5/2011

FIPS-140 Level 4+ Security Supervisor Data Sheet

Description

The MSFIPS integrated circuit provides 4 physical tamper switch inputs (3 with polarity control), over/under voltage detection and a temperature sensor. The MSFIPS provides the sensor interfaces needed for the Federal Information Processing Standard (FIPS) 140.

The polarity selectable inputs are intended to interface with a variety of tamper switches, The 1 kHz lowpass filters provide better noise immunity than the single input available on other interfaces. An internal bandgap reference provides an accurate comparison voltage for sensing a over-voltage or undervoltage tampering technique. Temperature variation outside of expected environmental conditions also will trigger an alarm. The MSFIPS operates from 2.4V up to 5.5 VDC. For battery backup, the supply switching is automatically done internally.

The MSFIPS is available in die form and in a 24 pin SSOIC package. Temperature range is –40 to +85 °C.

Features

Temperature sensor
Bandgap reference for under/over voltage detect
Four switch inputs (Three with polarity selection)
Automatic battery switchover

Applications

Cryptography boxes
Electronic Medical Storage security
Credit processing storage security
Point of Sales Terminals
Alarm Systems.

Absolute Maximum Ratings

Power Supply Voltage	+6V
Storage Temperature Range	-60 to +150 °C
Operating Temperature Range	-40 to +85 °C

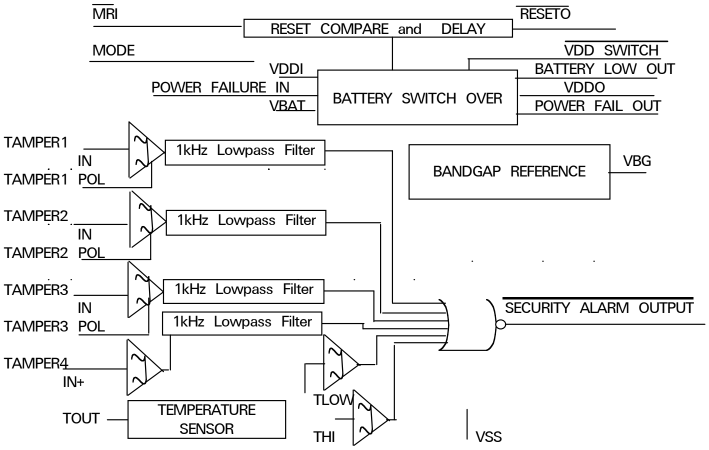

Figure 1 - Block Diagram

FIPS-140 Level 4+ Security Supervisor Data Sheet

Electrical Characteristics

(VDD = +5.0V, T = 25 °C)

MSFIPS

PARAMETER	SYMBOL	CONDITIONS	MIN	TYP	MAX	UNITS
DC Specifications						
Operating Voltage	VDD		2.4	5.0	5.5	V
Supply Current	IDD+IBAT		0.5	0.8	2.0	mA
Supply Current	IDD+IBAT	VDD = +3.3V		0.5		mA
Reference Voltage	VREF	RL = 1 MΩ		1.25		V
Reset Threshold Voltage 5V	V_{RST}	RESETC=0		4.7		V
		RESETC=1/2*VDD		4.4		V
		RESETC=VDD		4.1		V
Reset Threshold Voltage 3.3V	V_{RST}	RESETC=0		3.1		V
		RESETC=1/2*VDD		2.85		V
		RESETC=VDD		2.6		V
Voltage Output Low	V_{OL}	-		0.2		V
Voltage Output High	V_{OH}			4.0		V
Input Voltage Low	V_{IL}	-		0.4*V		V
Input Voltage High	V_{IH}			0.6*V		V
Battery Backup SwitchoverV	V_{SO}	VDD=5.0V or 3.3VDC		2.6		V
Under Voltage Detect	V_{LV}	VDD=5.0V		3.3		V
Under Voltage Detect	V_{LV}	VDD=3.3		2.7		V
Over Voltage Detect	V_{HV}	VDD=5.0		5.5		V
Over Voltage Detect	V_{HV}	VDD=3.3		4.2		V
Battery Low Detect Voltage	V_{DET}	-		2.4		V
Power Failure Comparator V	V_{PFI}			1.25		V
TOUT Voltage	V_{TOUT}	T = 25 °C		1.6		Vdc
TOUT Voltage tempco	VTOUT/°C	from -40°C to +85°C		3		mV/°C

FIPS-140 Level 4+ Security Supervisor Data Sheet

Principle of Operation

The MSFIPS integrated circuit with 4 physical tamper switch inputs are ideal for either normally open or normally closed switches. With these switches attempts to open the system, or remove socketed components are detected.

