УДК 004.415.2

А.В. Осинцев, М.Е. Комнатнов

Метод выявления и исправления ошибок данных в памяти микроконтроллера на основе аппаратного подсчета контрольной суммы

Разработан метод выявления ошибок в памяти микроконтроллера (МК), необходимый при исследованиях и испытаниях на помехоустойчивость МК. В основу метода заложена работа аппаратного блока хеш-функции для подсчета контрольной суммы (КС) полезных данных. На основе метода предложен способ исправления ошибочных битов памяти различных вычислительных устройств. Способ включает алгоритм детектирования и исправления ошибок, позволяющий восстанавливать данные в памяти посредством вычисления их КС с организацией хранения данных в виде структуры. Предложенный метод позволяет распознать, в каком объекте произошла ошибка, и восстановить ошибочные биты памяти. Реализация алгоритма проверки данных в виде системного процесса операционной системы реального времени позволила автоматизировать процесс поиска ошибок в фоновом режиме и определить причину возникновения сбоя. Программная реализация метода детектирования и исправления ошибок, без изменений аппаратной части, может быть применена при эксплуатации радиоэлектронных средств в сложных условиях, содержащих любое вычислительное устройство.
Ключевые слова: ЭМС, РЭС, микроконтроллер, битовая ошибка, хеш-сумма, контрольная сумма.
DOI: 10.21293/1818-0442-2021-25-1-70-78

Современные микроконтроллеры (МК) содержат различные виды памяти, например такие, как постоянное запоминающее устройство (ПЗУ), оперативное запоминающее устройство (ОЗУ) и пр. [1]. Воздействие внешних электромагнитных помех может привести к изменению данных, которые содержат эти устройства. Так, повышенная восприимчивость к электромагнитным помехам может привести к неконтролируемому переключению транзисторов в регистрах памяти [2, 3]. Вследствие этого возникают битовые ошибки, которые следует выявлять и своевременно устранять для стабильной работы радиоэлектронного средства (РЭС). Для выявления и исправления ошибок в памяти применяют аппаратные [4–8] и программные средства, основанные на битах четности, специализированных кодах исправления ошибок [9, 10], а также различных модификациях классических алгоритмов кода Грея, Рида–Соломона [11], Хэмминга, турбокодов [12–14] и пр. Последние необходимы для распознавания и исправления битовой ошибки в двух и более битах данных памяти. Однако классические алгоритмы неполностью справляются с коррекцией ошибок и не способны определить адрес памяти, в которой произошёл сбой [15]. Кроме того, они представляют собой ресурсоемкие алгоритмы, что сказывается на производительности и скорости отклика РЭС в целом. Современные МК обладают большим объемом ОЗУ и ПЗУ. В случае физического разрушения логических элементов (вентилей транзистора) невозможно локализовать поврежденную страницу в памяти, используя классические алгоритмы. Тем самым в случае выявления ошибки невозможно определить, какие данные можно использовать, а какие повреждены. Таким образом, существует потребность в новых методах диагностики памяти МК, способных эффективно найти и исправить ошибки.

В настоящее время при проверке целостности данных часто используют контрольную сумму (КС). Это делают по нескольким причинам. Во-первых, простота реализации алгоритма проверки КС не требует использования сложных и затратных вычислительных алгоритмов [16, 17], а также специализированных внешних библиотек. Во-вторых, многие МК имеют аппаратный блок подсчёта КС (SHA, CRC, MD5 и др.), что позволяет снизить объем программного кода и получить результат за 1–3 системных такта (в зависимости от объема памяти, метода вычисления КС и аппаратных возможностей МК). В-третьих, в большинстве современных МК реализован аппаратный блок прямого доступа к памяти (ПДП), что позволяет обращаться к данным в памяти в обход ядра МК, повышая скорость обработки и проверки данных на наличие ошибок и снижая расходы вычислительных ресурсов МК. Использование КС при проверке данных в памяти обладает рядом преимуществ, позволяющих локализовать область памяти, содержащей ошибки, и исправить их. Таким образом, целесообразна разработка новых методов, позволяющих на основе КС выявлять и исправлять ошибки в памяти при эксплуатации МК в сложных условиях, в том числе при внешних климатических и электромагнитных воздействиях.

Цель работы – разработать метод выявления и исправления ошибок памяти МК на основе аппаратного подсчета КС для надежного их хранения.

Проверка состояния регистров МК

С целью обеспечения покрытия тестами большинства блоков МК и выявления наиболее уязвимых и восприимчивых к внешнему воздействию блоков МК, которые могут быть подвержены ошибкам, а также для определения источника или причины их возникновения разработан комплекс тестовых задач. Выбранные для тестирования блоки МК

используются в большинстве современных РЭС (табл. 1).

