SLATE™
SIL Safety Manual

32325298-001
Revision 11

Revision History

Rev.	Date	Author	Description
1	August 23, 2016	R. Sorenson	Initial draft
2	August 26, 2016	R. Sorenson	Updated based on review comments
3	August 31, 2016	R. Sorenson	Added target demand mode.
4	October 21, 2016	R. Sorenson	Added more explanation for HFT level and SIL rating assigned to safety modules. Added further explanation of the safety verification procedure. Added overall diagnostic test interval. Added cyber-security risk analysis table for flame amplifier.
5	October 25, 2016	H. Stolz	Revised the Installer experience description in section 3.4 Installer Requirements.
6	October 26, 2016	R. Sorenson	Corrected description of CRC diagnostic test.
7	October 31, 2016	H. Stolz	Corrected HFT 1 to HFT 0 in section 2.4 and removed HFT 1 in Section 2.7
8	November 1, 2016	R. Sorenson	Updated systematic integrity and diagnostic test interval.
9	November 3, 2016	R. Sorenson	Clarified mode of operation, systematic integrity, and random integrity sections.
10	November 18, 2016	HW Stolz	Renamed Section 5.1 and revised figure 1.
11	January 3, 2017	R. Sorenson	Simplified random integrity to state FMEDA results and reference it for more details. Changed cyber-security section to reference the SLATE Security Manual for information.

Contents

List of Figures

1. Introduction

This document describes the information necessary to design, install, verify, and maintain SLATE™ safety modules in an application.

1.1 Terms and Abbreviations

The following terms or abbreviations are used in this document.

Term, Abbreviation	Definition
Base module	Single non-safety module in system that provides power to all other modules and contains the application programmable logic.
DIN rail	Metal rail used for mounting control equipment.
Hard Lockout	Lockout that always requires human intervention to clear the shutdown.
Lockout	Safety shutdown that requires human intervention before normal operation can be resumed.
Recycle	Return to an idle condition to be ready to start again. A delay may be required before operation can be continued.
Risks addressed state	State where all safety loads are turned off and the system is still able to operate when the fault is cleared.
Safety	Freedom from unacceptable risk of harm.
Safety key	Periodic data “key” signal sent between safety and monitor processors to indicate operational status and functional coverage of safety function.
Safety shutdown	Safety device that enters a risks addressed state.
Soft Lockout	Special form of lockout that normally requires human intervention to resolve the shutdown, but can also be cleared by itself after a (typically long) period of time or power re-cycle. Used when permitted by codes to ensure that a system does not remain offline needlessly after it’s safe to try again, especially when conditions have changed such that the next attempt might succeed.

Table 1 Terms and Abbreviations

1.2 Acronyms

The following acronyms are used in this document.

Acronym	Definition
FFRT	Flame Failure Response Time
HFT	Hardware Fault Tolerance
IR	Infrared light
SFF	Safety Failure Fraction – the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault.
SIL	Safety Integration Level, level that specifies the safety integrity requirements of the safety functions in the individual modules of the system.
SLATE™	Overall product name for the safety and non-safety modules addressed by this document.
UL	Underwriters Laboratories Inc.
UV	Ultraviolet light.
VFD	Variable Frequency Drive is a motor controller type that varies the frequency and voltage supplied to an electric motor.

Table 2 Acronyms

1.3 Product Support

Product support can be obtained from:

Automation and Control Solutions
Honeywell International Inc.
1985 Douglas Drive North
Golden Valley, MN 55422
https://customer.honeywell.com

1.4 Reporting Product Safety Issues to Honeywell

Any product failures that are detected and that compromise functional safety should be reported to Honeywell International. Please contact:

https://customer.honeywell.com

1.5 Reference Standards

The following standards have been referenced in the development of SLATE:

- ANSI/UL 1998, Software in Programmable Components, Third Edition
- IEC 61508: 2010 Functional safety of electrical/electronic/programmable electronic safety-related systems

1.6 SLATE Product Documentation

Additional information about the SLATE system may be found on the following website:

https://combustion.honeywell.com/user/login

2. Device Descriptions

Descriptions of the SLATE safety modules are contained in this section.