Attempts to heat a box, to remove potting material, or to cause RAM R/W errors, are detected by the temperature sensor.

If the unit is unplugged from its power source, the switch to battery power is detected. When the battery voltage is too low, a signal is provided for action to be taken

Attempts at glitching the reset signal or overvoltage are detected by the reset voltage timing compare with the VDDO voltage and a delay. If attempts to override the system firmware by applying an overvoltage to VDD are detected, action to protect the internal code can be taken.

VDDO for the controller can switch up to 0.2 A..

MSFIPS

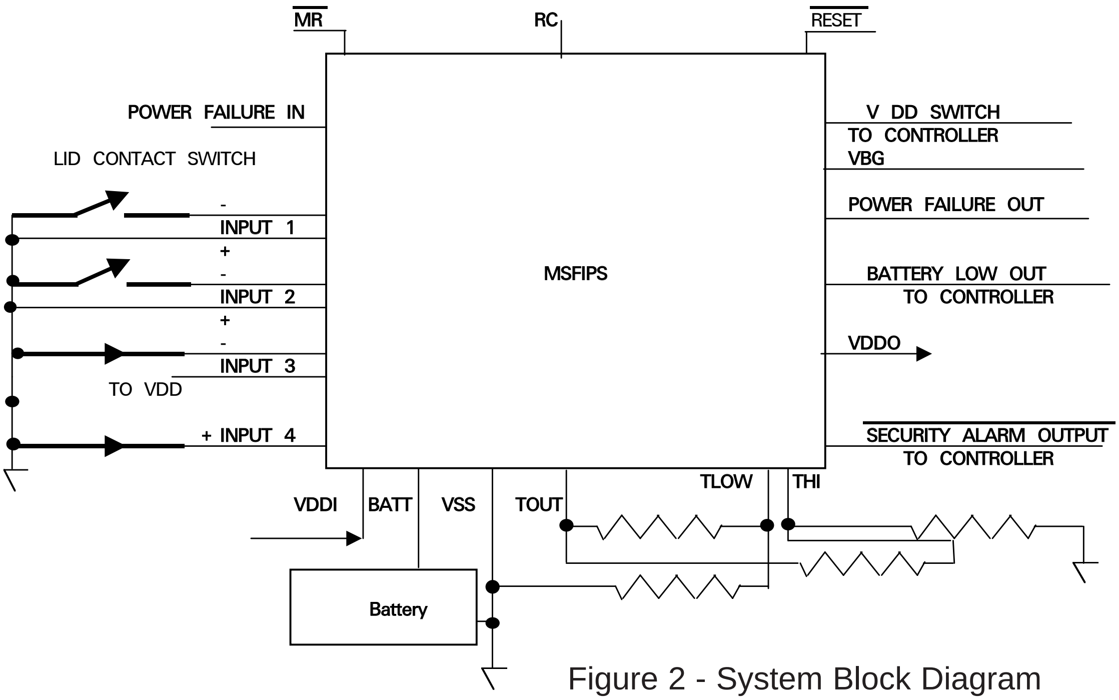

Figure 2 - System Block Diagram

Mixed Signal Integration Corporation reserves the right to change any product or specification without notice at any time. Mixed Signal Integration products are not designed or authorized for use in life support systems. Mixed Signal Integration assumes no responsibility for errors in this document.

MSFIPS

Pin Description

1. MODE Selects 3.3V or 5.0 VDC operation. When MODE is at Logic "1" 3.3V thresholds are selected, When MODE is at Logic "0", 5.0VDC is selected.

