AN1879
Application note

How to use the M41ST87W tamper detect and RAM clear

Introduction

The M41ST87W is a supervisory family circuit that provides the industry with the latest in onchip security solutions. The tamper detection and RAM clear circuit can be used in any system to protect sensitive data from tampering. This chip can be used to secure a wide range of applications from credit card machines and point-of-sale (POS) terminals to electric data meters. The M41ST87W features the ability to detect and timestamp any tampering of the system, and corrupt the device memory when the event occurs. This prevents the intruder from accessing data stored in memory by clearing the device memory and/or external RAM when the tampering event occurs.

Contents

1 Description 3
1.1 How it works 3
1.2 Clearing the external memory with the tamper registers 3
1.3 Clearing the external memory with an external charge pump 3
1.4 RAM clear data 5
1.5 Tamper timestamp 5
2 Conclusion 6
3 Revision history 7

1 Description

1.1 How it works

The M41ST87W device provides two independent tamper input pins, $TP1_{IN}$ and $TP2_{IN}$ that can be used to monitor two separate signals. These two tamper input pins can be set to indicate that a tamper event has occurred by either 1) closing a switch (normally open) to ground or V_{OUT} or 2) opening a switch that was previously closed (normally closed) to ground or V_{OUT}. The closing and opening of the switch is configurable using bits that are set in the tamper registers.

The M41ST87W device includes 128 bytes of internal RAM that the user has the option of clearing by setting the TEB and CLR bits in the tamper registers.

1.2 Clearing the external memory with the tamper registers

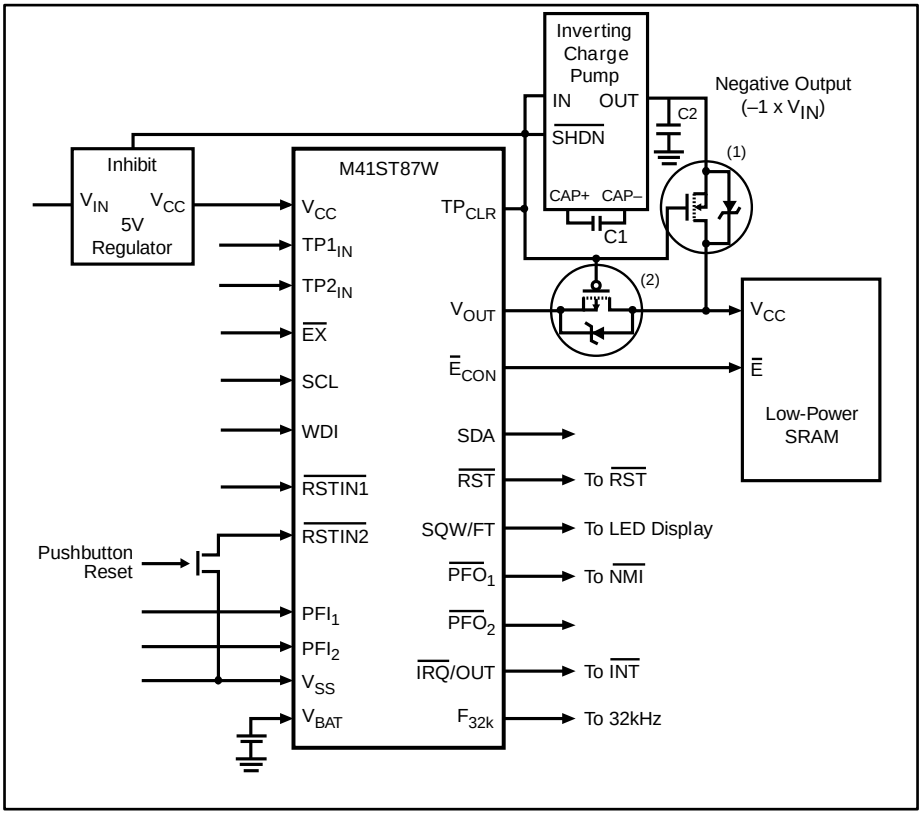
The M41ST87W can also clear the external, battery-backed up SRAM of the device by setting the TEB and CLREXT bits in the tamper registers. To clear/corrupt the external memory, V_{CC} of the SRAM can be taken to ground. However, certain SRAMs require a significant amount of time for the memory to be corrupted if V_{CC} is simply grounded. To corrupt the memory in a reasonable amount of time, one can take V_{CC} of the SRAM to a negative voltage. By taking V_{CC} to a negative voltage, the input protection diode turns on and goes into conduction mode so that it corrupts the memory.