2.1 Product Components

2.1.1 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.

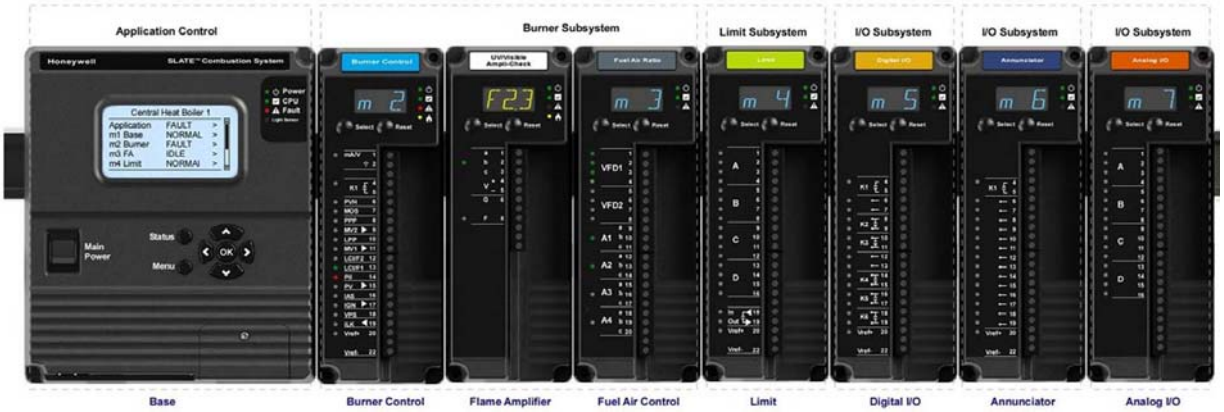

Figure 1 SLATE system with control boundaries

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.

2.1.2 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.

2.1.3 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 amplifiication check (ampli-check) feature that is used to test the integrity of the circuit to detect a flame-out condition.

2.1.4 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.

2.2 Safety Functions

2.2.1 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.

2.2.2 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 it's own hands and turns off it's safety relay to force a safety shutdown.

2.3 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.

2.4 Mode of Operation

SLATE safety modules are Type B devices. Their targeted demand mode of operation can vary from low to high, and even possibly continuous, depending on the application that the module is used in. The modules are used in residential, commercial, and industrial burning environments which may call for any one of those modes of operation. The safety modules are designed to act in any of these modes to respond to any potential hazard.

2.5 Systematic Integrity

All SLATE safety modules have been developed using development and manufacturing processes that require techniques and measures designed to avoid and/or control systematic faults and comply with the requirements for Systematic Capability Level 3 (SC 3).

A system designed with these modules must not be used at a SIL level higher than listed without justification by the end user.

2.6 Failure Rates

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from Honeywell International Inc. This report details all failure rates and modes for the safety modules. A summary of the FMEDA analysis is provided in the following table.

Safety Module	SFF
Burner Control with flame amplifier	99%
Limit Control without application I/O	99%
Limit Control with application I/O	80%

Table 1 FMEDA Summary

2.7 Random Integrity

The SLATE modules are type B devices that are suitable for use up to SIL 3 with HFT = 0. More information regarding this evaluation can be obtained from the the FMEDA report available at Honeywell International Inc.

2.8 Demand Response Time

The Burner Control module responds to a fault detected by it or the flame amplifiers within the flame failure response time (FFRT) which is configurable to one of the following:

- 0.8 second
- 1 second
- 2 seconds
- 3 seconds

The Burner Control may also be informed of a fault from either a Fuel Air Control or Limit Control module.

For any of these fault conditions the Burner Control enters a safety shutdown state by shutting down the burner system and declaring a lockout state.

The Limit Control module responds to a limit fault within 2.5 seconds. The Limit Control must be configured to initiate a safety shutdown itself or to notify a Burner Control to do the safety shutdown. If configured to notify the Burner Control to act on the fault, the Burner Control must acknowledge the fault within 5 seconds afterwards or else the Limit Control initiates a safety shutdown using it's safety relay circuit.