2. VBAT Positive Battery Input,

3. VBG Bandgap Voltage Output

4 $\overline{\text{SAO}}$ Security Alarm Output Not

5 VDDI Positive System Supply; For 5V Operation Typically 5.0 VDC

6. RC Set Reset Voltage: Tertiary Control

7. VTL Temperature Low set Input

8. VTH Temperature High set input

9. BLO Battery Low Voltage Indicator. When High, Battery is below 2.4V

10. PFI Power Failure Input Sense

11. PFO Power Failure Output: Output high when power is absent

12. VSS Negative Supply; Typically 0.0 VDC

13. $\overline{\text{MR}}$ Master Reset Not Input

14 IP1 Tamper Switch Polarity Input 1 When tied to logic "1", Tamper switch logic is inverted (uses NO switch). NC switch when logic "0".

15. IN1 Tamper Switch Input 1

16. IP2 Tamper Switch Polarity Input 2 When tied to logic "1", Tamper switch logic is inverted (uses NO switch). NC switch when logic "0".

17. IN2 Tamper Switch Input 2

18. TOUT Temperature Sensor Output

19 IP3 Tamper Switch Polarity Input 3 When tied to logic "1", Tamper switch logic is inverted (uses NO switch). NC switch when logic "0".

20. IN3 Tamper Switch Input 3

21. IN4 Tamper Switch Positive Input 4

22. $\overline{\text{RST}}$ Voltage Qualified Reset Not Output

23 VDDSW Power Switch Indicator: When High, Battery backup is in use

24. VDDO Positive Power Supply Output Typically 5 VDC for 5V operation

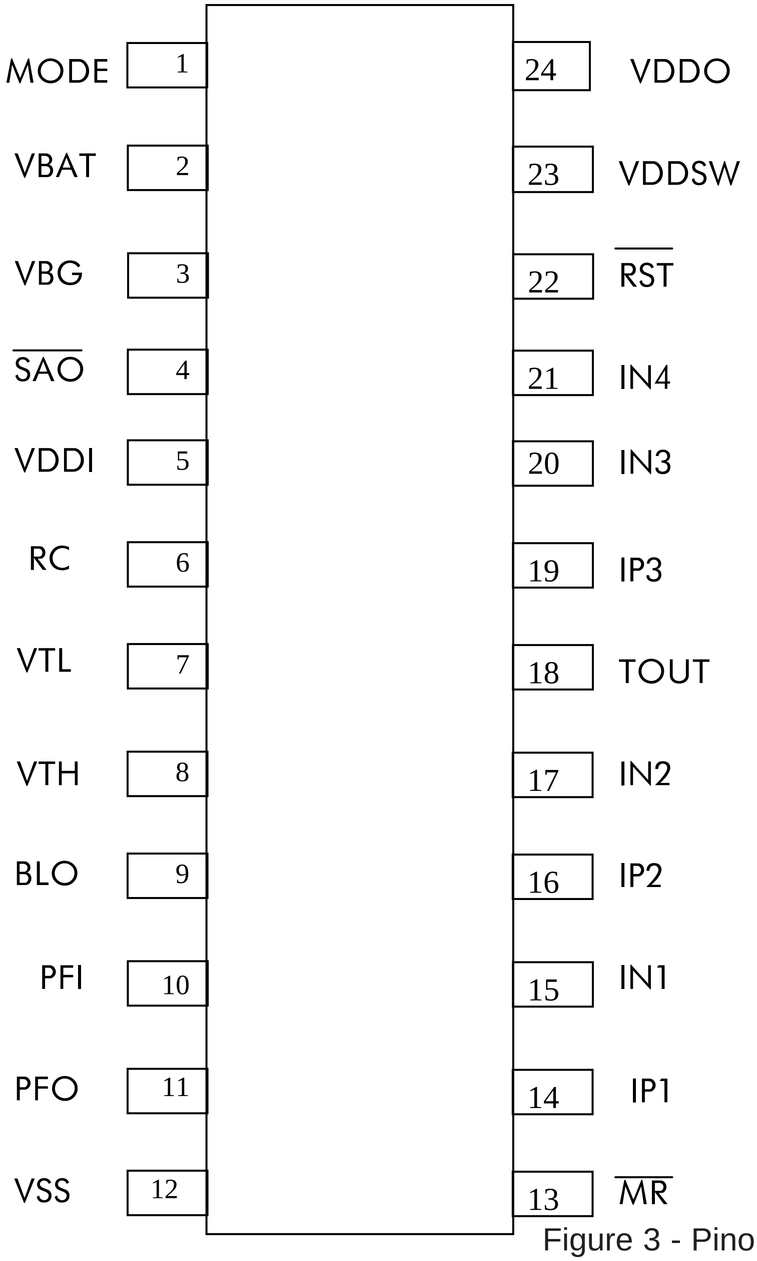

Figure 3 - Pinout Diagram

MSFIPS

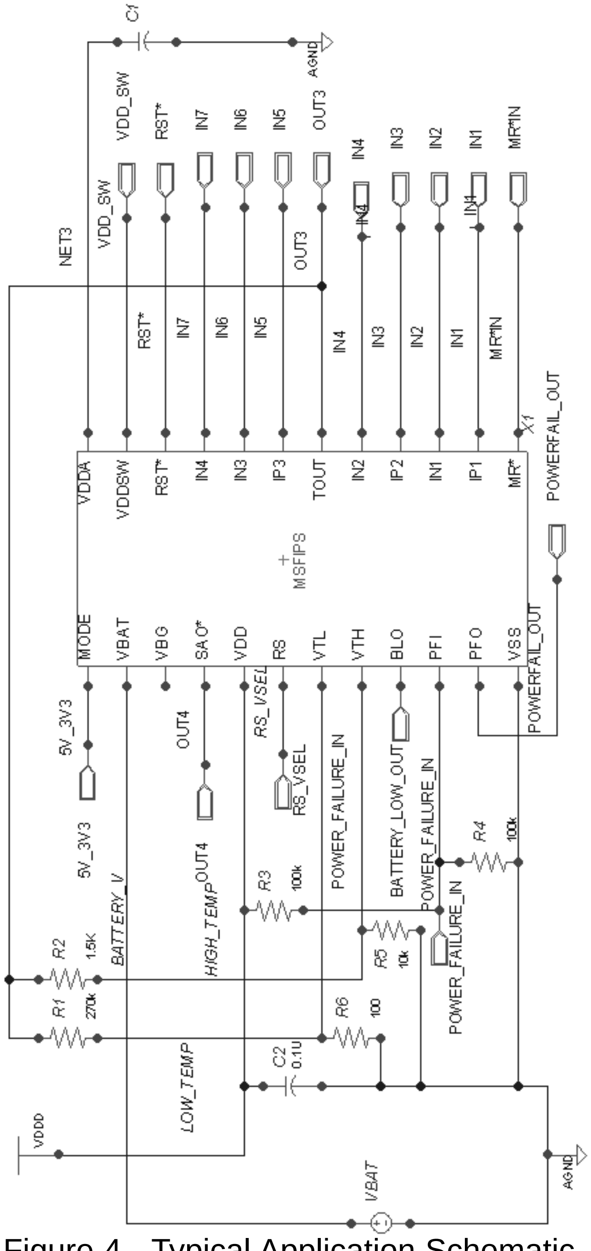

Figure 4 - Typical Application Schematic

STANDARD PRODUCTS

MSGEQ5A	Five Band Graphic Equalizer Display Filter
MSGEQ7	Seven Band Graphic Equalizer Display Filter
MSHFS1-6	Selectable High Frequency LP/BP Filter
MSFS1-6	Selectable Lowpass/Bandpass Filter
