Results of the IEC 61508 Functional Safety Assessment

Project:

SLATE™ Burner Control System

Customer:

Honeywell Process Solutions
Golden Valley, MN
USA

Contract No.: Q17/10-158
Report No.: HON 15-11-043 R002
Version V1, Revision R1, December 22, 2017
John Yozallinas

Management Summary

The Functional Safety Assessment of the Honeywell Process Solutions

SLATE™ Burner Control System

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

- *exida* assessed the development process used by Honeywell Process 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 Process 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 Process Solutions SLATE™ Burner Control System **development project, complies with the relevant safety management requirements of IEC 61508 SIL 3**.

The assessment of the FMEDA also shows that the SLATE™ Burner Control System **meet 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 versions of the SLATE™ Burner Control System, specified in section 3.4 of this document, are capable for use in SIL 3 applications in Low demand mode, or High Demand mode, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual. PFD_{AVG} and Architecture Constraints must be verified for each application.

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:

- SLATE™ Burner Control System

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 SLATE™ Burner Control System with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

and

- the SLATE™ Burner Control System 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 SLATE™ Burner Control System hardware analysis represented by the Failure Mode, Effects and Diagnostic Analysis with the relevant requirements of IEC 61508-2.

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

The results of this assessment provide the safety instrumentation engineer with the required failure data per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

1.1 Tools and Methods used for the assessment

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

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

The assessment was planned by *exida* agreed with Honeywell Process 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 Process Solutions	Manufacturer of the SLATE™ Burner Control System
exida	Performed the hardware assessment [R3]
exida	Performed the Functional Safety Assessment [R1] per the accredited *exida* scheme.

Honeywell Process 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.

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

2.4 Reference documents

2.4.1 Documentation provided by Honeywell Process 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

Doc. ID	Project Document Filename	Version	Date
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
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
D021e	SLATE Tools.docx		6/28/2016
D023b	SIL-3 Impact Analysis Template.docx	rev. 1	8/25/2016
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	711680 Kettos Project Development Plan.docx	Rev. 5	9/24/2014
D026c	Slate Functional Safety Management Plan FSM.docx	Rev. 1.3	10/19/2016
D027	711680 Kettos Configuration Management Plan.docx	Rev. 5	9/24/2014
D027b	AID-050 PRS Baseline & Software Version.pdf	screenshot	
D029b	ASDP_CodeReview_Checklist.xlsx	Rev. 1	
D032	Kettos Team List (ACS Unity).pdf		3/8/2016
D034	Skills Matrix.xlsx	n/a	Dec.2017
D036	ISO9001 - 014501_QMS_ENG nov 2015.pdf		exp: 9/14/2018
D040	Kettos Product Requirements Specification.docx	Rev. 1	
D040b	Safety Requirement - Capacity Scalability.doc	Screenshot	
D040c	Safety Requirement - Hardware Fault Tolerance.pdf	Screenshot	
D040d	Kettos-ADR-2100 3rd Party Software.pdf	export	
D040e	Kettos PRS ADR-2101 SIL-3.pdf	Draft	
D040f	Targeted demand mode - SafetySummary.doc		10/18/2016
D040g	Kettos PRS - Tagged Safety Paremeter.docx		10/18/2016
D041	Ref - Burner Control Spec Review.pdf		10/1/2012
D045	Kettos Safety Architecture_1.3_140107.pdf	Rev. 1.3	1/7/2014
D045c	Kettos System Architecture Description.docx	Rev. 3.0	10/19/2016
D049	Kettos Safety Architecture.doc	Rev. 1.6	9/22/2014
D049b	D049_High Level Software Design Specification	Many	
D049c	BurnerSIO.XLS	No rev	No date
D050	D050_SW HAZOP or Criticality Analysis	Many	
D050b	Kettos FMEA support.zip	Many	Dec.2017
D051b	D051_Detailed Software Design Specification	Many	
D051c	OS SDD.doc		5/16/2016
D051d	Slate Limit Module Software Description_140917.pdf		9/17/2014
D051e	BC SDD.doc	Many	
D053	AID-078 KTS-CR-5 Burner Control SDD.msg		11/1/2016
D054	CQ Required Tests.pdf	screenshot	
D054b	CQ4039A Hardware Tests.pdf	Rev. A	1/13/2015
D054c	CQ4113H SLATE Safety Architecture Loop 4a Retest Software Release 2.02.pdf	Rev. A	1/27/2015
D054d	CQ4116A IR Flame Amp & Post CQ Integration Test Program.pdf	Rev. A	8/10/2015
D056	Traceability Example.pdf	Screenshot	Oct.2016