2.9 Capacity/Scalability

Maximum number of total modules (safety and non-safety) in the system is limited to a total power consumption of 40 watts. A physical limit of 20 modules including the Base module is also constrained by the system. The mix of safety modules to non-safety modules is not restricted and is application dependent.

2.10 Non-SIL Functions

The Limit Control module offers some non-SIL functions for the system:

- NTC temperature input
- Pot input
- RTD input
- Thermocouple input
- Voltage input
- Current input
- Voltage output
- Current output
- PWM output

2.11 Security

Commissioning and setting safety parameters in the safety modules requires an authorized user to login to the system before they can be performed. The login password is customizable by the system designer of the application.

3. Designing a SLATE Safety Application

3.1 Environmental Limits

All SLATE safety modules are rated to operate in an ambient temperature range of -20˚F to 150˚F (-29˚C to +66˚C). Supported humidity is up to 95% continuous, noncondensing at 104˚F for 14 days. Shipping temperature range is -40˚F to 150˚F (-40˚C to +66˚C).

3.2 Application Limits

All safety modules must be mounted in an electrical enclosure with adequate clearance for servicing, installation, and removal of modules as specified in their respective Installation Instructions (I & I) manual. Wiring must comply with all applicable codes, ordinances, and regulations with NEC Class 1 (Line Voltage) wiring. Cable shielding must be terminated to ground at both ends.

3.3 Connection to Equipment

3.3.1 Burner Control

Burner Control module may be connected to valves, ignition system, and optionally, a blower to control the operation of the burner. These devices are connected to relays in the module to turn them on at the correct times in the burner sequence. Signals indicating the burner condition are input to the Burner Control via input terminals.

Burner Control interfaces with flame amplifier modules using a dedicated communication bus between them. Control and status information is passed between them using a safety packet mechanism to ensure reliable and trusted communication.

3.3.2 Flame Amplifier

The Flame amplifier module is connected to it's Burner Control module with a dedicated communication bus to receive control information and send status information. A safety packet mechanism is used to transfer the safety data in this communication.

3.3.3 Limit Control

Limit Control module is connected to different monitor points in the system. Sensors (individual or redundant pairs) are connected to input terminals on the module that are monitored for pressure or temperature levels at various positions in the system. A safety relay in the module must be connected to the system load string to shutdown the burner system when a limit fault occurs or a Burner Control module must be informed of the fault and let it handle the shutdown. In the latter case a continuous safety packet mechanism communication occurs between the Limit Control and the Burner Control using the system platform bus.

3.4 Installer Requirements

Installation and commissioning of the safety modules requires the user to be a trained, experienced flame safeguard service technician, knowledgeable of the application environment that the modules are installed in. This expert must be familiar with and have received proper training of the SLATE product line. Proper wiring methods described in the product I & I manual must be used by the installer.

3.5 Cyber-Security Requirements

Only authorized users are allowed access to SLATE safety modules for configuration and software maintenance purposes. Mechanisms are in place to ensure that only verified modules that have not been tampered with will permit their operation to occur. More details regarding the security measures used can be obtained from the SLATE Security Manual available from Honeywell International Inc.

4. Installation and Commissioning

4.1 Installation

All safety modules are installed and wired as specified in their respective Installation Instructions (I & I) manual. Environmental conditions must be satisfactory for the limits specified in the I & I.

Configuration of the safety parameters in the modules are only allowed by authorized users. Users are required to login with the correct password at both the browser and local display interfaces in order to change the parameters.

4.2 Physical Location and Placement

Each safety module is inserted into a subbase and mounted on the DIN rail along with the Base module. Flame amplifier modules may alternatively be mounted locally on the DIN rail or mounted remotely off the DIN rail and nearer the flame itself if desired.

The modules can be physically located in any order on the DIN rail with the following exceptions (see the following figure):

- All modules, safety and non-safety, must be positioned to the right of the Base module when they are on the DIN rail. Remote flame amplifiers may be positioned anywhere.
- Flame amplifier modules must be positioned immediately to the right of their controlling Burner Control module. Remote flame amplifier modules are wired directly into the Burner Control module through a connection into the Burner Control's subbase. Location of another non-flame amplifier type module on the DIN rail denotes the end of the flame amplifiers controlled by the Burner Control.