MSCAHF	Selectable High Frequency Active Lowpass/Bandpass Filter
MSU1F1-4, MSU2F1	Resistor Programmable Universal Active Filter
MSU1HF1-4, MSU2HF1	High Frequency Resistor Programmable Universal Active Filter
MSELP	Switched Capacitor Elliptic Lowpass Filter with Op Amps
MSNBLP	Switched Capacitor Butterworth Lowpass Filter
MSLE/B/C5L/M	Switched Capacitor General Purpose Lowpass Filter
MS2LFS	Dual Selectable Low Voltage Lowpass/Bandpass Filter
MSLFS	Selectable Low Voltage Lowpass/Bandpass Filter
MSHN1-6	Selectable High Pass/Notch Filter
MSRAAF	Resistor Programmable Active Audio Filter
MSRAHF	Resistor Programmable Active High Frequency Filter
MSDET	Tone Detector
MSEPAF	Electrically Programmable Active Filter
MSCBT	Communications Baseband Transceiver
MSVL14	14 MHz Video Lowpass Filter
MSSPSI	Smart Programmable Sensor Interface
MSCPSI	Computer Programmable Sensor Interface
MSLOSC	15 Hz to 64 kHz All Silicon Sine Source
MSTHDA	Total Harmonic Distortion Analyzer
MSSCSA	Single Chip Spectrum Analyzer
MSFIPS	FIP-140 Level 4+ Security Supervisor
MSLSA	Low Power Single Chip Spectrum Analyzer
MSRFIF	Radio Frequency Interface Front-End
MSVHFS1-6	Selectable Very High Frequency LP/BP Filter
MSMXVHF	High Frequency Mixer and Selectable VHF LP/BP Filter

2157F O'Toole Avenue
San Jose, California 95131-1332
Phone: (408)-434-6305
Fax: (408)-434-6417

IF YOUR STATE OR COUNTRY IS NOT LISTED BELOW, PLEASE CONTACT MSI DIRECTLY

In Mississippi, Alabama, Georgia South Carolina, North Carolina, and Tennessee contact:

AdeptRep
280 Metaire Lane
Madison, Alabama 35758
Telephone: 256-772-1922
Facsimile: 256-325-2841
Toll Free: 1-888-419-2563
Web site: www.adeptrep.com

In northern Illinois and southeastern Wisconsin contact:

M&S Sales Inc.
