burner Controller Safety Manual, V3R2 and higher

80 N Main St
Sellersville, PA 18960

Results of the IEC 61508 Functional Safety Assessment

Project:
Honeywell 7823 Flame Switch

Customer:
Honeywell Process Solutions
Honeywell Thermal Solutions
Houston, TX
USA

Contract No.: Q19/01-116
Report No.: HON 19-01-116 R001
Version V1, Revision R2, October 2, 2019
John Yozallinas

Management Summary

The Functional Safety Assessment of the Honeywell Thermal Solutions

7823 Flame Switch

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 7823 Flame Switch 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 7823 Flame Switch 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 according to Table 2 of IEC 61508-1.

The assessment of the FMEDA also shows that the 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 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 3.1 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:

7823 Flame Switch

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 7823 Flame Switch with the technical requirements of IEC 61508-2 and -3 for SIL 3 and the derived product safety requirements

and

- the 7823 Flame Switch development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial requirements of IEC 61508-1, -2 and -3 for SIL 3.

and

- the 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 *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 accredited *exida* certification 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 500 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 Thermal Solutions	Manufacturer of the 7823 Flame Switch
exida	Performed the hardware assessment [R3]
exida	Performed the Functional Safety Assessment [R1] per the accredited *exida* certification scheme.

Honeywell Thermal Solutions contracted *exida* with the IEC 61508 Functional Safety Assessment of the above-mentioned device.

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

2.4.1 Documentation provided by Honeywell Thermal Solutions

Doc. ID	Typical Name	Project Document Filename	Version	Date
D001	Quality Manual	ECC Global Quality Systems Manual.pdf	Issue 7	10/3/2014
D003	Overall Development Process	ECC New Product Introduction Process Swimlane.pdf (includes a set of process templates and instructions cited in Safety Case D003b thru D003k)	Rev. M	2011
D004	Configuration Management Process - Engineering Change	EP4.1.1_Y Eng Change Orders.pdf	Y	8/1/2015

Doc. ID	Typical Name	Project Document Filename	Version	Date
D004b	Configuration Management Process - SW Release and Change	EP4.16.6_F Software Change Process.pdf	F	4/1/2013
D005	Field Failure and Return Reporting Procedure	70-0568_WarrantyPolicy.pdf	Rev. 10-15	Oct.2015
D005b	Field Failure Reporting Procedure-FLexG	RMA process Flow.pptx	n/a	Sep.2017
D007	Manufacturer Qualification Procedure	Supplier Approval Process.pdf	Rev. 5.5	n/a
D007b	Manufacturer Qualification Procedure	Supplier Approval Process Procedure Sheet PS-3.4.doc	17	Sep.2014
D008	Part Selection Procedure	DA3.5.2_A Conditional Qualification Testing.pdf	Rev. A	12/1/2015
D010	Quality Management System (QMS) Documentation Change Procedure	EP4.1.1_Y ECRO Process.pdf	Rev. Y	8/1/2015
D012	Non-Conformance Reporting procedure	eCATS_Users_Guide.doc	n/a	(c) 2010
D012b	Non-Conformance Reporting procedure	CHP14.pdf	Rev. P	9/25/2016
D013	CAPA and Action Tracking Procedure	711680_Kettos ASDP Quality Plan.docx	Rev. 2	9/24/2014
D019	Customer Notification Procedure	LightBlue Functional Safety Management Plan FSM.docx	Rev. 1.7	Sep.2019
D021	Software Development Process	ASDP Software Development Lifecycle.pdf	Screenshot	
D021b	Software Tool Qualification Procedure	SLATE Software Tool Qualification Procedure.doc	n/a	6/28/2016
D021c	Software Tool Qualification Procedure - IAR Cert	IAR Certified tools.pdf	n/a	6/28/2016
D021d	Software Tool Qualification Procedure - IAR FAQ	IAR Certified tools FAQ.pdf	n/a	6/28/2016