Doc. ID	Project Document Filename	Version	Date
D056b	Safety_Architecture_Traceability.xls	Database export	Oct.2016
D056c	AID-112-SafetyArchitectureRequirementsLinkingAsSafetyRelevant.PNG	Database export	Dec.2017
D056d	AID-113-RequirementDownstreamLinkToTestCase-example.PNG	Database export	Dec.2017
D056e	AID-113-TestCaseUpstreamLinkToTestCase-example.PNG	Database export	Dec.2017
D057	D057_Software Test Coverage Analysis Report	Folder	Nov.2016
D058	KTS-1218 Flame amps code review UVTube SSIR SSUV.pdf		3/19/2015
D058b	KTS-2188 Review limit_block.c module test cases.pdf		8/22/2016
D058c	KTS-2189 LimitBlock_getinput lacks required coverage.pdf		8/22/2016
D058d	Code Review Example description - Analog Cell.pdf		10/21/2016
D058e	Code Review Objectives - Analog Cell.pdf	Screenshot	
D058f	Code Review Checklist (ACS NPI).pdf	1.3.2b	Oct.2016
D059	exida suggested Fault Injection List - Burner, Flame.xls		9/1/2016
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	ECC_Kettos_Burner_Control - Issues.pdf		3/28/2016
D062b	ECC_Kettos_Limit - Issues.pdf		3/28/2016
D062c	ECC_Kettos_FuelAir - Issues.pdf		3/28/2016
D062d	Static Code Analysis Results.zip	many	Dec.2017
D064	SLATE Module Test Plan.docx		8/25/2016
D064b	SLATE Module Test Procedure.doc		
D064c	SW Module Classifications.txt		
D066	D066_module test Results	Many	
D066b	SLATE_unit_tests.zip	Many	Dec.2017
D067	Kettos Test Cases.xlsx		8/25/2016
D067b	UL Test Plan Outine for Slate Modules_updated.xls		8/7/2016
D068c	Integration+Test+Plan+and+Detailed+Results.doc		Dec.2017
D068d	IntegFailedTestSupport.zip		Dec.2017
D070	Electrical Fast Transients Test Case Review.PNG		1/30/2015
D070b	Electrical Fast Transients Test Run Review.PNG		1/17/2015
D075b	Kettos-TSTRN-165 Highly Accelerated Life Test (HALT) Test Results.doc	Rev. 1	8/23/2016
D078	32-00010_A Burner Control Module R8001B2001 I&I.pdf		(C) 2015
D078b	D078_Operation _ Maintenance Manual	Many	
D079	32325298-001 R09 SLATE Safety Manual.docx	Rev. 9	11/3/2016
D080	KTS-2265 Safety Manual Review.pdf		9/2/2016
D081	D081_Engineering Change Documentation	Folder	
D081b	KTS-2329 Burner Control does not exit Postpurge at the programmed time.pdf		9/20/2016
D081c	ECR-0091439 Slate 2.30 Release.pdf		11/11/2016
D085	BurnerCFiles.txt		8/29/2016
D085b	FuelAirCFiles.txt		8/29/2016
D085c	LimitCFiles.txt		8/29/2016
D086	SLATE Tools.docx	n/a	Dec.2017
D086b	IAR Compiler - Validation Of Compliance-EWAVR32-4.21.pdf	Rev. 4.21.1	3/23/2016
D086c	SLATE Tool HAZOP.docx		10/20/2016
D088	Slate 2.30 Impact Analysis - TimN.docx		11/11/2016
D091	UL Release Notes - 15Q1_SLATE2.02_mod.docx	Rev. 1.1	1/20/2015
D091b	SLATE Bootloader-final.pdf		
D091c	Software Release Notes.doc	1.1	Dec.2017
D092	Kettos_Threat_Claims.xlsx		

Doc. ID	Project Document Filename	Version	Date
D092b	Honeywell SLATE Threat Analysis meeting minutes.msg		3/23/2016
D093	SLATEOverview_131220.pdf	Rev. 1.0	12/21/2013
D093b	SLATESystem_150316.pdf		3/16/2015
D093c	SLATEModuleConfig_150723.pdf		7/23/2015
D094	Description of Justification for Honeywell Slate Safety Communications e-mail with history.pdf		3/10/2016

2.4.2 Documentation generated by *exida*

[R1]	HON 15-11-043 V1R5 61508 SafetyCaseWB - SLATE controller.xlsm	Safety Case
[R2]	Q1511043 SLATE Certification ProposalA.pdf	Assessment Plan
[R3]	Honeywell Slate FMEDA Summary Sheet 03-08-2016.xlsx	FMEDA Summary

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 Process Solutions

The following IEC 61508 objectives were subject to detailed auditing at Honeywell Process 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 project teams, not individuals, were audited. Both onsite and remote assessment was performed.

