AN1879
应用笔记

如何使用M41ST87W的入侵检测及RAM清除功能

前言

M41ST87W是一款可为业界提供最先进的片上安全解决方案的监控电路产品。
入侵检测和RAM清除电路可用于任何系统，保护敏感数据免遭入侵。
该芯片可用于多种不同应用场合的保护，从信用卡机器、刷卡机（POS）终端到电子数据仪表。
M41ST87W可以对任何系统入侵进行侦测和记录时间戳，并在入侵发生时就破坏掉设备存储器中的数据。 通过在发生入侵事件时清除设备存储器和/或外部RAM的方式，防止入侵者访问存储器中的数据。

Contents

1 简介

1.1 工作原理

M41ST87W设备有两个独立的入侵输入引脚TP1IN和TP2IN，可监视两路独立的信号。
任意入侵输入引脚的电平变化都表明发生了入侵事件，变化原因可包括1）引脚由悬空状态变为短路到地或电源，或 2）引脚由对地或电源短路状态变为悬空态
确定入侵引脚原始状态的开关的闭合及打开可以通过入侵寄存器中的比特位进行配置。

M41ST87W设备包含128字节的内部RAM，用户可以选择通过将入侵寄存器中的TEB和CLR比特位置为1的方式进行清除。

1.2 使用入侵寄存器清除外部存储器

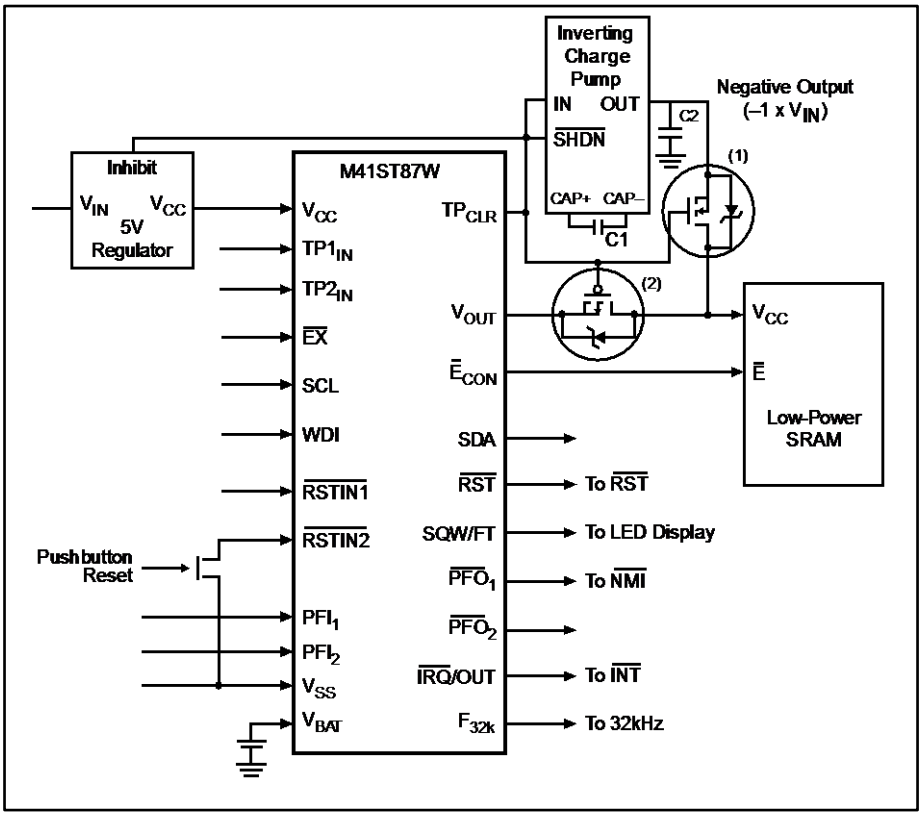
M41ST87W也可以通过将入侵寄存器中的TEB和CLREXT置位的方式清除由备用电池供电的外部SRAM中的数据。 为清除/破坏外部存储器数据，SRAM的V_{CC}可接地。
不过，如果V_{CC}仅简单接地，某些SRAM可能需要较长的时间来破坏存储的数据。
为在合理的时间内破坏存储器，可将SRAM的V_{CC}接至负电位。
将V_{CC}接到负电位上，输入保护二极管就会接通，并进入导通模式，进而破坏存储器。