Doc. ID	Typical Name	Project Document Filename	Version	Date
D023	Modification Procedure	EP4.1.1_Y ECRO Process.pdf	Rev. Y	8/1/2015
D023b	Impact Analysis Template	SIL-3 Impact Analysis Template.docx	rev. 1	8/25/2016
D023c	Modification Procedure	EP4.16.6_F Software Change Process.pdf	Rev. F	4/1/2013
D023d	Modification Procedure - Prod. Safety	EP 3.20.1_E PRODUCT SAFETY & EMC LISTING.pdf	Rev. E	4/1/2013
D023e	Modification Procedure - Form, Fit, Function	EP 4-3_D_1_D Form Fit or Function.pdf	Rev. D	12/1/2008
D026	FSM Plan or Development Plan	LightBlue Functional Safety Management Plan FSM.docx	Rev. 1.7	Sep.2019
D026b	FSM Plan or Development Plan	Light Blue Project Plan.docx	Rev. 5	10/25/2017
D027	Configuration Management Plan	Light Blue Configuration Management Plan.doc	Rev. 2	3/23/2017
D029	Verification Plan	40013_LightBlue_quality_assurance_plan.xlsx	Rev. .01	10/13/2017
D029b	Verification Plan - Code review checklist	LightBlue-CodeReviewChecklist.docx	Rev. 0.06	Oct.2017
D032	Job Descriptions and Competency Levels	D032_Job Descriptions and Competency Levels	many	Oct.2017
D034	Skills Matrix	Light Blue SkillsMatrix.xlsx	n/a	10/23/2017
D034b	Skills Matrix	Unity_ Light Blue (728207).pdf	n/a	10/15/2017
D036	ISO 900x Cert or equivalent	Guadalajara North ISO 9001 2015 del 2018 al 2021.pdf	n/a	Exp.: Dec.2021
D038	List of Design Tools	LightBlue Design Tools.docx	Rev. 0.4	Sep.2019
D040	Safety and SW Requirements Specification	SafetyArchitecture - ASDP Requirements.doc	1 (for 7823)	Aug.2019
D040b	Safety and SW Requirements Specification	Safety Architecture and Requirements RM7800.docx	1 (for 7800)	Oct.2017
D041	Safety Requirements Review	SafetyArch_Review.PNG	n/a	Jul.2017
D041b	Safety Requirements Review - notes	REVIEW IN CONTOUR.txt	n/a	Jul.2017
D045	System Architecture Design Specification	7823_FS Safety Relay Module Description.doc	1	Aug.2019

Doc. ID	Typical Name	Project Document Filename	Version	Date
D045b	System Architecture Design Specification	LightBluePlatformDifferences.xlsx	1	Oct.2018
D045c	System Architecture Design Specification - SIO	sio00L_vp_2009_12_18.pdf	1	Dec.2007
D049	High Level Software Design Specification	Burner Control Software Architecture.docx	4	Sep.2017
D050	SW HAZOP or Criticality Analysis	Honeywell Light Blue HAZOP Report V0R1.doc	V0R1	Oct.2017
D050b	SW HAZOP or Criticality Analysis	RE 20170725 Minutes of LightBlue SIL3 - Architecture Audit Review - Few SW Questions.msg	n/a	7/25/2017
D051	Detailed Software Design Specification	_Software Detailed Design (Contour).docx	1	Sep.2017
D051b	Detailed Software Design Specification - 7823	7823_FS Safety Relay Module Description.doc	n/a	Jul.2019
D051c	Detailed Software Design Specification-SafetyKey	Software+Tasks+that+Contribute+to+the+Safety+Key.doc	1	Aug.2019
D051d	Detailed Software Design Specification-NGPL	ngpl.txt	1	Jul.2004
D051e	Detailed Software Design Specification - OS	OS SDD.doc	1	Sep.2017
D051f	Detailed Software Design Specification - RAMcheck	RAMcheck module SDD.doc	1	9/5/2017
D051g	Detailed Software Design Specification - SafetyVars	Safety Vars SDD.doc	1	9/5/2017
D053	Design Review Record - HW Flame Sense	FlameSenseConceptReview.docx	n/a	5/10/2016
D053b	Design Review Record - concept review	HCC 7823 Flame Switch Review Notes.docx	n/a	Nov.2018
D053c	Design Review Record - Schem. rev.	Light Blue Design Review.docx	n/a	6/27/2016
D053e	Design Review Record - FMEA	LightBlue7823rev5_FMEA.xlsx	5	Jun.2019
D054	Verification Results	REV-14601.png	screenshot	Mar.2018

