A10 - Reliability and Safety Analysis

Year: 2025 Semester: Spring Team: 20 Project: Encrypted USB Drive

Creation Date: ­April 5, 2025 Last Modified: April 30, 2025

Author: Brandon Liu Email: liu3394@purdue.edu

1. Reliability Analysis

* The components of interest are the STM32H7 Microcontroller [1], the USB ESD protection, and the TVS ESD protection diodes. The microcontroller was chosen due to its complexity and high volume of pins; the USB ESD protection diode [2] was chosen due to the fact that USB is a key functionality of the project and if it is damaged via excessive voltage spikes, the device may not work;the TVS ESD protection diode was chosen due to for a similar reason as the USB ESD protection, except this is for other components of the product including but not limited to the keypad and fingerprint sensor.
* The following equations are used for the reliability analysis with the first one for the failure rate for the microcontroller [4], the second equation for the mean time to failure, and the third equation for the failure rate of the diodes [4] being analyzed:
  + Lambda\_p\_MCU = (C1 \* temp coeff + C2 \* env const) \* learning factor \* quality factor
  + MTTF = 10^6 / (24 \* 365 \* lambda\_p) years
  + Lambda\_p\_diode = lambda\_b \* temp coeff \* e stress \* env const \* contact construct factor \* quality factor
* Microcontroller:

Table 1 STM32H7A3RGT6

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments regarding choice of parameter value, especially if you had to make assumptions.* |
| C1 | Die complexity | *0.56* | *32-bit bus* |
| πT | Temperature coeff. | *0.98* | 85 deg C max |
| C2 | Pin/Package Constant | *0.025* | MCU is to be soldered so assuming that hermetic column of 5.9 table to be used |
| πe | Environmental Constant | *0.5* | G\_B |
| πl | Learning Factor | *1.0* | Device produced for over 2 years (based on manuals and technical notes released in 2019) |
| πq | Quality Factor | *10* | Device uses commercial components |
| Entire design: |  |  |  |
| Lambda\_p | | *5.61* | |
| MTTF | | *20.3 years* | |

* USB ESD Protection:

Table 2 USBLC6-2SC6

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments regarding choice of parameter value, especially if you had to make assumptions.* |
| Lambda\_b | Base failure rate | *0.0013* | Transient suppressor |
| πT | Temperature coeff. | *21* | 150 deg C max |
| πS | Electrical stress factor | *1.0* | Transient suppressor |
| πe | Environmental Constant | *1.0* | G\_b |
| πC | Contact construction factor | *1.0* | Metallurgically bonded (soldering) |
| πq | Quality Factor | *5.5* | Lower (chosen because device not necessarily for military but no indication of plastic in data sheet) |
| Entire design: |  |  |  |
| Lambda\_p | | *0.15015* | |
| MTTF | | *760 years* | |

* TVS ESD Protection:

Table 3 D5V0L2B3SO-7

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter name | Description | Value | *Comments regarding choice of parameter value, especially if you had to make assumptions.* |
| Lambda\_b | Base failure rate | *0.0013* | Transient suppressor |
| πT | Temperature coeff. | *21* | 150 deg C max |
| πS | Electrical stress factor | *1.0* | MCU is to be soldered so assuming that hermetic column of 5.9 table to be used |
| πe | Environmental Constant | *1.0* | G\_b |
| πC | Contact construction factor | *1.0* | Metallurgically bonded (soldering) |
| πq | Quality Factor | *8.0* | Plastic |
| Entire design: |  |  |  |
| Lambda\_p | | *0.2184* | |
| MTTF | | *522 years* | |

* Summary:
  + The MTTF for all components is extremely high, meaning that the device will last well within its reasonable usage which is just to temporarily store files. One solution for even greater longevity is to use these devices at normal room temperatures, and not extreme ones that are too hot or too cold. This allows for the device’s minimum and maximum temperature to not be stressed as much.

1. Failure Mode, Effects, and Criticality Analysis (FMECA)

* The two failure modes in consideration are medium and low. Medium refers to damage to the device such that components no longer work at all, and low refers to errors that result in illogical operation despite the component still being functional. There is no high category as there is not a voltage in the device that should lead to human injury. The acceptable failure rate (arbitrary value) is 10^-9 for both medium and low failure modes. It is under the assumption that the user will read the manual in its entirety before using the device, and the device will not be used in extreme climates (including but not limited to scorched heat or freezing temperatures) or weather conditions (including but not limited to rain or snow).

