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

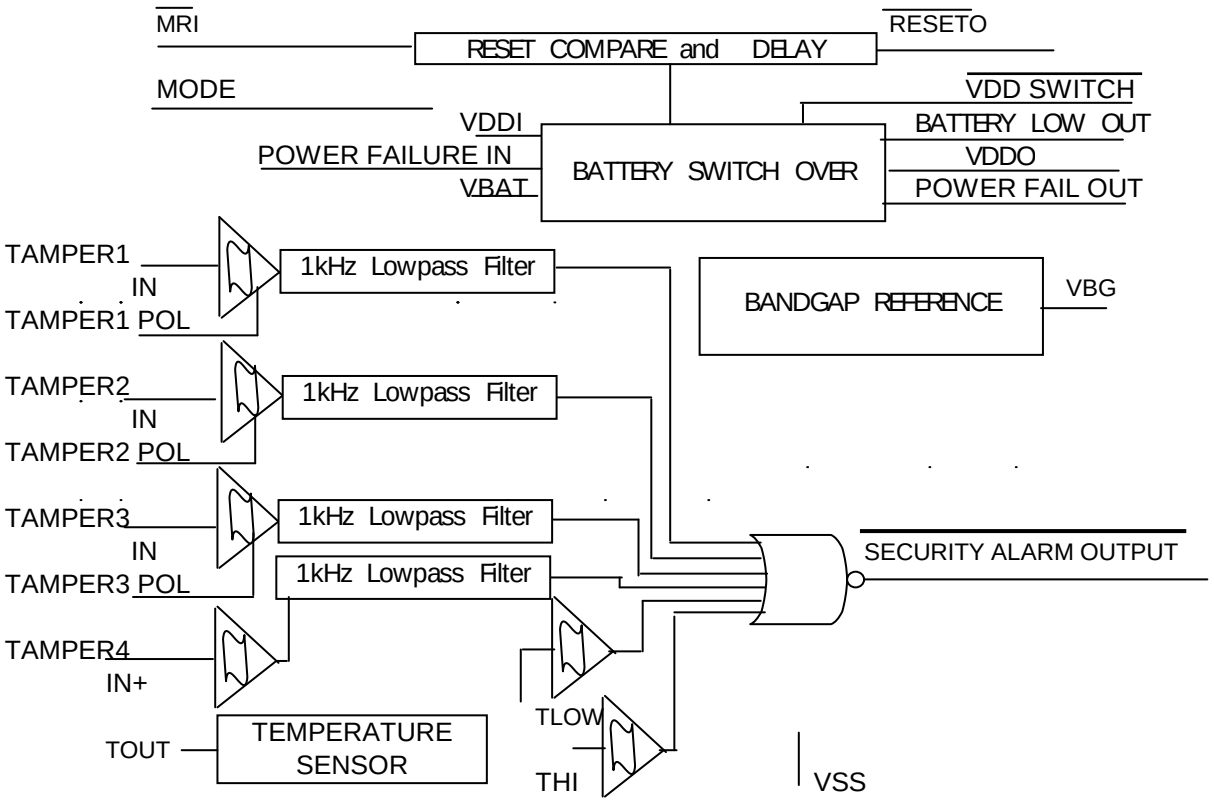
What is F.I.P.S.

