# STM1403, STM1404

## 3V FIPS-140
## Security Supervisors with Battery Switchover

**DATA BRIEFING**

## FEATURES

- STM1403 SUPPORTS FIPS-140 SECURITY LEVEL 3+
  - 4 High-Impedance Physical Tamper Inputs
  - Over/Under Operating Voltage Detector
  - Security Alarm ($\overline{SAL}$) on Tamper Detection
- STM1404 SUPPORTS FIPS-140 SECURITY LEVEL 4
  - STM1403+ Over/Under Operating Temperature Detector
  - Over/Under Temperature Thresholds are Customer-Selectable and Factory-Programmed
- STM1403 AND STM1404 ARE 100% PIN-COMPATIBLE
- SUPERVISORY FUNCTIONS
  - Automatic Battery Switchover
  - $\overline{RST}$ Output (Open Drain)
  - Manual (Push-button) Reset Input ($\overline{MR}$)
  - Power-fail Comparator (PFI/$\overline{PFO}$)
- $\overline{Vccsw}$ ($V_{CC}$ SWITCH OUTPUT)
  - Low When Switched to $V_{CC}$
  - High When Switched to $V_{BAT}$ (BATT ON Indicator)

**Figure 1. Package**

QFN16, 3x3mm (Q)

- BATTERY LOW VOLTAGE DETECTOR (POWER-UP)
- OPTIONAL $V_{REF}$ (1.237V)
  (Available for STM1403A/1404A only)
- LOW BATTERY SUPPLY CURRENT (TYPICAL)
  - STM1403: 2.8µA ($V_{BAT}$ = 3.3V, 25°C)
  - STM1404: 5.3µA ($V_{BAT}$ = 3.3V, 25°C)
- SECURE LOW PROFILE 16-PIN, 3x3mm, QFN PACKAGE

**Table 1. Device Options**

| | STM704 Functions(1) | Physical Tamper Inputs | Over/Under Voltage Alarms | Over/Under Temperature Alarms | $V_{REF}$ (1.237V) Option | $V_{OUT}$ Status, During Alarm | $\overline{Vccsw}$ Status, During Alarm |
|---|---|---|---|---|---|---|---|
| STM1403A | ✔ | ✔ | ✔ | | ✔ | ON | Normal Mode(2) |
| STM1403B | ✔ | ✔ | ✔ | | Note 3 | High-Z | High |
| STM1403C | ✔ | ✔ | ✔ | | Note 3 | Ground | High |
| STM1404A | ✔ | ✔ | ✔ | ✔ | ✔ | ON | Normal Mode(2) |
| STM1404B | ✔ | ✔ | ✔ | ✔ | Note 3 | High-Z | High |
| STM1404C | ✔ | ✔ | ✔ | ✔ | Note 3 | Ground | High |

Note: 1. $\overline{SAL}$, $\overline{RST}$, $\overline{PFO}$, and $\overline{BLD}$ are Open Drain.
2. Normal Mode: Low when $V_{OUT}$ is internally switched to $V_{CC}$ and High when $V_{OUT}$ is internally switched to battery.
3. Pin 9 is the $V_{REF}$ pin for STM1403A, STM1404A. It is the $V_{TPU}$ pin for STM1403B/C and STM1404B/C.

## SUMMARY DESCRIPTION

The STM1403/4 family of security supervisors are a low power family of intrusion (tamper) detection chips targeted at manufacturers of POS terminals and other systems, to enable them to meet **physical and/or environmental** intrusion monitoring requirements as mandated by various standards, such as Federal Information Processing Standards (FIPS) Pub 140 entitled “Security Requirements for Cryptographic Modules,” published by the National Institute of Standards and Technology, U.S. Department of Commerce), EMVCo, ISO, ZKA, and VISA PED.

STM1404 will target the highest security level 4 and include both physical and environmental (voltage and temperature) monitoring, while STM1403 will be a 100% pin-compatible, functional subset of the STM1404, to target levels 3 and lower, and includes all of the functionality of the STM1404, except for the over/under temperature monitoring.