Doc. ID	Typical Name	Project Document Filename	Version	Date
D054b	Verification Results	REV-15541.png	screenshot	Mar.2018
D056	Requirements Traceability Matrix - Contour Note	RE Exida-Traceability-Meeting notes 20171013.msg	n/a	Oct.2017
D056c	Requirements Traceability Matrix - General	Traceability+Report.pdf	n/a	Sep.2019
D056d	Requirements Traceability Matrix - forward	Donwstream+Traceability+Report.pdf	export	Oct.2017
D056e	Requirements Traceability Matrix - backward	Upstream+Traceability+Report.pdf	export	Oct.2017
D057	Software Test Coverage Analysis Report	FLAME_FULL_REPORT.html	snapshot	Sep.2019
D057b	Software Test Coverage Analysis Report	SAFETY_RELAY_FlameSwitch_FULL_REPORT.html	snapshot	Sep.2019
D057c	Software Test Coverage Analysis Report- Relay	ENV_REL_HW_FlameSwitch_FULL_REPORT.html	snapshot	May.2019
D057d	Software Test Coverage Analysis Report	OPTO_SAMPLING_full_report.html	snapshot	Sep.2017
D058	Code Review Record	CodeReview_ECLGBHL-CR-148.txt	n/a	Oct.2018
D058b	Code Review Record	CodeReview_ECLGBHL-CR-161.txt	n/a	May.2019
D059	Fault Injection Test Plan	HCC 18-10-152 R002 V0R3 FIT List 7823A.xls		7/1/2019
D060	Coding Standard	Kettos Coding Standard ver 1.15 31Oct2016.docx	Rev. 1.15	10/31/2016
D061	Static Code Analyzer Configuration Description	checker_response_file.txt	n/a	Sep.2019
D062	Static Code Analysis Results	FlameSwitch_Coverity_Screen1.png	screenshot	Sep.2019
D062b	Static Code Analysis Results	SecurityReport_FlameSwitch.pdf	n/a	Sep.2019
D064	Module Test Plan	SAFETY_RELAY_FlameSwitch.tst	screenshot	Mar.2018
D064b	Module Test Plan	ENV_REL_HW_FlameSwitch.tst	screenshot	Mar.2018

Doc. ID	Typical Name	Project Document Filename	Version	Date
D066	module test Results	SAFETY_RELAY_FlameSwitch_FULL_REPORT.html	snapshot	May.2019
D066b	module test Results	ENV_REL_HW_FlameSwitch_FULL_REPORT.html	snapshot	May.2019
D066c	module test Results	FLAME_FULL_REPORT.html	snapshot	Oct.2018
D067	Integration Test Plan	RM7823+sw+rev+5028.doc	n/a	Sep.2019
D068	Integration Test Results - 7823	RM_EC7823Flame+Switch+5028+release.xls	n/a	Sep.2019
D068b	Integration Test Results - 7823 summary	40013 LightBlue SW REV 5028 Test Summary.docx	A	Aug.2019
D069	Validation Test Plan	7823TestPlan ECC_DQA.DOC	snapshot	Aug.2019
D069b	Validation Test Plan - witness	Safety related SW tests for 7823 JiKa update.docx	n/a	Aug.2019
D069c	Validation Test Plan	ASDP_TestSuitesSW_manual_7823Specific.doc	export	Aug.2019
D074	Validation Test Results	Test Run ECCDQA.DOC	snapshot	Oct.2018
D074b	Validation Test Results - summary	19Q3_LIGHTBLUE_5028_mod.docx	build 5028	Aug.2019
D074c	Validation Test Results -safety relay	Safety+architecture+tests_saved.xls	snapshot	Oct.2018
D075	Environmental Test Results	60730-2-5_RM7823A&legacy_FLAmp-Brno.doc	n/a	Sep.2019
D075b	Environmental Test Results-Vib	LTBLU-TSTRN-39_Vibration+Test.doc	n/a	Dec.2017
D075c	Environmental Test Results-CE declaration	GAR CE Declaration Manufaturer Controls_EC78_RM78_series.pdf	n/a	Sep.2019
D076	EMC Test Results	HW-Testing-7823-Flame-Switch-rev5-UL.doc	1	Sep.2019
D077	Fault Injection Test Results	HCC 18-10-152 R002 V0R3 FIT List 7823A.xls	R3	Jul.2019
D077b	Fault Injection Test Results -setup1	7823-FIT-setup1-20190718.jpg	snapshot	Jul.2019
D077c	Fault Injection Test Results -setup2	7823-FIT-setup2-20190718.jpg	snapshot	Jul.2019
D078	Operation / Maintenance Manual	32-00230_A.pdf	1	Sep.2019
D079	Safety Manual	Light Blue SafetyManual_HON.docx	V3R2	Oct.2019
D081	Engineering Change Documentation	JIRA_Report_5028.docx	n/a	Aug.2019