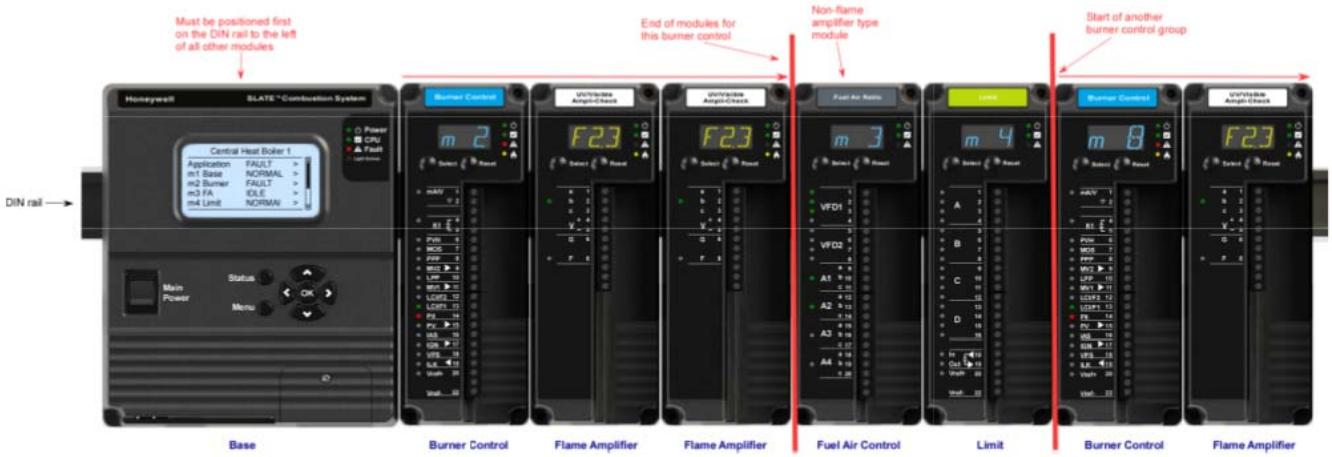

Figure 2 Module positions on DIN rail

If some modules need to be separated from each other, the DIN rail can be extended onto another section of DIN rail and the two segments connected to each other via the subbases.

4.3 Connections

Subbases of modules are connected together using side connectors and locking tabs to fix them onto the DIN rail. Modules are inserted and screwed into each subbase to access power and control.

4.4 On-site Configuration

Safety modules can be configured on-site or off-site. In both cases a designer application kit is installed into the Base module and distributed to all modules, non-safety as well as safety. The designer kit sets the configuration parameters to initial values that may or may not need further changing. Once the configuration settings are final, all safety configuration parameters in each safety module must be verified and approved by the safety expert. The safety module remains locked out until all the safety configuration parameters are verified by the safety expert. The installer must login with the correct password before safety verification is possible. Expert is warned with a safety notice indicating that only safety knowledgeable personnel should perform safety verification.

If a safety parameter setting needs to be changed later, i.e., after kit installation, the change is only allowed by a safety expert that logs in with the correct security password. The safety parameter may be changed when the system is operational or idling, but in either case, the safety module shuts down immediately and enters the Lockout state. It is up to the judgement of the safety expert to when the safety parameter is changed. The expert may deem it easier to change the parameter setting than to perform the steps necessary to turn down the burner application in another method. Safety verification is required by the safety expert before the lockout can be cleared allowing the module to operate again.

Safety verification involves each safety module presenting the safety parameter that has changed and it's new setting. The safety parameter and it's setting is driven by the safety module itself with the user interface simply presenting the data to the safety expert. An explanation of the purpose for the safety parameter is provided and the safety expert approves

or disapproves of the new setting. The safety module ensures in the verification procedure that the new value is the one being approved. Once all safety settings have been approved and the lockouts cleared in the safety modules the system is ready for operation. If one or more safety parameters are not approved, the module remains locked out until the matter is resolved (reset the parameter to the original or a new value). It is up to the safety expert's judgement whether a test run should be performed after the verification procedure is complete since the safety parameter change may or may not be possible to introduce a failure trigger that the setting change will show it's effect.