The STM1403 and STM1404 include Automatic Battery Switchover, $\overline{RST}$ Output (Open Drain), Manual (Push-button) Reset Input ($\overline{MR}$), Power-fail Comparator (PFI/$\overline{PFO}$), Physical and/or Environmental Tamper Detect/Security Alarm, and Battery Low Voltage Detect features.

The STM1404A and the STM1403A also offer a $V_{REF}$ (1.237V) as an option on pin 9. On STM1403B/C and STM1404B/C this pin is $V_{TPU}$ (internally switched $V_{CC}$ or $V_{BAT}$).

### $V_{OUT}$ Pin Modes

Either part type can be made available in three versions, corresponding to three modes of the $V_{OUT}$ pin (Supply Voltage Out), when the $\overline{SAL}$ (Security Alarm) is asserted (active-low) upon tamper detection:

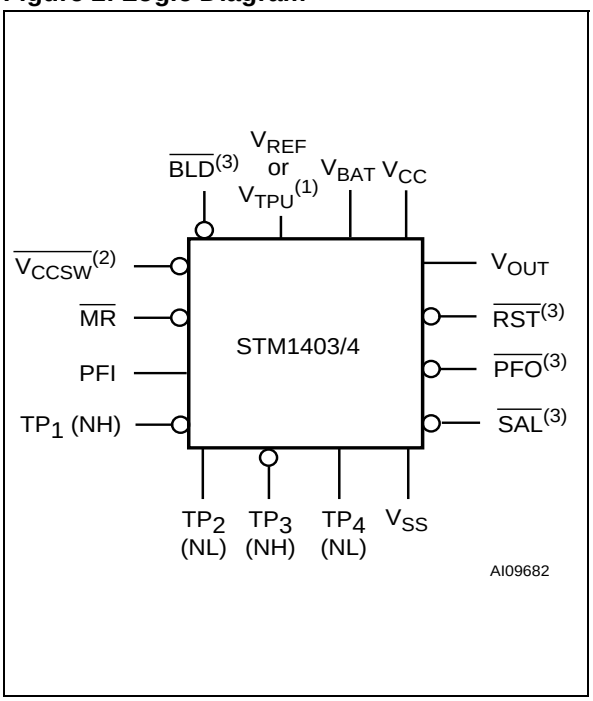
**STM1403A, STM1404A.** $V_{OUT}$ stays ON (at $V_{CC}$ or $V_{BAT}$) when $\overline{SAL}$ is driven low (activated).

**STM1403B and STM1404B.** $V_{OUT}$ is set to High-Z when $\overline{SAL}$ is driven low (activated).

**STM1403C and STM1404C.** $V_{OUT}$ is driven to Ground when $\overline{SAL}$ is activated (may be used when $V_{OUT}$ is connected directly to the $V_{CC}$ pin of the external SRAM that holds the cryptographic codes).

All variants (see Table 1., Device Options) are pin-compatible and available in a security-friendly, low profile, 16-pin QFN package.

**Figure 2. Logic Diagram**



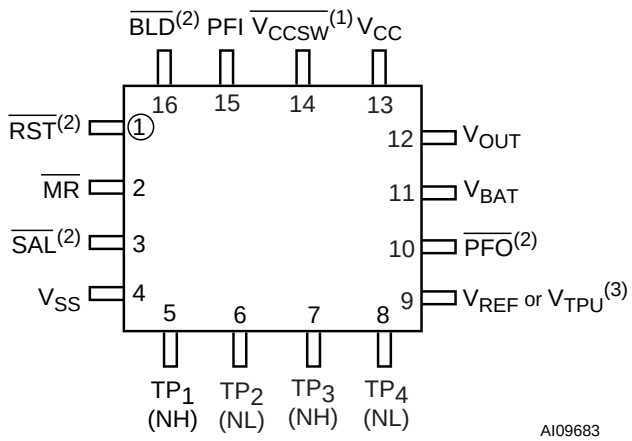

Note: 1. $V_{REF}$ only for STM1403/4A; $V_{TPU}$ for STM1403B/C and STM1404B/C.
2. Normal Mode: Low when $V_{OUT}$ is internally switched to $V_{CC}$ and High when $V_{OUT}$ is internally switched to battery.
3. $\overline{SAL}$, $\overline{RST}$, $\overline{PFO}$, and $\overline{BLD}$ are Open Drain.