3 Product Description

Descriptions of the SLATE™ Burner Control System (also called "SLATE“ throughout this report) are contained in this section.

3.1 Product Components

3.1.1 Safety and Non-Safety Modules

SLATE includes both SIL-capable safety modules and other modules which are non-safety. It is important to understand the boundaries between them. Each module is responsible for controlling or interacting with a subsystem that is independent of the others, i.e., the safety subsystems are operated independently with regard to the non-safety subsystems and vice versa. Safety modules may also interact if they are working together to control the same subsystem, e.g., Limit module may interact with a Burner Control module when they are both managing the same subsystem. The following figure depicts these boundaries.

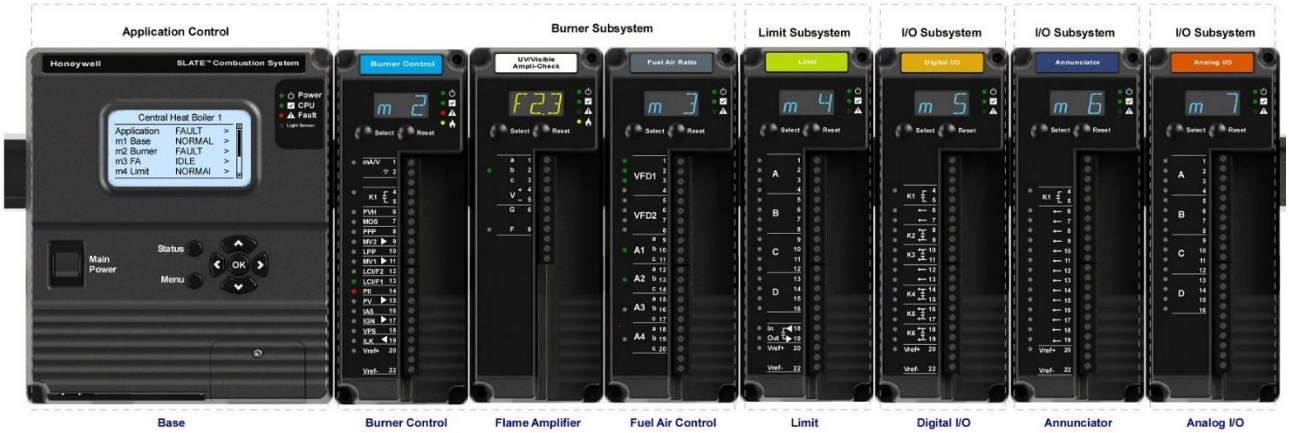

Figure 1 SLATE system with control boundaries

The control boundaries allow for flexible and modular designs that isolate safety functions from the non-safety functions of the system.

It is also important to note that SLATE is scalable in that one or more of any module type may be present in the system. Multiple modules of the same type may be used to control different subsystems of the system. All safety module types are not required in a system either; only the modules needed by the application are necessary.

3.1.2 Burner Control

The Burner Control module provides flame safeguard controls for a variety of applications within the system. It can be configured as a control for primary or secondary burners that operate in an automatic or semi-automatic mode.

3.1.3 Flame Amplifiers

A Flame amplifier module is responsible for detecting the presence of flame at a designated location in the system. This information is provided to a specific Burner Control module that is controlling this part of the burner system, and therefore, the flame amplifier is considered a “child“

module of the Burner Control. Several flame amplifier types exist that are selected based on the type of application the system is intended for:

- Infrared (IR) sensor is used to detect flame
- Low voltage UV or visible light flame detector is used to detect flame
- Rectification with a flame rod is used to detect flame
- UV power tube is used to detect flame

Some of these types offer a flame signal amplification check (ampli-check) feature that is used to test the integrity of the circuit to detect a flame-out condition.

3.1.4 Limit Control

The Limit Control module provides the ability to use any type of analog signal to detect when pressure or temperature limits are exceeded in the system in order to safely shut down operation.

3.2 Safety Functions

3.2.1 Burner Control (and Flame Amplifiers)

Burner Control module is responsible to ensure that the events which make up a burner control operation cycle occur in the correct order and at the proper time. Failure to follow the configured sequence causes the Burner Control to put the system into a safety shutdown state, Lockout, where the safety relay and other safety critical outputs (ignition and gas valves) are turned off to abort burner startup or terminate a previously burning system. The system can be configured to either lockout and not permit further operation without human intervention, “Hard Lockout“, or to recycle and retry in case the unsafe condition is cleared, “Soft Lockout“. Residential markets often prefer soft lockouts while industrial/commercial markets prefer hard lockouts. The system designer selects which method is desired for their application. A single Lockout state exists that performs the safety shutdown due to a safety fault with other states indicating the sequence of the burner as it is turned on, turned off or is idling.