1.3 使用外部电荷泵清除外部存储器

外部电荷泵设备应当与M41ST87W一起使用，在入侵状况下将SRAM的V_{CC}拉至负电位。
Figure 1: "电路连接" 显示了如何连接此电路。
当M41ST87W与电荷泵设备一起使用时，用户必须提供两个额外的MOSFET，在正常运行中将M41ST87W的V_{OUT}与电荷泵的输出（OUT）隔离，在入侵发生时将其与M41ST87W的V_{OUT}隔离。 正常运行时，TP_{CLR}信号强制拉低，从而禁用电荷泵。
当禁用时，大部分电荷泵的输出将强制接地。
为正确使用SRAM，MOSFET(1)必须“关断”从而将SRAM的V_{CC}与电荷泵输出隔离。 同时，P沟道MOSFET(2)会“导通”，为SRAM提供电源电压。

发生入侵时，TP_{CLR}信号强制拉高，控制直流稳压器的抑制引脚。
这将使稳压器进入待机模式，时间为t_{CLR}。
t_{CLR}是入侵清除的定时时间，稳压器可以关断1、4、8或16秒的时间，具体取决于寄存器中CLRPW1和CLRPW0比特位的设置。 TP_{CLR}信号也可以启动电荷泵。
当电荷泵使能时，OUT会在SRAM的V_{CC}引脚上产生一个负电位（其持续时间可以进行编程控制），从而破坏数据。 M41ST87W必须与SRAM的V_{CC}隔离，避免M41ST87W V_{OUT}输出寄生二极管的前向偏置引起的数据破坏。
具体实现方式是使用TP_{CLR}信号，“导通”N沟道MOSFET(1)，关断P沟道MOSFET(2)。