Doc. ID	Typical Name	Project Document Filename	Version	Date
D086	Tool Qualification Report	Tool Qualification Report.xlsx	n/a	Sep.2019
D086b	Tool Qualification Report - IAR compiler	IAR Compiler - Validation Of Compliance-EWAVR32-4.21.pdf	Rev. 4.21.1	3/21/2016
D088	Impact Analysis Record	LTB-1135_LTB-1145_ LTB-1146_ImpactAnalysis.docx	n/a	Aug.2019
D089	Test Witness Audit Record	Safety related SW witness tests for 7823 final.docx	n/a	Aug.2019
D089b	Test Witness Audit Record-FIT	HCC 18-10-152 R003 V0R1 FIT WitnessList 7823A_15Aug2019.xlsx	n/a	Aug.2019

2.4.2 Documentation generated by *exida*

Doc. ID	*exida* Document Filename	Description
[R1]	HON 19-01-116 V2R3 61508 SafetyCaseWB – 7823.xlsm, Oct.2019	Safety Case Workbook
[R2]	Q19-01-116_Light Blue 7823 Flame Switch Certification Proposal, Jan.2019	Assessment Plan
[R3]	HCC 18-10-152 R001 V1R3 FMEDA 7823A.pdf, Jul.2019	FMEDA Report

2.5 Assessment Approach

The certification audit was closely driven by requirements of the accredited *exida* certification 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 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 assessment was done in Sellersville with online internet sessions for safety lifecycle audit and test witnessing.

3 Product Description

The Honeywell 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 7823 Flame Switch include flame monitoring, system status indication, system or self-diagnostics and troubleshooting.

The 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.