- 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

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

MSI's MSFIPS provides Monitoring Functions

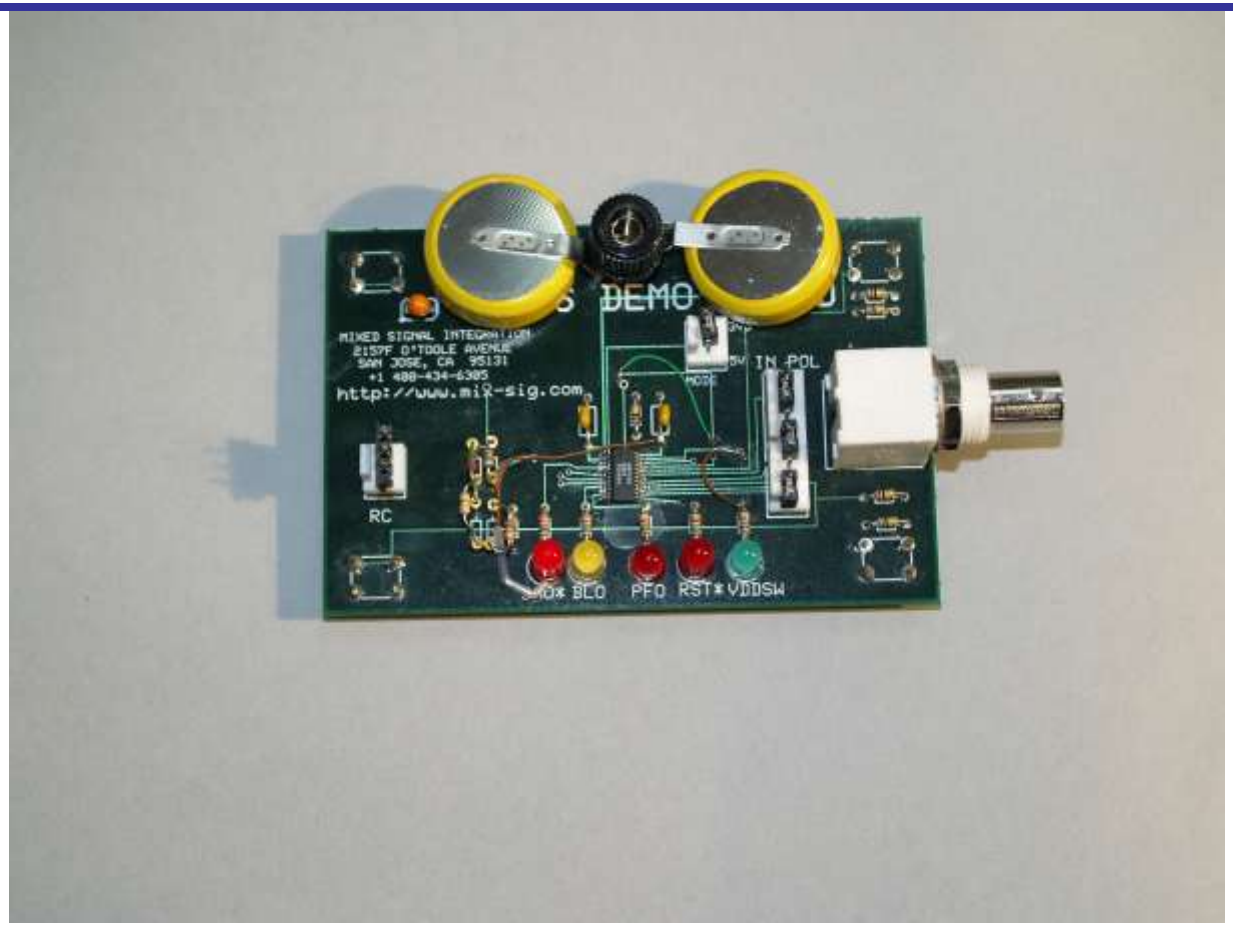


System Design

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.

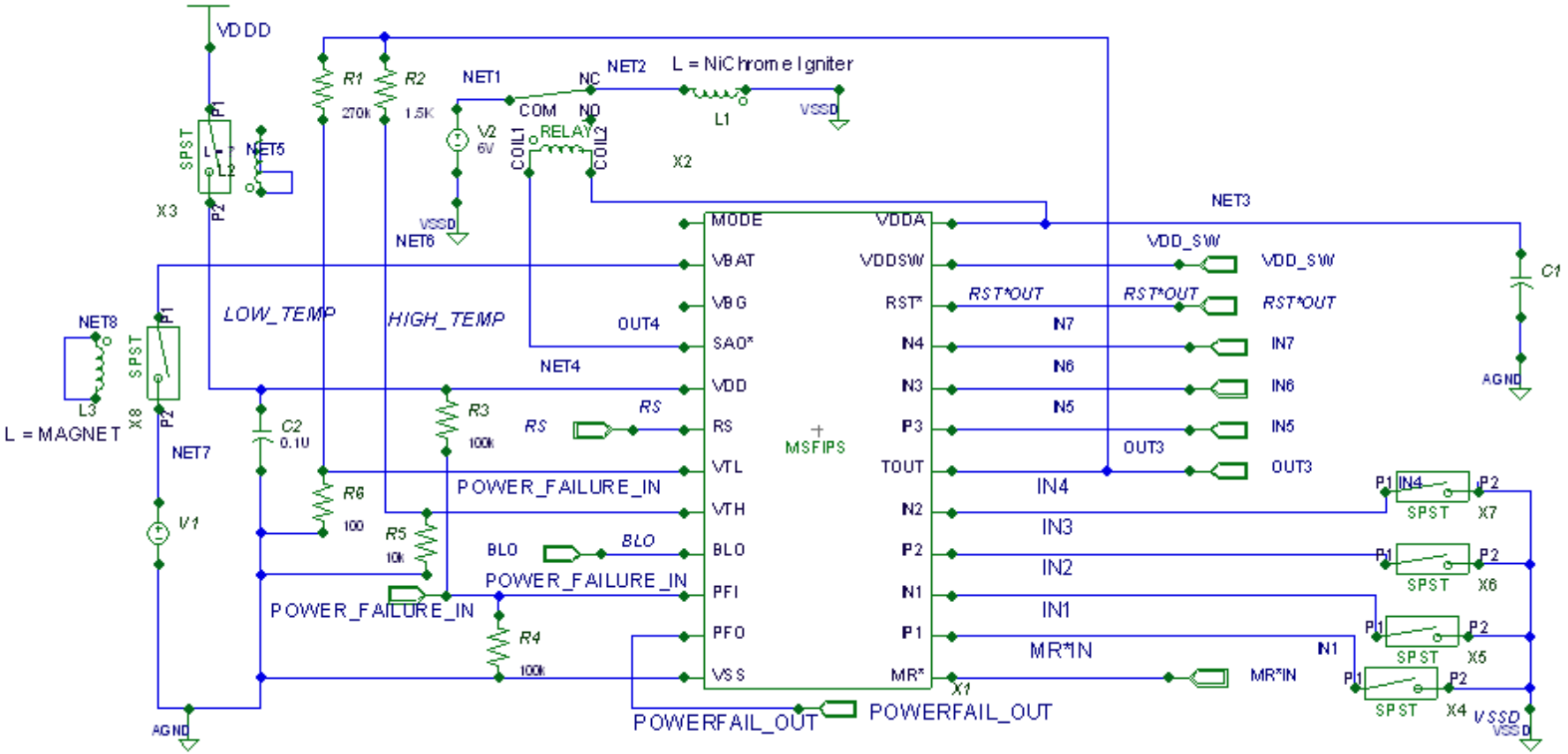
MSFIPS Evaluation Board



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.

Simplified Schematic



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.

Summary

MSFIPS provides monitor and protection to Fuzing technology

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