CLAIMS

1. A system for providing a secure boot image loading, comprising:

a microcontroller;

a plurality of physically modifiable internal components (PMIC) disposed on the microcontroller, wherein each of the plurality of PMICs can only be modified one time;

an image loader configured to load a boot image from memory of the microcontroller;

a checksum calculator configured to calculate a checksum value for the boot image; and

a checksum burner configured to modify the plurality of PMICs to create a binary representation of the checksum value for the boot image.; and

2. The system of claim 1 wherein the image loader is configured to call the checksum calculator to calculate a second checksum value for the boot image each time the boot image is loaded, and to compare the second checksum value with the checksum value in the plurality of PMICs to determine if the second checksum value and the checksum value are the same.

3. 2. The system of claim 21 wherein the second checksum value and the checksum value are the same, wherein the image loader is configured to continue to allow the boot image to load.

4. 3. The system of claim 21 wherein the second checksum value and the first checksum value are not the same, wherein the image loader is configured to execute a mismatch response.

4.

5. The system of claim 43 wherein the mismatch response is burned into the plurality of PMICs.

5.

6. The system of claim 54 wherein the mismatch response prevents further loading of the boot image.

6.

7. The system of either of claims 5 or 6,claim 4 wherein the mismatch response alerts a user of the mismatch.

8.

7. The system of claim 76 wherein the mismatch response further prevents loading of the boot image until a response is received from the user.

~~9. The system of any of claims 5 to~~ 8~~.~~. The system of claim 4 wherein the mismatch response that is burned into the plurality of PMICs is a partial response.

9. ~~10.~~ The system of claim ~~9~~8 wherein the partial response is a pointer to an address where a complete mismatch response is stored.

10. ~~11. A method for securing a boot image load, the~~A method comprising:

calculating a checksum value for a boot image;

writing the checksum value to a microcontroller;

burning in the checksum value into the microcontroller; and

burning in responses to a checksum mismatch into the microcontroller.

11. ~~12.~~ The method of claim ~~11~~10 wherein the checksum value is burned into a plurality of physically modifiable internal components (PMIC) disposed on the microcontroller, wherein each of the plurality of PMICs can only be modified one time.

12. ~~13. The method of either of claims 11 or 12,~~ The method of claim 11 wherein the checksum value is burned into the plurality of PMICs as a binary representation of the checksum value.

13. The method of claim 10 wherein the response to a checksum mismatch are burned into a plurality of physically modifiable internal components (PMIC) disposed on the microcontroller, wherein each of the plurality of PMICs can only be modified one time.

~~14. The method of any of claims 11 to 13, wherein the checksum value is burned into the plurality of PMICs as a binary representation of the checksum value.~~

~~15.~~ A method of ~~any of claims 11 to 14, the method further~~securing a boot image load, comprising:

loading the boot image from a microcontroller;

calculating a checksum value for the boot image;

comparing the checksum value with a stored checksum value, wherein the stored checksum value is permanently burned into the microcontroller;

allowing the boot image to continue loading in response to a match when comparing the checksum value with the stored checksum value; and

executing a mismatch response in response to a mismatch when comparing the checksum value with the stored checksum value~~.~~, wherein the mismatch response is permanently burned into the microcontroller.

15. ~~16.~~ The method of claim ~~15 wherein the mismatch response is permanently burned into the microcontroller.~~

~~17. The method of claim 16~~14 wherein the mismatch response stops further loading of the boot image.

~~18.~~ 16. The method of claim ~~16~~14 wherein the mismatch response alerts a use of the mismatch.

~~19.~~ 17. The method of claim ~~18~~16 wherein the mismatch response further stops further loading of the boot image until a response is received from the user.

~~20.~~ 18. The method of ~~any of claims 16 to 19~~claim 14 wherein the mismatch response is a partial response as a pointer to an address where a complete mismatch response is stored.

~~21. A computer program product for securing a boot image load, the computer program product comprising:~~

~~a computer readable storage medium readable by a processing circuit and storing instructions for execution by the processing circuit for performing a method according to any of claims 11 to 20.~~

~~22. A computer program stored on a computer readable medium and loadable into the internal memory of a digital computer, comprising software code portions, when said program is run on a computer, for performing the method of any of claims 11 to 20.~~