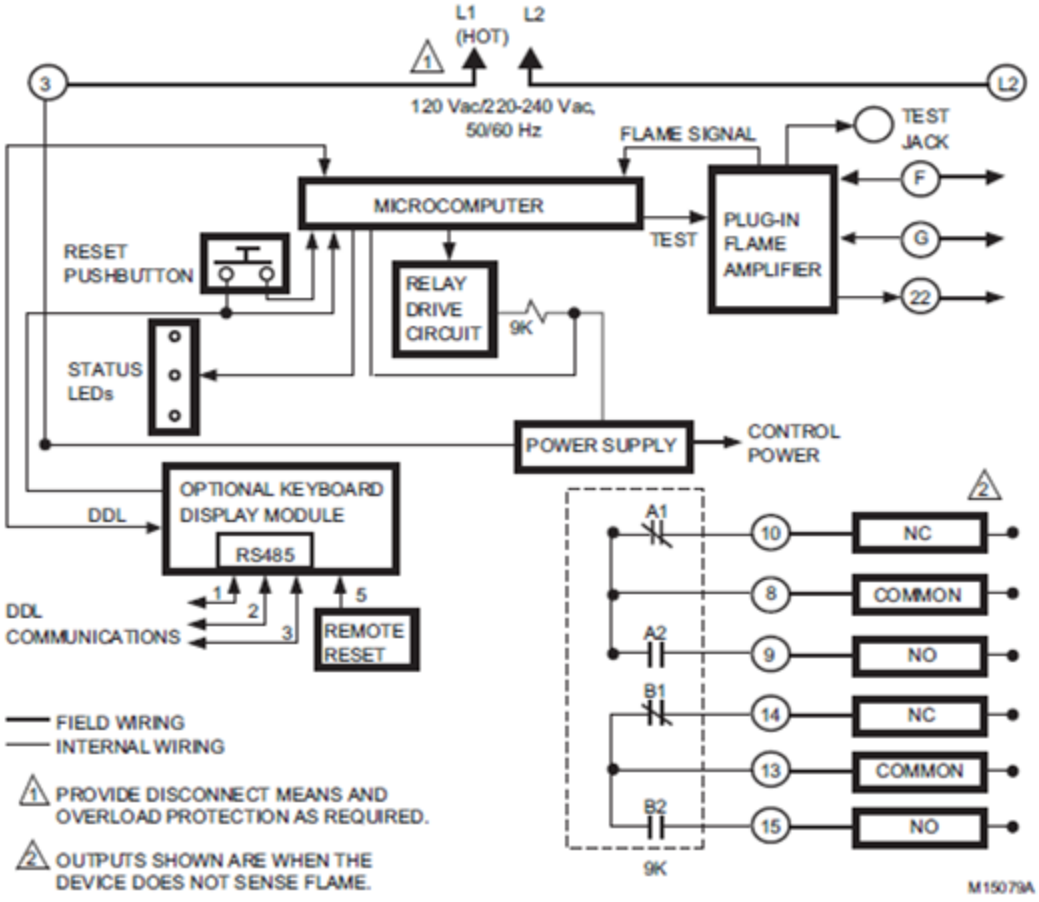


Figure 1: Flame Switch Overview

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

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

3.1 Hardware and Software Versions

This assessment is applicable to the hardware and software versions shown in Table 1. Flame detectors and amplifiers from Table 2, 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 Thermal Solutions for information on version updates or compatibility issues.

Table 1 Version Overview

7823 Flame Switch using Detectors/Amplifiers with Ampli-Check modules (see Table 2)	Hardware: Doc # 32329382, Rev 5 or higher, Jan.2019 Firmware: Build 5028 or higher, Aug.2019
7823 Flame Switch using Detectors/Amplifiers with Self-Check modules (see Table 2)	

Table 2 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 Thermal Solutions for this development project against the objectives of the accredited *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 the assessment 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. Assessment was followed by a certification audit 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 7823 Flame Switch, with IEC 61508.

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

The results of the assessment show that the 7823 Flame Switch is capable for use in SIL 3 safety 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 if they do not affect the safety functions.

As part of the accredited *exida* certification scheme a surveillance audit must be 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 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 accredited *exida* certification scheme which includes IEC 61508 parts 1, 2, & 3 [N1]. The development of the 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 Thermal Solutions has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented in [D003 thru 3k].

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 accredited *exida* certification scheme which includes subsets of IEC 61508 requirements tailored to the SIL 3 work scope of the development team. The result of the assessment can be summarized by the following observations:

The audited development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1.1 Functional Safety Management

Objectives

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

- 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.

Assessment

The functional safety management plan [D026] defines the safety lifecycle for this project. It 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 [D021] identifies the phases of the software development lifecycle and the inputs/outputs associated with each phase.

The Manufacturer has a quality management system [D001] in place and has been ISO 9001 certified [D036]. All Honeywell Thermal Solutions sub-suppliers have been qualified through the Manufacturer Qualification procedure [D007].

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 most 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 Document Management System is used to control documentation. There are many templates provided for documents that support the above properties. The document database is the official repository for all controlled and versioned documents.

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 and Project Plan list the key people working on the project along with their roles and competencies for functional safety. Honeywell Thermal Solutions maintains the skills assessment records for all employees.

A competency matrix has been created and includes the following:

- Competency requirements for each role on project.
- List of people who fulfill each role
- List of competencies for each individual matched up to required competencies based on roles that they fill.
- 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. See section 6 of the functional safety management plan [D026].

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. 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 certification. A Software Tool Upgrade Procedure exists as part of [D038] 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 level 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 faults;
- functions that allow the PE system to be safely modified;
- safety accuracy and response time.

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

All system, operator and software interfaces necessary to achieve the required functional safety level are specified. All safety related constraints between the software and hardware have been documented in the Software Safety Requirements or other suitable design document.

The SRS has been reviewed to verify it has enough detail to support the required SIL can be achieved during design and implementation. The SRS content is available and sufficient for the duties to be performed. This has been confirmed by the validation testing and assessment.