**Table 2. Signal Names**

| | |
|---|---|
| $\overline{V_{CCSW}}$(1) | $V_{CC}$ Switch Output |
| $\overline{MR}$ | Manual (Push-button) Reset Input |
| PFI | Power-fail Input |
| $TP_1$ - $TP_4$ | Independent Physical Tamper Detect Pins 1 through 4 |
| $V_{OUT}$ | Supply Voltage Output |
| $\overline{RST}$(2) | Active-low Reset Output |
| $\overline{PFO}$(2) | Power-fail Output |
| $\overline{SAL}$(2) | Security Alarm Output |
| $\overline{BLD}$(2) | Battery Low Voltage Detect |
| $V_{REF}$(3) | 1.237V Reference Voltage |
| $V_{TPU}$(3) | Tamper Pull-up ($V_{CC}$ or $V_{BAT}$) |
| $V_{BAT}$ | Back-up Supply Voltage |
| $V_{CC}$ | Supply Voltage |
| $V_{SS}$ | Ground |

Note: See PIN DESCRIPTIONS, page 9 of the full datasheet for details.
1. Normal Mode: Low when $V_{OUT}$ is internally switched to $V_{CC}$ and High when $V_{OUT}$ is internally switched to battery.
2. $\overline{SAL}$, $\overline{RST}$, $\overline{PFO}$, and $\overline{BLD}$ are Open Drain.
3. $V_{REF}$ only for STM1403/4A; $V_{TPU}$ for STM1403B/C and STM1404B/C.