The Burner Control may also be configured to respond to limit faults reported by a Limit Control module and enter the same “Lockout“ safety shutdown state described above.

Flame amplifier modules continuously monitor for the presence of flame and report it’s findings to the Burner Control. Flame status not proper for the state of the burner sequence causes the Burner Control to enter the “Lockout“ safety shutdown state.

3.2.2 Limit Control

Limit Control module continuously monitors an analog input signal to detect when an unsafe limit has been exceeded. When such a condition occurs the Limit Control can be configured to turn off a safety relay circuit that is wired in series with the Burner Control’s interlock string (and therefore turn off safety critical outputs) or notify an associated Burner Control module of the limit violation and let it perform the safety response. The Limit Control module can also act as a stand-alone module that it alone turns off the safety relay circuit for a limit fault.

When the Burner Control notification approach is used the Burner Control must respond back to the Limit Control within 2 seconds to acknowledge the fault or the Limit Control takes matters into its own hands and turns off its safety relay to force a safety shutdown.

3.3 Safe State

The Burner Control and Limit Control modules place their part of the system into a safe state to protect it from a hazardous condition. The Burner Control performs this action by being connected to a safety relay circuit that shuts down the flow of fuel and air into the combustion chamber of the burner and remains in this shutdown condition until the problem causing the situation is corrected. This shutdown condition is called a “lockout“ in the burner control.

The Limit Control module uses the same principle as the Burner Control of being connected to a safety relay circuit that controls the interlock of the fuel and air flow into the burner. The circuit is closed when an unsafe limit is sensed in the system. The Limit Control remains in the “lockout“ state until an operator indicates that the hazardous condition is resolved.

3.4 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions of SLATE™ Burner Control System:

Model Number	System Component Name	Version	Safety Critical
R8001B2001	Burner Control Module	2	Yes
R8001L8001	Limit Control Module	2	Yes
R8001S1051	Power Tube Flame Amp with Dynamic Self-Check	2	Yes
R8001S1071	Power Tube Flame Amp with Dynamic Ampli-Check	2	Yes
R8001F1041	Low Voltage Infrared Flame Amp with Dynamic Ampli-Check	2	Yes
R8001F1091	Low Voltage UV/Optical Flame Amp with Dynamic Ampli-Check	2	Yes
R8001V1031	Rectification Flame Amp with Dynamic Ampli-Check	2	Yes
R8001A1001	Base Module	2	No
R8001S9001	Sub-Base Module	2	No
R8001D4001	Digital I/O Module	2	No
R8001N7001	Annunciator Module	2	No
R8001C6001	Fuel/Air Ratio Module	2	No
R8001U3001	Analog I/O Module	2	No
R8001K5001	LCD Display	1	No

Figure 2 - Module Versions

4 IEC 61508 Functional Safety Assessment Scheme

exida assesses the development process used by Honeywell Process Solutions for this development project against the objectives of the *exida* certification scheme. The results of the assessment are documented in [R1].
All objectives are considered in the Honeywell Process Solutions development processes for the development.

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

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

The detailed assessment evaluated the compliance of the processes, procedures and techniques, as implemented for the Honeywell Process Solutions SLATE™ Burner Control System, with IEC 61508.

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

The result of the assessment shows that the SLATE™ Burner Control System are capable for use in SIL 3 (Systematic Capability is SC3) applications, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

4.1 Product Modifications

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

As part of the *exida* scheme a surveillance audit is conducted prior to renewal of the certificate. The modification documentation listed below is submitted as part of a surveillance audit. *exida* will review the decisions made by Honeywell Process Solutions with respect to the modifications made. The following will be reviewed.

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

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Honeywell Process 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 SLATE™ Burner Control System 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 Process Solutions has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented [D01].

This functional safety assessment evaluated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the product development. The assessment was executed using the *exida* certification scheme which includes subsets of IEC 61508 requirements tailored to the SIL 3 work scope of the development team. The result of the assessment can be summarized by the following observations:

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

5.1.1 Functional Safety Management

Honeywell Process Solutions has documented their development and manufacturing processes in overall safety lifecycle procedures. They specify the required management and technical activities, as well as the responsibilities of the persons, departments and organizations, involved in each product and software safety lifecycle phase.

