FIPS 140-2 Tamper Detection to protect Fuze Technology

Douglas Cox,Trong Huynh,
John Ambrose

Presented at the 55th Annual Fuze Conference in Salt Lake City, Utah on May 25, 2011

by Douglas Cox
info@mix-sig.com

Mixed Signal Integration
2157F O'Toole Avenue
San Jose, CA 95131
+1 408-434-6305
www.mix-sig.com

This presentation is about the use of the standard product MSFIPS in detecting tampering of fuze technology.

Mixed Signal Integration is a Silicon Valley chip maker specializing in mixed signal CMOS based ASICS. Incorporated in 1997, Mixed Signal Integration specializes in analog and mixed-signal integrated circuits. MSI offers both standard products and custom ASICs in CMOS technologies. Consumer audio and video, wireless personal communications, automatic test equipment and medical are some of the markets where MSI enjoys excellent customer relationships.

What is F.I.P.S.

- Federal Information Processing Standard
  - 5 Levels of Protection
  - Level 1 is Cryptography
  - Level 2 is Physical protection
  - Level 3 is Voltage and Reset protection
  - Level 4 is Temperature monitoring +Level 3
  - Level 5 is Current monitoring protection +Level 4

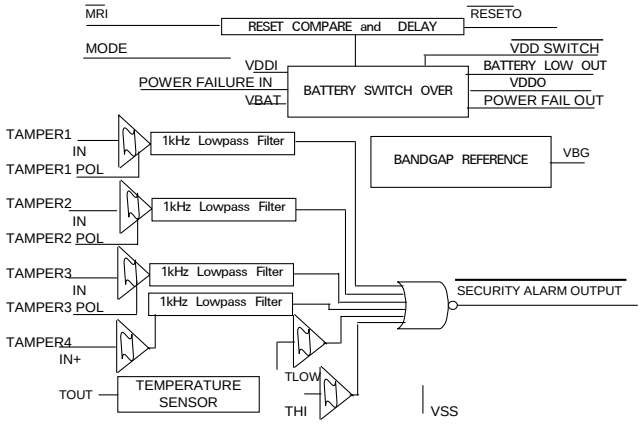
FIPS stands for Federal Information Processing Standard. The FIPS 140-2 is the latest approved cryptography standard. There are 4 approved levels and one new level in discussion. Level one is the encrypting of data. This is generally done with a microprocessor. Level 2 is the physical protection of the unit to prevent unauthorized access. Level 2 is done with tamper switches and potting material. Level 3 is voltage and reset hack detection and protection. Hackers had found that by reducing or increasing voltage on a system, the memory clear can sometimes by bypassed in code. Level 4 adds temperature monitoring to detect a freeze spray hack. Level 5 is the modification of firmware to prevent a current probe on a deep memory oscilloscope monitoring the power supply detecting the actual executed code and decoding. Oddly the modification to the firmware will produce “spaghetti code”, but, it prevents the hack. The MSFIPS provides levels 3 and 4.

The Problem

- Fuze Technology needs protection
  - Sophisticated Analog and Digital Signal Processing techniques
  - Danger of reverse engineering
  - No battery drain
  - Tampering with Fuze ignition sequence
  - Tampering with Safe and Arm

Fuzes are stored before use, and this storage is armed storage to prevent tampering. As proximity fuzes use more complex and proprietary techniques, there needs to be a way to detect tampering and react accordingly. In the case of reverse engineering, the fuze electronics must be rendered unusable. For the Safe and Arm and fuze ignition sequence, there must be a way to detect attempts to modify and thwart the efforts.

MSI's MSFIPS provides Monitoring Functions



The MSFIPS provides the following monitoring functions: Tamper switch inputs with polarity selection (NC or NO) and noise filtering. Bandgap reference to detect over or under voltage hacking attacks. Reset compare and delay to prevent glitching attack. Battery switchover in case of main power being cut and a temperature sensor to protect against freezing memory attacks. The SAO* (Security Alarm Output) will be driven low when any trigger event occurs (tamper, voltage, or temperature). The SAO* output can then be applied to a microcontroller for deciding what to do (clear memory, sound alarm or self destruct).

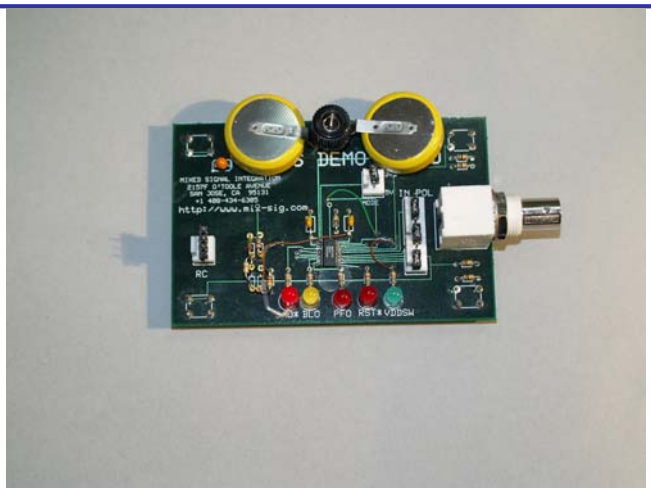
System Design

Life of Lithium Battery with no drain is ~10 years.