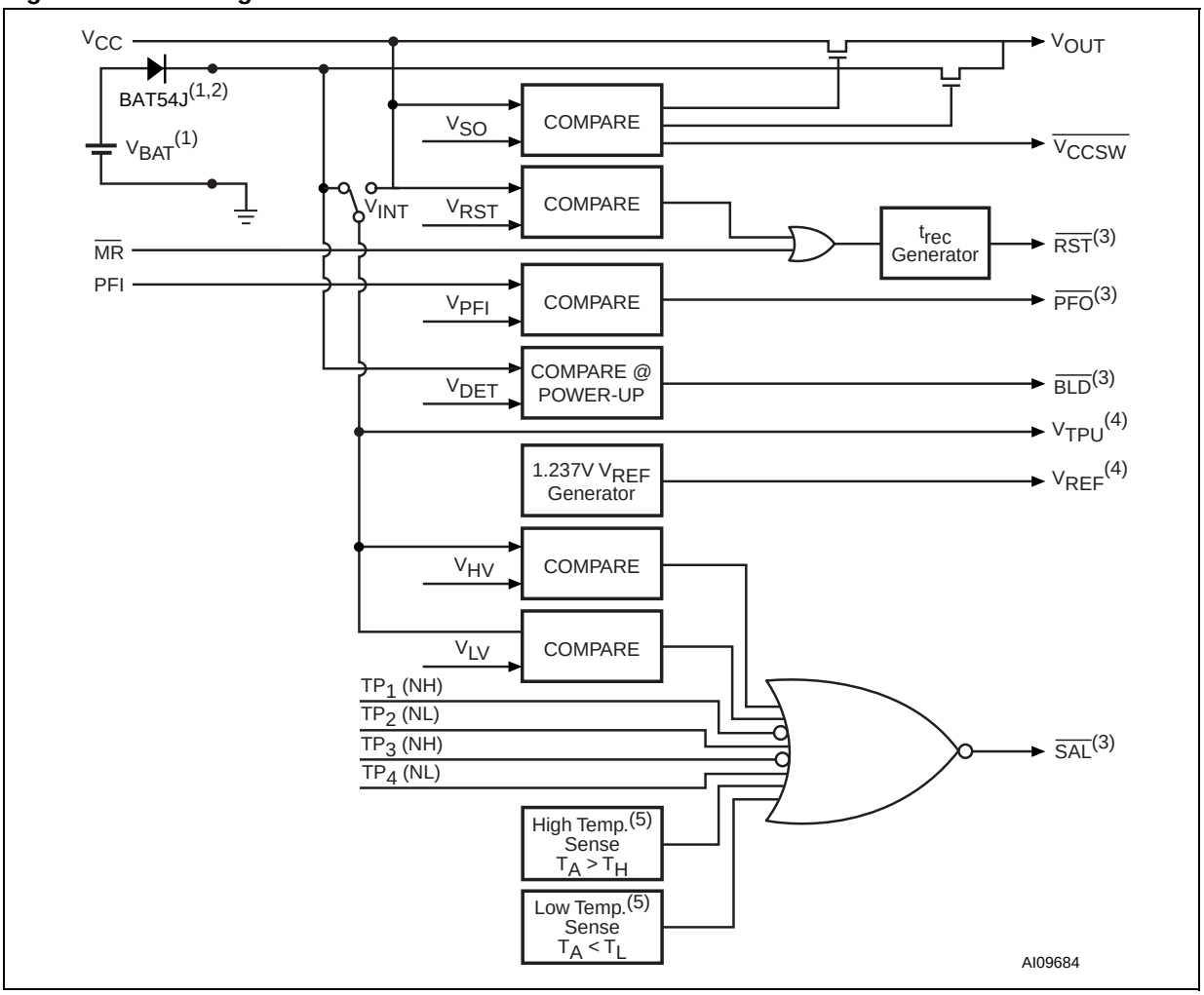
**Figure 3. QFN16 Connections**




Note: See PIN DESCRIPTIONS, page 9 of the full datasheet for details.

1. Normal Mode: Low when $V_{OUT}$ is internally switched to $V_{CC}$ and High when $V_{OUT}$ is internally switched to battery.
2. $\overline{SAL}$, $\overline{RST}$, $\overline{PFO}$, and $\overline{BLD}$ are Open Drain.
3. $V_{REF}$ only for STM1403/4A; $V_{TPU}$ for STM1403B/C and STM1404B/C.

**Figure 4. Block Diagram**




Note: 1. BAT54J (from STMicroelectronics) recommended.
2. Required for battery-reverse charging protection.
3. Open Drain
4. $V_{REF}$ only for STM1403/4A; $V_{TPU}$ for STM1403B/C and STM1404B/C.
5. Available only on STM1404.

## TAMPER DETECTION

### Physical

There are four (4) high-impedance physical tamper detect input pins, 2 normally set to High (NH) and 2 normally set to Low (NL). Each input is designed with a glitch immunity. These inputs can be connected externally to several types of actuator devices (e.g., switches, wire mesh). A tamper on any one of the four inputs that causes its state to change will trigger the security alarm ($\overline{SAL}$) and drive it to active-low. Once the tamper condition no longer exists, the $\overline{SAL}$ will return to its normal High state.

$TP_1$ and $TP_3$ are set Normally to High (NH). They are connected externally through a closed switch or a high-impedance resistor to $V_{OUT}$ (in the case of STM1403/4A or STM1404A) or $V_{TPU}$ (in the case of STM1403B/C, or STM1404B/C), A tamper condition will be detected when the input pin is pulled low. If not used, tie the pin to $V_{OUT}$ or $V_{TPU}$.

$TP_2$ and $TP_4$ are set Normally to Low (NL). They are connected externally through a high-impedance resistor or a closed switch to $V_{SS}$. A tamper condition will be detected when the input pin is pulled high. If not used, tie the pin to $V_{SS}$.