5.1.2 Safety Lifecycle and FSM Planning

A Functional Safety Management Plan [D026c], and other documents, are used to maintain information needed to tailor company procedures to the project and define functional safety related procedures not covered by company procedures. Activities are identified as phases, each of which is specified in terms of its input documentation, activities to be performed, work products to be produced/revised, work product verification activities (testing, analysis, review). In addition to requirements, design and implementation phases, overarching activities, including version control, configuration management and document control are identified and specified. References to procedures for notification of customers, field failure reporting and field returns are included.

5.1.3 Documentation

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

5.1.4 Training and competence recording

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

5.1.5 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.

5.1.6 Tools

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

5.2 Safety Requirement Specification

The safety requirements for each module are documented in a requirements database. Requirements on the safety functions, safety integrity properties, self-test, proof test, interface, designed safe states and environmental limits are specified.

5.3 Change and modification management

To ensure that safety integrity of the product is maintained after corrections and enhancements, procedures are defined that describe how change requests are initiated, analyzed, approved, planned, executed and tracked [D023]. All changes are first reviewed and analyzed for impact before approval. Impact analysis [D023b] is carried out to identify the extent to which the change is needed to be used safely. The change is also assessed to identify and document a plan for safe development of the requested change, including measures to verify and validate the change, following the normal design process.

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

5.4 Product Design

Product Architecture Design has been documented [D45], [D45b] and [D45c] and verified through review. The Architecture Design is partitioned into components and each component's design is documented, specifying interface and function, as well as how the design meets the product and safety requirements. The safety components have been shown to be independent of the non-safety components. The SIL capability of all safety components has been documented. Clear and unambiguous notation and language has been used to convey the design. It is clear how the architectural components are related to detailed design.

5.5 Hardware Design and Verification

The hardware design is captured in schematics, which are under revision control and configuration management. The design is verified through review and verification testing.

5.5.1 Hardware architecture design

Hardware architecture design [D045] [D045c] 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.

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

5.5.2 Hardware Design / Probabilistic properties

To evaluate the hardware design of the SLATE™ Burner Control System, a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) was performed by *exida* for each component in the system. This is documented in [R3]. The FMEDA was verified using Fault Injection Testing as part of the development, see [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 PFD_{AVG} of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL). The Safety Manual states that the application engineer should calculate the PFD_{AVG} for each defined safety instrumented function (SIF) to verify the design of that SIF.

5.6 Software Design and Verification

Software safety requirements are allocated to the software from product safety requirements and further derived into detailed requirements. The software architecture design [D049] [D049b] and detailed design is documented for each of the hardware modules containing software. The design documentation fulfils the relevant requirements for software safety with respect to the required safety integrity level, including specification and description of the components involved in the safety function execution and safety-related diagnostics. The design is partitioned into software modules, which are all developed to SIL 3 capability. The design identifies each module's SW/HW interfaces.

The software architecture design and detailed design for each of the modules is peer reviewed to verify its integrity. Identified defects and change requests are written up and tracked to completion in a change management database.

Module testing is planned and executed. The plans are reviewed and the test results are documented and controlled. Complexity metrics are periodically calculated and checked. Static analysis is used, in conjunction with reviews, to ensure that the code adheres to the rules documented in the Coding Standard [D060].

The software modules are integrated together and integrated with the target electronic hardware and tested to ensure it meets all software safety requirements and to ensure compatibility with its use of the hardware.

5.7 Safety Validation

Product validation planning results in a Safety Validation Plan, which contains test set up information and test cases. 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 procedures used to properly judge that the validation test is successful or not. Environmental tests are included in validation activities.

5.8 Safety Manual

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

6 Terms and Definitions

Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
High demand mode	Mode where the demand interval for operation made on a safety-related system is less than 100x the diagnostic detection/reaction interval, or where the safe state is part of normal operation.
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
SFF	Safe Failure Fraction - Summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
AI	Analog Input
AO	Analog Output
DI	Digital Input
DO	Digital Output
Type A element	“Non-Complex” element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the document

7.1 Liability

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

7.2 Version History

Contract Number	Report Number	Revision Notes
Q15/11-043	HON 15-11-043 R002 V1R0	Initial Certification, D. Butler, November 18, 2016.
Q17/10-158	HON 15-11-043 R002 V1R1	Surveillance audit, JCY, 22-Dec-2017

Review: V1R0, John Yozallinas, 11/8/2016
V1R1, Ted Stewart, 12/22/2017
Status: Released, 12/22/2017

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

John C. Yozallinas, CFSE, Sr. Safety Engineer

Ted E. Stewart, CFSP, Program Development & Compliance Manager