M41ST87 — новая жизнь кассовых аппаратов

5 июня 2003 года компания STMicroelectronics, один из ведущих производителей электронных компонентов для систем защиты информации, представила новый чип памяти типа SUPERVISOR, ориентированный на приложения, предъявляющие исключительно высокие требования к защите данных. M41ST87 включает в себя контур «Tamper Detect» (определение фальшивки) со стиранием памяти, что позволяет использовать микросхему как устройство для «защищенных приложений», таких, как кассовые аппараты на торговых терминалах или считыватели для кредитных карт. В устройство также интегрирован контроллер энергонезависимой памяти, последовательные часы реального времени, а также минипроцессор. При этом все это выполнено на 28-выводном кристалле SOIC, включающем также генератор 32 кГц. Будучи доступным в 3- и 5-вольтовом исполнении, M41ST87 включает в себя множество общих функций и использует в качестве дублирующего внешнего источника батарею, которая обычно применяется во многих устройствах.

Игорь Лепихин

igorl@gamma.spb.ru

Контур «Tamper Detect» (определение фальшивки) имеет два независимых входа, и каждый, в свою очередь, может быть сконфигурирован под различные схемы включения, обеспечивая тем самым максимальную гибкость для пользователя. Во время детектирования события «подмена» может быть включено очищение встроенной 128-байтной памяти, отправка сигнала прерывания на микроконтроллер и вывод сигнала для очистки внешней памяти. Эти функции не позволят «настойчивому злоумышленнику» проникнуть к данным в памяти, а также проинформируют системный процессор о том, что была попытка взлома системы безопасности. Эти функции также работают в режиме питания от батареи. В микросхему встроены и другие средства защиты, например определение сбоя осциллятора, а также автоматическая маркировка времени, когда фиксируется событие «подмена». Кроме того, M41ST87 имеет уникальный 64-разрядный серийный номер.

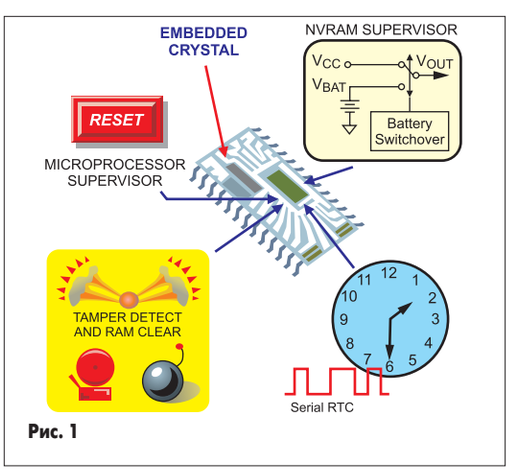

Рис. 1

Новый корпус микросхемы M14ST87 тоже способствует увеличению ее защитных свойств — кристалл не может быть заменен злоумышленниками, таким образом, он продолжит свою работу после попытки взлома. В дополнение к этому, новый корпус лучше защищает кристалл от внешних вредных воздействий, таких, как повышенная влажность, и уменьшает суммарную стоимость за счет отсутствия необходимости монтирования кристалла.

M41ST87 «NVRAM SUPERVISOR» может быть подключена к энергонезависимой статической памяти малого потребления, и для этого в ее функции входят автоматическое включение-выключение батареи, шлюз Chip Enable для осуществления защиты записи, а также мониторинг батареи.

В сердце микросхемы находятся программируемые, с возможностью питания от батареи, часы реального времени, содержащие счетчики, которые считают время с разрешением от сотых долей секунд до веков. Часы реального времени доступны по интерфейсу I^2C, работающему с частотой 400 кГц. Построенные по технологии низковольтной статической КМОП-памяти, часы реального времени организованы 256 линейками по 8 бит, из которых 21 байт используется для регистров часов реального времени, 128 байт — для энергонезависимой памяти и 8 байт — для уникального серийного номера.

Минипроцессор, встроенный в M41ST87, содержит два независимых компаратора — по входу (PFI — Power Fail In) и по выходу (PFO — Power Fail Out) с точностью 1,25 В, а также мощный контур сброса, который управляется несколькими источниками, которые имеют два входа Reset и сброс по включению (Power-On-Reset) и определение низкого напряжения (Low Voltage Detect). Сторожевой таймер (Watchdog) программируется на временные интервалы от 62,5 мс до 128 с, а также может быть запрограммирован как источник сброса. Контур «определения фальшивки» также может быть сконфигурирован как источник сброса. Более того, при использовании в качестве преждевременного сигнализатора тревоги, контуры PFI и PFO могут также быть использованы в качестве управляющих для контура сброса, что позволяет M41ST87 контролировать до трех различных питающих источников (включая Vcc).