### Supply Voltage

The internally switched supply voltage, $V_{INT}$ (either $V_{CC}$ input or $V_{BAT}$ input) is continuously monitored. If $V_{INT}$ should exceed the over voltage trip point, $V_{HV}$ (set at 4.2V, typical), or should go below the under voltage trip point, $V_{LV}$ (set at 2.0v, typical). $\overline{SAL}$ will be driven active-low. Once the tamper condition no longer exists, the $\overline{SAL}$ pin will return to its normal High state.

### Temperature (STM1404 Only)

The STM1404 has a built-in, bandgap-based sensor to monitor the temperature. If a preset (customer-selectable, factory-programmed) over-temperature trip point ($T_H$) or under-temperature trip point ($T_L$) is exceeded, the $\overline{SAL}$ is asserted low.

When no tamper condition exists, $\overline{SAL}$ is normally High (see PIN DESCRIPTIONS, page 9 of the full datasheet for details).

When a tamper is detected, the $\overline{SAL}$ is activated (driven low), independent of the part type. $V_{OUT}$ can be driven to one of three states, depending on which variant of STM1403 or STM1404 is being used (see Device Options, page 1):

- ON;
- High-Z; or
- Ground ($V_{SS}$).

**Note:** The STM1403 or STM1404 must be initially powered above $V_{RST}$ to enable the tamper detection alarms. For example, if the battery is on while $V_{CC}$ = 0V, no alarm condition can be detected until $V_{CC}$ rises above $V_{RST}$ (and $t_{rec}$ expires). From this point on, alarms can be detected either on battery or $V_{CC}$. This is done to avoid false alarms when the device goes from no power to its operational state.

# PART NUMBERING

**Table 3. Ordering Information Scheme**

Example: STM1403 A T M – Q 6 F

**Device Type**

STM1403: Physical, Voltage Tamper Detect

STM1404: Over/Under Temperature Detect

**$V_{OUT}$ Status ($\overline{SAL}$ = Active-Low)**

A: $V_{OUT}$ = ON; $\overline{Vccsw}$ = Normal Mode

B: $V_{OUT}$ = High-Z; $\overline{Vccsw}$ = High

C: $V_{OUT}$ = Ground; $\overline{Vccsw}$ = High

**Reset Threshold Voltage**

T: $V_{RST}$ = 3.00V to 3.15V

S: $V_{RST}$ = 2.85V to 3.00V

R: $V_{RST}$ = 2.55V to 2.70V

**Battery Low Voltage Detect Threshold ($V_{DET}$)**

M: $V_{DET}$ = 2.3V (Typ)

N: $V_{DET}$ = 2.5V (Typ)

O: $V_{DET}$ = 3.2V (Typ)

**Under (TL)/Over (TH) Temperature Alarm Thresholds (STM1404 only)**

STM1403: Use dash (“–”).

STM1404: Use designators (below).

B: –25/+80°C H: –35/+80°C

C: –25/+85°C I: –35/+85°C

D: –25/+95°C J: –35/+95°C

**Package**

Q = QFN16

**Temperature Range**

1 = 0 to 70°C

6 = –40 to 85°C

**Shipping Method**

F = Tape & Reel

For other options, or for more information on any aspect of this device, please contact the ST Sales Office nearest you.

## REVISION HISTORY

**Table 4. Document Revision History**

| Date | Revision | Description |
|---|---|---|
| 11-October-04 | 1.0 | First Edition |
| 26-Nov-04 | 1.1 | Corrected footprint dimensions; update characteristics (Figure 2, 3, 4, 5, 6, 7, 8, 9, 27, 28, 31; Table 1, 2, 3, 6, 7) |
| 22-Dec-04 | 1.2 | Update characteristics (Figure 5; Table 6, 7, 3) |
| 03-Feb-05 | 1.3 | Update characteristics (Figure 5; Table 6, 7) |
| 25-Feb-05 | 1.4 | Update temperature trip limits (Table 3) |
| 06-May-05 | 2.0 | v2.0 of DB corresponds to v1.5 of DS |