- To increase life, switches for access power the MSFIPS.
- Once case is opened, MSFIPS would monitor status.

Fuzes must be able to be stored for the length of the battery life. In the case of Lithium batteries, this is 10 years. Any current load would shorten this time. To avoid this problem, MSI proposes to use magnetic switches to connect the MSFIPS when access to the electronics is attempted. The MSFIPS, once powered, would monitor status of voltage, temperature, attempts to glitch the microcontroller and access other areas of the fuze.

MSFIPS Evaluation Board



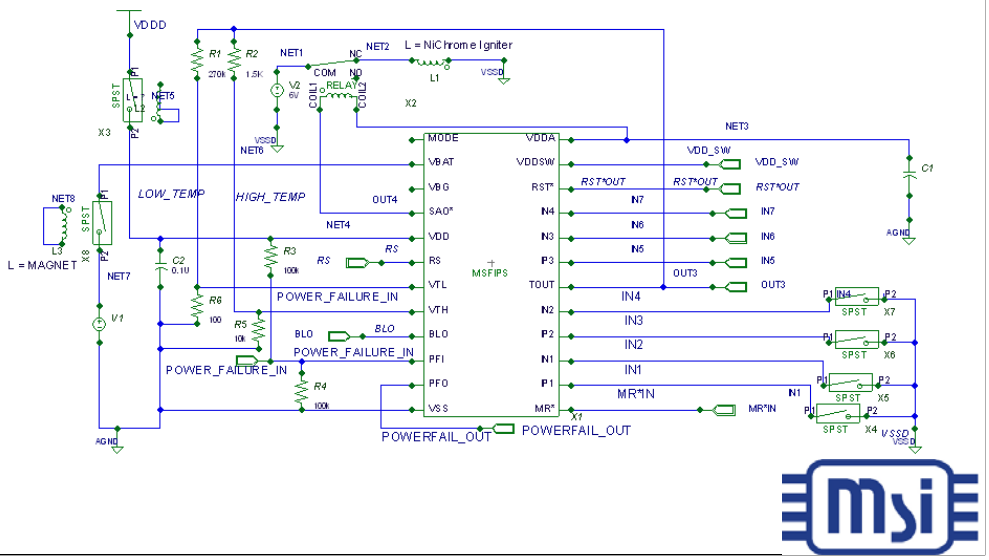
This photograph is of the MSFIPS evaluation board. The board provides input polarity switching control, temperature detection control, high and low voltage sense, low voltage sense battery switchover. Reset can be applied and de-glitched. The large 1000mA button cells were used for the igniter. The MSFIPS draws less than 1 mA at 5V.

What if Triggered?

- SAO* goes low closing relay to igniter.
- 50 gauge NiChrome© wire requires only 500 mA current.
- Able to burn and damage components to prevent reverse engineering.

The SAO* output is active low and can be connected to a 3 V relay to control the 6 V battery needed to ignite the 50 gauge match head as used in model rocketry. Two CR-2477 coin cell batteries as shown in the first picture, wired in series provide up to 1 A at 6 V. With only ~500 mA needed, the ignition is quick. The match head should ignite a small flammable material to damage the integrated circuits in the fuze. Another approach would be to have a greater voltage applied to the pins of the proprietary devices to damage them internally.

Simplified Schematic



The simplified schematic shows the connections of the MSFIPS with batteries and the relay for the igniter. Most applications, the SAO* output is not tied to a relay, but, is tied to a microcontroller to wipe memory.

Technical Issues

- Position of the tamper switches
  - Ensure they cannot be bypassed
- Selection of temperature range
  - Need to be set for range found in outdoors
- Ensuring destruction of fuze technology is complete.

What is a concern in the system design is the location of the tamper switches to prevent bypass. Magnetic switches, such as used with home alarm systems are bypassed with a simple magnet. By hiding where the switches are located, this attack can be avoided. For microswitches, small wires can be fed in and used to hold the switch open or closed. Sealing around the access panel should prevent this attack.

The temperature range needs to be set to detect a freeze spray attack on memory. But, in use, the temperature may be quite cold or hot. With the external resistors on the MSFIPS evaluation board, the temperature detection points can be carefully set.

The complete destruction of the fuze technology without causing injury of the attacker will need to be carefully adjusted. The overvoltage solution may work out to be a better way to destroy the technology.

Summary

MSFIPS provides monitor and protection to Fuzing technology

- Monitors tampering.
- Monitors typical hacking techniques
- Triggers destruction of fuze technology.

To protect the more advanced signal processing of fuzes, tamper monitors such as the MSFIPS will detect tampering and protect the devices with either burning, wiping memory, or overvoltage.