The settings are saved to non-volatile storage in each module so that they can be recalled when a module is reset. An audit record is made showing when the safety parameter is changed and what the new value has been set to. The application designer has a further capability to save the verified safety parameter settings back into a pre-verified kit that can be re-installed and not require re-verification.

5. Operations and Maintenance

No manual off-line proof testing is required in the useful life of the safety modules.

5.1 Automatic Diagnostic Testing

All safety modules perform the following automatic diagnostic tests (test intervals specified):

- CRC check of non-volatile memory where application and safety code are stored is performed continuously and completes within 3 seconds.
- RAM safety data validation - safety data in RAM is checked for possible corruption and configuration parameter settings are verified with their values stored in non-volatile memory every time the safety data is accessed.
- Checkerboard RAM test is performed continuously in background when not executing anything else by checking 48 bytes at a time during each main loop pass. It finishes a complete RAM test pass within 1.5 seconds.
- Stack depth is monitored for overflow condition during every pass of the main loop.
- Periodic instruction test is conducted once every second.

All of the above tests are performed during each main loop pass in background when the primary application code is finished. The periodic instruction test is executed once every second and completes within milliseconds. The checkboard RAM test executes continuously, but takes approximately 3 seconds to complete. Since all other tests finish in much less than a second and are executed continuously, the overall diagnostic test interval needed to complete all automatic tests is 3 seconds.

5.1.1 Burner Control and Flame Amplifier

The Burner Control module performs the following additional diagnostic tests:

- System clock is checked continuously for drift to ensure that timing is accurate within ±10%.

- Periodic testing of the safety key recognizer to detect key bit errors (validate that all bits of safety key can be set).
- During the Pre-ignition state, which is part of every burner sequence, the safety processor tests the monitor processor's end-to-end ability to respond by verifying that it will drop the safety relay drive in case an unsafe condition occurs.
- Safety relay drop out timing during the Pre-ignition state – Ensures that the safety relay is not welded and drops out within 250ms.
- Stuck load control relay (not closing/opening as commanded) detection when starting a burner sequence.

5.1.2 Limit Control

The Limit Control module performs the following additional diagnostic tests:

- System clock is checked continuously for drift to ensure that timing is accurate within ±10%.
- Periodic testing of the safety key recognizer to detect key bit errors (validate that all bits of safety key can be set).
- Whenever the safety relay is about to be turned on, the safety processor tests the monitor processor's end-to-end ability to respond by verifying that it will drop the safety relay drive in case an unsafe condition occurs.
- Safety relay drop out timing during module start up – Ensures that the safety relay is not welded and drops out within 250ms.

5.2 Repair and Replacement

Safety modules can be replaced to resolve malfunctioning units or to add new features. The system should be powered off for safe replacement, and the old module removed from the subbase followed by re-inserting the new module into the subbase.

The replaced module can be reconfigured from the Base module with the original application kit or any newer configuration sets. The safety configuration parameter settings in the replaced safety module must be re-verified unless a pre-verified application kit is re-installed.

Module software can be upgraded using a service pack when needed. The service pack is encrypted by Honeywell to ensure trusted content and to deliver the new software to the installation site. Proper login authorization is required to install the service pack and to also do the software upgrade (two step procedure). After the software upgrade re-verification of safety parameters may be necessary. A record of the service pack installation is recorded in the Base module for audit purposes.

5.3 Useful Life

Expected lifetime of the safety modules are approximately 20 years.

5.4 Manufacturer Notification

Any failures that are detected which compromise functional safety or software malfunction are to be reported to:

Honeywell International Inc.
Automation and Control Solutions
1985 Douglas Drive North
Golden Valley, MN 55422
customer.honeywell.com

Recommended changes or improvements to the software can be addressed to the above location also by filling out the feedback comment card.