Figure 1: 电路连接



1. N沟道MOSFET
2. P沟道MOSFET

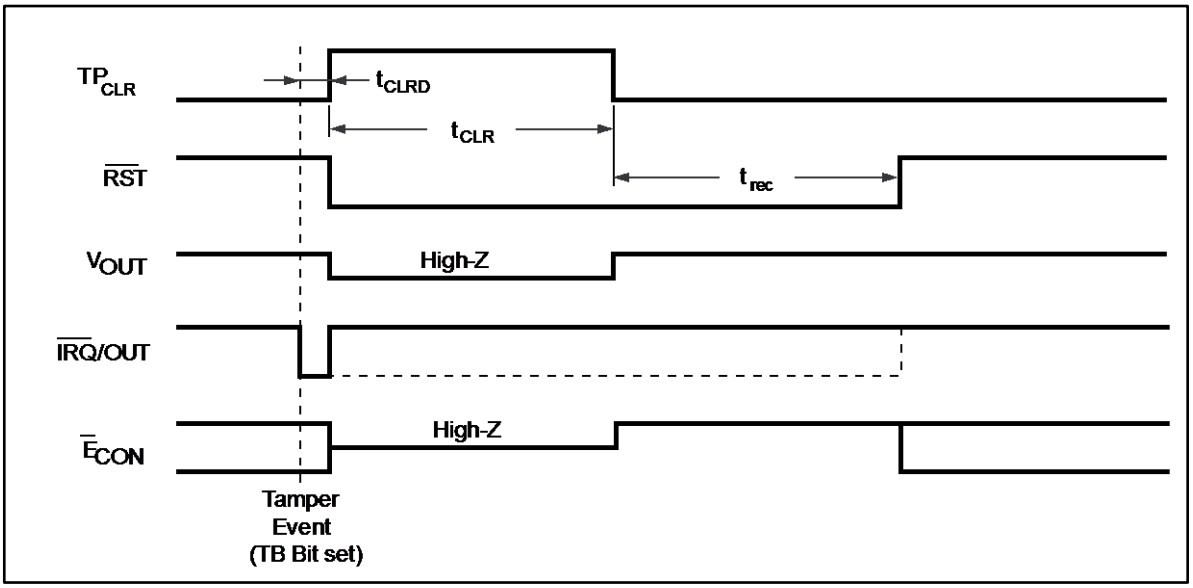
1.4 清除RAM数据

根据外部SRAM制造工艺的不同，清除存储器可能需要VCC引脚上的负电位持续不同的时间。 M41ST87W设备允许用户针对其特定应用对时间进行编程。

日期寄存器中的CLRPW0和CLRPW1比特位可以确定入侵事件中tCLR脉冲宽度的持续时间（见 *Figure 2: "入侵输出时序"*）。

所以，用户可以控制电压和负脉冲的持续时间，从而为许多不同的LPSRAM配置电路。

Figure 2: 入侵输出时序



注意：参看M41ST87W数据手册，获得关于时序的更多详情。

1.5 入侵时间戳

当设备被入侵时，无论先发生何种入侵，都会产生一个冻结时钟寄存器更新的时间标记，让用户知道何时发生入侵。 入侵比特位（标志寄存器中的TB1或TB2位）将立即置为1。
所以当发生入侵时，用户可以选择首先读取时间寄存器，精确确定何时发生入侵，然后读取标志寄存器，查看触发了何种入侵条件。
在入侵寄存器中的TEB位置为0后，时钟将更新到当前的时间。
相应的TEB比特位必须一直置为“0”，以读取当前时间。
入侵检测功能在V_{CC}供电和电池供电的情况下都可以工作。

2 结论

随着信用卡诈骗和身份盗用事件的频发，意法半导体正在利用其最新的安全RTC系列产品，引领敏感数据保护领域的技术潮流。
这些敏感数据通常存储在ATM或POS终端机这类设备的内部或外部存储器中。
当这些设备被入侵时，M41ST87W解决方案可以进行早期检测，在入侵者访问数据之前清除RAM。

3 版本历史

Table 1: 文档版本历史

日期	版本	变更
2004年2月4日	1	第一版
2004年4月12日	2	重新编排格式；更新供应商SRAM信息（表1）
2004年6月3日	3	更正图纸 (*Figure 1: "电路连接"*)
2009年1月16日	4	重新编排文档格式；更新封面、*Section 1.3: "使用外部电荷泵清除外部存储器"*、*Figure 1: "电路连接"*和RAM清除数据
2013年10月16日	5	去除表1（不同的供应商RAM清除数据）并更新 *Section 1.4: "清除RAM数据"*

请仔细阅读下列内容

本文档中信息的提供仅与ST产品有关。
意法半导体公司及其子公司（“ST”）保留随时对本文档及本文所述产品与服务进行变更、更正、修改或改进的权利，恕不另行通知。

所有ST产品均根据ST的销售条款出售。

买方自行负责对本文所述ST产品和服务的选择和使用，ST概不承担与选择或使用本文所述ST产品和服务相关的任何责任。

无论之前是否有过任何形式的表示，本文档不以任何方式对任何知识产权进行任何明示或默示的授权或许可。
如果本文档任何部分涉及任何第三方产品或服务，不应被视为ST授权使用此类第三方产品或服务，或许可其中的任何知识产权，或者被视为涉及以任何方式使用任何此类第三方产品或服务或其中任何知识产权的保证。

除非在ST的销售条款中另有说明，否则，ST对ST产品的使用和/或销售不做任何明示或默示的保证，包括但不限于有关适销性、适合特定用途（及其依据任何司法管辖区的法律的对应情况），或侵犯任何专利、版权或其他知识产权的默示保证。

**意法半导体产品也不是为下列用途而设计并不得应用于下列用途：（A）对安全性有特别要求的应用，例如，生命支持、主动植入设备或对产品功能安全有要求的系统；（B）航空应用；（C）汽车应用或汽车环境，和/或（D）航天应用或航天环境。
如果意法半导体产品不是为前述应用设计的，而采购商擅自将其用于前述应用，即使采购商向意法半导体发出了书面通知，采购商仍将独自承担因此而导致的任何风险，意法半导体的产品设计规格明确指定的汽车、汽车安全或医疗工业领域专用产品除外。
根据相关政府主管部门的规定，ESCC、QML或JAN正式认证产品适用于航天应用。**

转售的ST产品如有不同于本文档中提出的声明和/或技术特点的规定，将立即导致ST针对本文所述ST产品或服务授予的任何保证失效，并且不应以任何形式造成或扩大ST的任何责任。