187 Old Sutton Road
Barrington Hills, IL 60010
Telephone: 847-426-8155
Facsimile: 847-426-8120

In Arizona, Utah, Colorado, Montana, Wyoming, Idaho, New Mexico and southern Nevada contact:

Nelco TWO Company
8617 Gold Peak Dr., Unit A
Highlands Ranch, CO 80130
Telephone: 303-792-0657

In Hong Kong and the People's Republic of China contact:

Alphatron
282, King's Rd.,
13th Floor, Flat C2,
North Point Centre, North Point
Hong Kong
H.K. Telephone: 852-9453-2305
China Telephone: 86 1392 3826 400
Facsimile: 852-22491-1365 or
852-2900-3616

In Korea contact:

H. B. Corp.
7F, Hyobong Building 1364-1,
Seocho-Dong, Seocho-Gu,
Seoul, Korea 137-070
Telephone: (02)3472-3450
Facsimile: (02)3472-3458
Website: www.hbcorp.co.kr

In Singapore, Indonesia and Malaysia contact:

EXER Technologies (S) PTE LTD
45 Kaki Bukit Industrial Terrace
Singapore 416125
Telephone: (65)-6-747-9669
Facsimile: (65)-6-749-9669

In Israel contact:

Phoenix Technologies Ltd.
3 Gavish St.
Kfar-Saba, 44424
Israel
Telephone: 09-764-4800
Facsimile: 09-764-4801
Website: www.phnx.co.il

In Taiwan contact

Maxtek Technology Co., Ltd.
5F, No. 13-20, Sec. 6, Min Chian E Road, Nei Hu
Taipei, 114 R.O.C.
Telephone: 886-2-2794-6060
Facsimile: 886-2-2879-8922

In the United Kingdom contact:

Broadband Technology 2000 Ltd
Victory House
Marino Way
Finchampstead
Berkshire
RG40 4RF
U. K.
Telephone: +44 (0) 118 932 4600
Facsimile: +44 (0) 118 973 0571
E-mail: sales@bt2000.co.uk
Web site: www.bt2000.co.uk

In Germany, Austria and Switzerland

ED-V GmbH
Behringerstrasse 13
D 63814 Mainaschaff
Germany
Telephone: 49 6021 79710
Facsimile: 49 6021 797144
Web site: www.ed-v.de

Catch our web site at "http://www.mix-sig.com"

Send us e-mail at "info@mix-sig.com"