1.3 Clearing the external memory with an external charge pump

An external charge pump device should be used with the M41ST87W to drive V_{CC} of the SRAM to a negative voltage during the tamper condition. *Figure 1: "Circuit connections"* shows how to connect this circuit. When using the M41ST87W with the charge pump device, the user must also provide two additional MOSFETs to isolate V_{OUT} of the M41ST87W from the output (OUT) of the charge pump during normal operation, and from V_{OUT} of the M41ST87W device during the tamper condition. During normal operation the TP_{CLR} signal will be forced low, disabling the charge pump. When disabled, the output of most charge pumps will be forced to ground. In order to allow proper operation of the SRAM, MOSFET(1) must be "off" to isolate V_{CC} of the SRAM from the charge pump output. At this same time, the P-channel MOSFET(2) will be "on" to provide the supply voltage for the SRAM.

During a tamper condition, the TP_{CLR} signal will be forced high, controlling the inhibit pin of the DC regulator. This will put the regulator in standby mode for t_{CLR}. The t_{CLR} is the tamper clear timing where the regulator will be switched off for 1, 4, 8, or 16 seconds, depending on the setting of the CLRPW1 and CLRPW0 bits in the register. The TP_{CLR} signal also enables the charge pump. When the charge pump is enabled, OUT generates a negative voltage on the V_{CC} pin of the SRAM (for a programmable period of time), causing data corruption. The M41ST87W must be isolated from the V_{CC} of the SRAM to avoid data corruption of the M41ST87W due to forward biasing of the parasitic diode of the M41ST87W V_{OUT} output. This is accomplished by using the TP_{CLR} signal to turn the N-channel MOSFET(1) "on," while turning the P-channel MOSFET(2) "off."