Приведем краткую сводку технических характеристик описываемого устройства:

1. Последовательные часы реального времени с интерфейсом I²C.
2. Минипроцессор.
3. Небольшая NVRAM.
4. Контур «обнаружения фальшивки» с режимом стирания памяти.

Контур «обнаружения фальшивки» выполняет следующие функции:

1. Два независимых контура обнаружения.
2. Выработка сигнала прерывания.
3. Очистка внутренней памяти.
4. Очистка внешней памяти.
5. Сохранение времени события.
6. Выработка сигнала RESET.

Последовательные часы реального времени:

1. Счетчики на 10/100 доли секунды, минуты, часы, дни, даты, месяцы, годы, века.
2. 128 байт энергонезависимой памяти.
3. Программируемые режимы «повтор» и «тревога»; даже при питании от батареи.

Минипроцессор включает в себя:

1. Программируемый сторожевой таймер с периодом от 62,5 мс до 128 с.
2. Сброс по включению и детектор низкого напряжения.
3. Два входа RESET.

Области применения для высокоинтегрированного, недорогого и компактного M41ST87 включают в себя кассовые аппараты, ридеры для кредитных карт, автоответчики, сетевое и телекоммуникационное оборудование, а также любое другое приложение, где требуется шифрование информации.

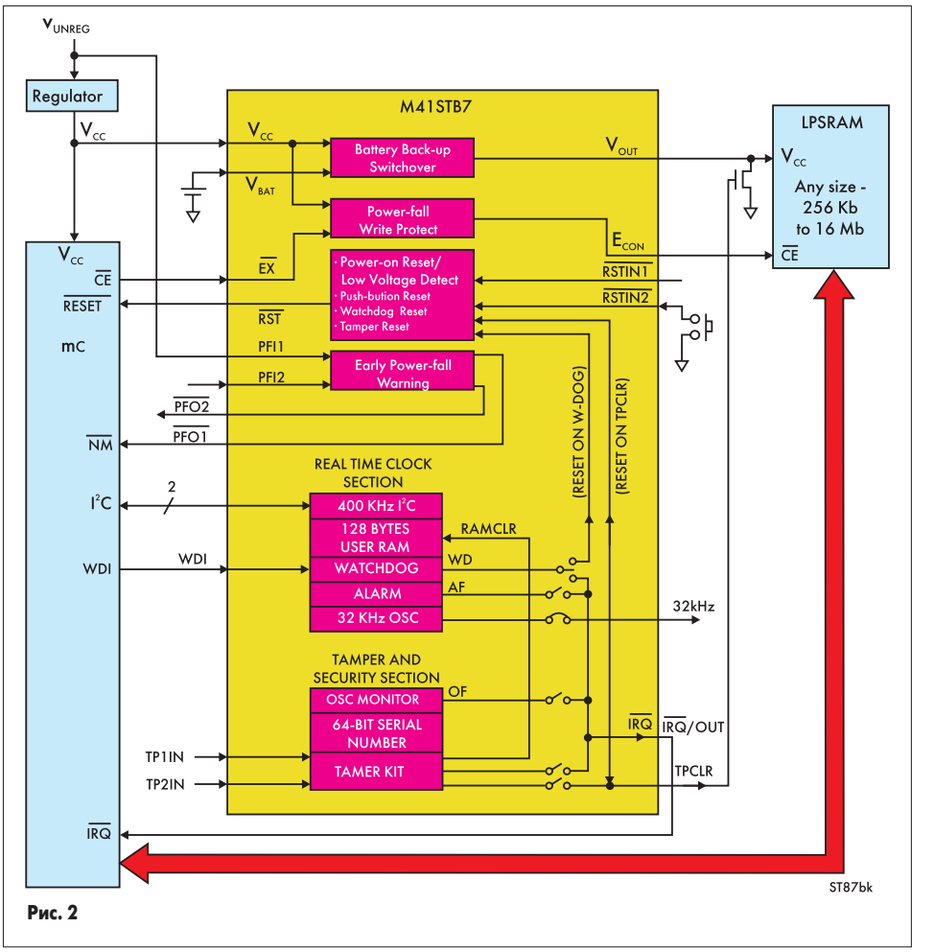

Рис. 2

Новый корпус SOX28 — размерами всего 2,4 мм в высоту, 10,42 мм в ширину и 18,4 мм в длину — вместе с этим высокая интеграция микросхемы позволяет существенно уменьшить занимаемое пространство и снизить цену конечного устройства. Микросхема M41ST87 может работать в промышленном диапазоне температур (от –40 до +85 °C). Образцы уже доступны, а серийный выпуск продукции начинается в третьем квартале 2003 года. Более подробную информацию по этому устройству можно найти на сайте **w ww .st.c om/nvram**.