3.0 Sources Cited:

[1] STM32H7A3RGT6 stmicroelectronics | mouser, https://www.mouser.com/ProductDetail/STMicroelectronics/STM32H7A3RGT6?qs=sPbYRqrBIVk%2BdecRlyVesQ%3D%3D (accessed Apr. 7, 2025).

[2] ST, USBLC6-2 Datasheet, https://www.st.com/content/ccc/resource/technical/document/datasheet/06/1d/48/9c/6c/20/4a/b2/CD00050750.pdf/files/CD00050750.pdf/jcr:content/translations/en.CD00050750.pdf (accessed Apr. 7, 2025).

[3] Diodes Incorporated, D5V0L2B3SO, https://www.diodes.com/assets/Datasheets/D5V0L2B3SO.pdf (accessed Apr. 7, 2025).

[4] Military Handbook, https://snebulos.mit.edu/projects/reference/MIL-STD/MIL-HDBK-217F-Notice2.pdf (accessed Apr. 6, 2025).

Appendix A: Schematic Functional Blocks

A diagram of a computer

AI-generated content may be incorrect.

Figure 1, microcontroller circuitry

A diagram of a circuit

AI-generated content may be incorrect.

Figure 2, reset circuitry

A diagram of a circuit board

AI-generated content may be incorrect.

Figure 3, debugging circuitry

A computer screen shot of a computer

AI-generated content may be incorrect.

Figure 4, programming circuitry

A diagram of a computer

AI-generated content may be incorrect.

Figure 5, oscillator circuitry

A diagram of a computer

AI-generated content may be incorrect.

Figure 6, Fingerprint circuitry

A computer circuit diagram with many wires

AI-generated content may be incorrect.

Figure 7, keypad circuitry

A diagram of a computer

AI-generated content may be incorrect.

Figure 8, flash IC circuitry

A diagram of a circuit

AI-generated content may be incorrect.

Figure 9, LCD circuitry

Appendix B: FMECA Worksheet

Table 4, Microcontroller circuitry

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | No signal coming out of a certain pin | Programmed wrong pin / damaged pin | Unpredictable | Slave devices do not respond or state machine is not followed | Medium | Assuming microcontroller is powered via USB connected to a computer |
| 2 | Extreme signal noise | Improperly soldered decoupling capacitor | Unpredictable | Slave devices do not respond and oscilloscope reads noisy signals coming from master | Medium | Assuming code and wiring is all correct |

Table 5, Reset Circuitry

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | Reset signal stays high | Damaged push button or poor soldering onto PCB | System cannot reset | Observation, pressing push button does not affect current function of device | Low | Assuming code is all correct |
| 2 | Reset signal stays low | A short through C3 | System is stuck in reset (looped) | Observation | Medium | Assuming push button is operational and wiring is soldered properly |

Table 6, Programming Circuitry

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | No data received via programming header | Damaged header / connection issues with the programmer on the STM32F4 dev board | Cannot program microcontroller | Observation (MCU functionality does not change) | Medium | Assuming programmer on dev board is powered |

Table 7, Oscillator circuitry

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | No signal coming into the oscillator pins of microcontroller | Connected to wrong pins / damaged crystal | Unable to reach oscillator speed and therefore will have to rely on in built clock | Observation | Low |  |

Table 8, Fingerprint circuitry

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | No response from fingerprint sensor | Improperly configured UART | Unable to communicate with slave | Reading communication bus via oscilloscope | Low |  |
| 2 | Fingerprint sensor does not scan | Damaged component | Unable to communicate with device | Oscilloscope reading correct but slave not operational | Medium | UART properly configured |

Table 9, Keypad circuitry

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | Pressing of a key not registered | Improper programming / damaged matrix circuitry | Certain key is unresponsive | Observation | Medium |  |

Table 10, Flash IC circuitry

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | Unable to read or manipulate data in flash IC | Damaged component | Unable to interact with data stored in flash IC | Oscilloscope reading / STM32CubeIDE debugger | Medium | Assuming SPI communication bus is configured properly |

Table 11, LCD circuitry

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Failure No.** | **Failure Mode** | **Possible Causes** | **Failure Effects** | **Method of Detection** | **Criticality** | **Remarks** |
| 1 | Back light not powered on | Not connected to power / damaged component | Unpredictable | Observation | Medium | Assuming SPI communication bus is configured properly |
| 2 | Logic failure in LCD display | Sending improper commands or illegal characters | LCD displays unexpected characters | Observation | Low | Assuming SPI communication bus is configured properly |