Figure 1: Circuit connections

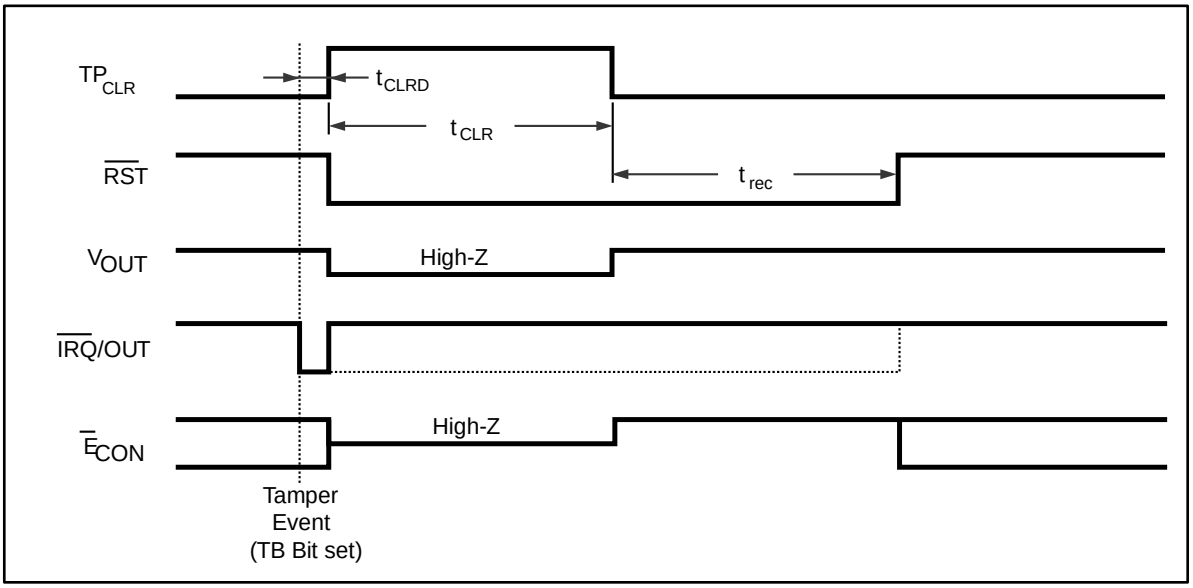


1. N-channel MOSFET
2. P-channel MOSFET

1.4 RAM clear data

Depending on the process technology used to manufacture the external SRAM, clearing the memory may require varying durations of negative potential on the VCC pin. The M41ST87W device allows the user to program the time needed for their particular application. The control bits CLRPW0 and CLRPW1, located in the day register, determine the duration of the tCLR pulse width during a tamper event (see *Figure 2: "Tamper output timing"*). Thus, users can control the voltage and duration of the negative pulse enabling them to configure the circuit for many different LPSRAMs.

Figure 2: Tamper output timing



Note: see M41ST87W datasheet for timing details.

1.5 Tamper timestamp

When the device is tampered with, and regardless of which tamper occurs first, a time stamp freezing the update of the clock registers will occur to let the user know when it was tampered with. The tamper bits (TB1 or TB2 in the flag register) will be set immediately. Therefore, when tampering occurs, the user may elect to first read the time registers to determine exactly when the tamper event occurred, then read the flag register to see which tamper condition was triggered. The clock will update to the current time after resetting the TEB bit in the tamper registers. The appropriate TEB bit must always be reset to '0' in order to read the current time. The tamper detect function operates in V_{CC} as well as in battery backup.

2 Conclusion

With the increasing frequency of credit card fraud and identity theft, ST is leading the way protecting this sensitive data with its new line of secure RTCs. This sensitive data is stored in internal or external memory of most devices like ATM machines or POS terminals. The M41ST87W solution can provide early detection when these devices have been tampered with and clear the RAM before the intruder can access this data.

3 Revision history

Table 1: Document revision history

Date	Revision	Changes
04-Feb-2004	1	First edition
12-Apr-2004	2	Reformatted; updated vendor SRAM information (Table 1)
03-Jun-2004	3	Corrected drawing (*Figure 1: "Circuit connections"*)
16-Jan-2009	4	Reformatted document; updated cover page, *Section 1.3: "Clearing the external memory with an external charge pump"* , *Figure 1: "Circuit connections"* , and RAM clear data
16-Oct-2013	5	Removed Table 1 (RAM clear data with different vendors) and updated *Section 1.4: "RAM clear data"*

Please Read Carefully

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

All ST products are sold pursuant to ST's terms and conditions of sale.

Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST'S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

ST PRODUCTS ARE NOT DESIGNED OR AUTHORIZED FOR USE IN: (A) SAFETY CRITICAL APPLICATIONS SUCH AS LIFE SUPPORTING, ACTIVE IMPLANTED DEVICES OR SYSTEMS WITH PRODUCT FUNCTIONAL SAFETY REQUIREMENTS; (B) AERONAUTIC APPLICATIONS; (C) AUTOMOTIVE APPLICATIONS OR ENVIRONMENTS, AND/OR (D) AEROSPACE APPLICATIONS OR ENVIRONMENTS. WHERE ST PRODUCTS ARE NOT DESIGNED FOR SUCH USE, THE PURCHASER SHALL USE PRODUCTS AT PURCHASER'S SOLE RISK, EVEN IF ST HAS BEEN INFORMED IN WRITING OF SUCH USAGE, UNLESS A PRODUCT IS EXPRESSLY DESIGNATED BY ST AS BEING INTENDED FOR "AUTOMOTIVE, AUTOMOTIVE SAFETY OR MEDICAL" INDUSTRY DOMAINS ACCORDING TO ST PRODUCT DESIGN SPECIFICATIONS. PRODUCTS FORMALLY ESCC, QML OR JAN QUALIFIED ARE DEEMED SUITABLE FOR USE IN AEROSPACE BY THE CORRESPONDING GOVERNMENTAL AGENCY.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

ST and the ST logo are trademarks or registered trademarks of ST in various countries.

Information in this document supersedes and replaces all information previously supplied.

The ST logo is a registered trademark of STMicroelectronics. All other names are the property of their respective owners.

© 2013 STMicroelectronics - All rights reserved

STMicroelectronics group of companies

Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany - Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Philippines - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States of America

www.st.com