Failure Modes and Effects Analysis (FMEA) Form

Approval Signatures:

Author:

Department	Name	Signature	Date
IS	Andrew Mason		5/21/12

Approval:

Engineering	Don Pegg		5/21/2012
Engineering	Brian Tompson		5/21/2012
QA	Andrea Miller		5/21/12

Product/Project Name: EPIC ClearView Firmware
Project Manager: Andy Mason
Date: 5/15/12

Risk Analysis Documentation Form: The firmware is a piece of software installed within the ClearView device. The user does not interface directly with the ClearView firmware. The ClearView software (which does directly interface with the user) sends commands to the ClearView firmware. As such, a Risk Analysis Documentation Form was not completed for the ClearView firmware. Additionally, the Part Name and Part Number and Process/Product Function columns were removed from the FMEA table since the firmware represents one particular part and process.

Failure Modes and Effects Analysis (FMEA) Form

ID	Potential Failure Modes	Potential Effects of Failure	Severity	Potential Causes of Failure	Occurrence	Current Controls	Detection	RPN	Comments
1	Control logic failure	Unexpected operation	3	Invalid pointers, stack corruption	1	The microcontroller's internal watchdog timer hardware is used to force the microcontroller to reset if the control logic fails to periodically service the watchdog	1	3	
2	Invalid or incomplete command received from host	Host command not executed	1	a. Invalid command sent by host b. Bad communication connections	1	Command timeout discards commands if more than 0.5 seconds elapse before the command is complete. Only known and properly formatted commands are processed	1	1	
3	Loss of positive control of Boost voltage	Undesired Boost voltage levels during exposure	6	Device hardware fails to control or sense Boost voltage	1	Upon power up the firmware verifies the Boost voltage is low. If this check fails the firmware enters a fatal state preventing normal operation. Additionally during operation if the Boost voltage is above or below the maximum or minimum limits the fatal state is entered.	1	6	
4	Processing of new host command interferes with exposure already in progress	An exposure with unknown parameters	5	Host issuing commands during an exposure	3	All host commands with the exception of the command to abort an exposure are rejected while an exposure is in progress	1	15	

ID	Potential Failure Modes	Potential Effects of Failure	Severity	Potential Causes of Failure	Occurrence	Current Controls	Detection	RPN	Comments
5	Host attempt to set illegal exposure parameters for; duration, frequency, or Boost voltage	An exposure with unknown parameters	6	Host attempting to set illegal exposure parameters	1	All host command parameters are checked for format and valid values or ranges	1	6	
6	Firmware exposure duration exceeds set value	An exposure with unknown duration	3	Firmware activity causes delay in terminating exposure	1	The microcontroller's internal timer hardware is used to produce a reliable 5ms clock to time the exposure duration	5	15	
7	Unexpected Boost voltages	An exposure with unknown Boost voltage	6	Incorrect timing of the period or duty cycle of the PWM0 signal that controls the Boost voltage	1	The microcontroller's internal PWM timer is used to produce PWM signal with reliable period and duty cycle. The PWM0 pin is gated to prevent a prolonged duty cycle when terminating the exposure.	1	6	
8	Host loss of firmware status information	Host settings may have different values than firmware	5	Operation in an unknown state	1	The firmware provides an information command to allow the host to see the current firmware state	3	15	
9	Exposure duration set incorrectly	An exposure of unintended duration	5	Operator error	1	The firmware provides an abort command to allow the host to abort an exposure in progress	5	25	

Failure Modes and Effects Analysis (FMEA) Form

ID	Potential Failure Modes	Potential Effects of Failure	Severity	Potential Causes of Failure	Occurrence	Current Controls	Detection	RPN	Comments
10	SPI communication failure with the devices onboard Boost control potentiometer or Boost voltage sensor	An exposure with unknown Boost voltage	6	Hardware failure	1	If an unexpected SPI failure occurs the firmware forces the device to reset. After reset the device is placed in a safe mode.	3	18	

No Required Mitigation

There were no Severity ratings above a “6” and/or RPN calculations above a “216”. Therefore, further mitigation is not required.

Document Revision History

Version Number:	Description of Change:	Date:	Updated by:
000	New Document	5/21/12	A. Mason