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. The normal design process contains measures to verify and validate the change. 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 [D023b] are documented and indicate the plan for software verification and validation of the modification.

Modification Request/Records will document the reason for the change and have a detailed description of the proposed change. The impact analysis determines 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 allows regression validation for certain modifications.

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 design [D040, D045, D045b] has been partitioned into subsystems and interfaces between subsystems are clearly defined and documented. 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). Code protection (information and/or redundancy for temporal and spatial protection) is considered where needed. Configurations are password protected. Semi-formal methods are used in the design and development.

Formal design reviews are conducted, and the results are recorded; action items are identified, assigned, and resolved. Reviews are documented using software tools.

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 electronic 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.

Hardware architecture design [D045b] 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 [D053e]. Measures against environmental stress and over-voltage are incorporated into the design.

The FSM Plan, development processes, and other work guidelines define the required verification activities related to hardware including documentation, verification planning, test strategy and traceability between requirements and validation test cases.

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 7823 Flame Switch, 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 results must be considered in combination with other devices of a Safety Instrumented Function (SIF) in order to determine the PFD_{AVG} and 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 function to verify the design of that SIF

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 and Verification

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.
- 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 [D040, D049] contains a description of the software architecture. The design is further partitioned into components and modules. 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 Detailed Design describes the design of all diagnostics required to detect faults in software control flow and data flow. The resulting device behavior is specified for any detected fault.

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 [D050] was performed, and module criticality differences have been documented.

A modular approach has been used in the software design. Design has been broken up into modules and functions which have a single entry and a single exit. The Software Architecture Design was reviewed to confirm that the architecture fulfills the safety requirements. All action items required to be addressed were submitted to the action item tracking system and have been resolved.

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. Static analysis tools are used to detect potential problems in the source code or violations of coding rules. The results of Static Analysis of source code are documented [D062, D062b], controlled with project documentation and verified. Therefore, 'C' can be considered a suitable programming language.

Module Test Results [D066, D066b] 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. Structural test coverage is documented by a tool or a manual trace of test coverage.

Integration Test Cases have been successfully run per the Integration Test Plan [D067] and Integration Test Results [D068] have been documented.

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.

5.7 Safety Validation

Objectives

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

- 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 validation 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 [D069] includes the procedure used to properly judge if the validation test is successful. An automated tool is used to manage the traceability of requirements to test cases.

Fault injection testing has been performed on the product as defined in the fault injection test plan [D059]. The results [D077] have been analyzed and adjustments have been made to the FMEDA based on these results.

Validation test results [D074, D074b] are documented, including reference to the test case and test plan version being executed. 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.

The EMC/Environmental Test results [D075, D075b, D076] support the suitability of the 7823 Flame Switch for the specified environmental conditions.

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 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 [D079] is provided and identifies and describes the functions of the product. The functions are described, including a description of the input and output interfaces, with particular focus on use in functional safety applications. This includes behavior for detected failures.

The Safety Manual gives guidance on routine maintenance and 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. The user manual [D078] 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 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 (1x10-9 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.
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

7 Status of the document

7.1 Liability

exida prepares reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

7.2 Releases

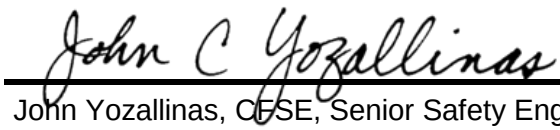
Contract Number	Report Number	Revision Notes
Q19/01-116	HON 19-01-116 R001 V1R1	Initial report; JCY, 2-Oct-2019
Q19/01-116	HON 19-01-116 R001 V1R2	Revised report after internal review; JCY, 9-Oct-2019

Authors: John Yozallinas
Review: David Butler, 10/3/2019
Release status: Released

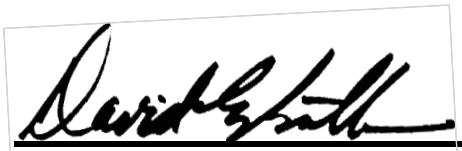
7.3 Future Enhancements

At request of client.

7.4 Release Signatures



John Yozallinas, CFSE, Senior Safety Engineer



David Butler, CFSE, Senior Safety Engineer