Таблица 1

Тестируемые блоки МК и описание тестовых задач

Блок МК	Описание тестовой задачи
АЛУ	Циклическое выполнение арифметических операций
Область памяти (ПЗУ, ОЗУ, ЭСППЗУ)	1. Выполнение операций записи в память с последующим чтением и проверкой записанных данных. 2. Выполнение подсчета КС данных во всей области памяти
Таймеры	1. Выполнение прямого и обратного счета таймерами. 2. Работа таймеров в режиме ШИМ. 3. Работа таймеров с использованием прерываний. 4. Использование системного таймера SysTick для выполнения задач с определенной периодичностью
Интерфейсы передачи данных	1. Прием и передача данных по интерфейсу UART с проверкой данных посредством вычисления КС. 2. Прием и передача данных по интерфейсу I^2C с проверкой данных посредством вычисления КС
АЦП	Проверка корректности функционирования АЦП посредством чтения аналогового сигнала регулярных и инжекторных каналов.
ЦАП	Генерация аналогового сигнала и его проверка на корректность
ПДП	Использование инструментов прямого доступа к памяти для организации передачи данных по UART, SPI, I^2C и др. в обход центрального процессора или АЛУ МК
Порты ввода-вывода	Изменение состояний выводов МК по набору заранее сформированных тестовых масок для 8-, 16-, 32-битных портов. Контроль соответствия заданному состоянию регистров тестируемого порта ввода-вывода МК. Циклическое выполнение битовых операций над числами: сдвиг вправо, сдвиг влево, чтение и запись бита
Прерывания	Контроль выполнения прерываний в блоках МК, а также мониторинг выполнения соответствующих функций прерывания

Признаком нарушения работы МК являются неконтролируемые и непредвиденные изменения в процессе тестирования. В процессе работы отслеживаются следующие параметры: время выполнения кода; амплитуда воздействующей электромагнитной помехи; состояние выводов общего назначения (GPIO); работа сторожевого таймера (DWT, контроль зависания ядра МК); частота тактирования ядра МК, КС всей памяти и отдельно каждого в ней объекта. Полученные данные во многом зависят от задействованных библиотек, версии компилятора, а также использования ключей оптимизации кода, операций с плавающей точкой и работы блока ПДП.

Измерительная печатная плата (ПП), соответствующая нормативным документам [18, 19] по измерению излучаемых эмиссий и устойчивости к излучению интегральной схемы в ТЕМ-камере, представлена на рис. 1.

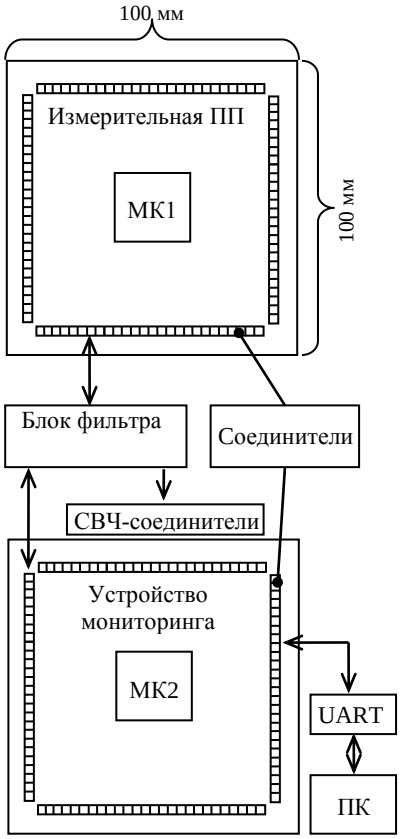

Рис. 1. Схема соединения устройства мониторинга и измерительной ПП

На одной стороне ПП находится измеряемый МК, а все необходимые компоненты, включая различные соединители для питания и программатора, расположены на обратной стороне ПП.

Необходимые компоненты для контроля параметров МК1 располагаются на устройстве мониторинга, которое содержит МК2 для контроля работы алгоритмов и записи данных с результатами тестов. Измерение состоит из 3 этапов:

1. Мониторинг параметров выполнения тестовых задач, задействующих исследуемые блоки МК, без внешнего воздействия. Это необходимо, чтобы получить эталонные значения параметров, по которым будет выполняться сравнение (до и после воздействия на МК).

2. Выполнение тестовых задач с внешними климатическим и электромагнитным воздействиями. Оно осуществляется МК2, расположенным на устройстве мониторинга. Он в режиме реального времени фиксирует состояние исследуемого МК1, расположенного на измерительной ПП. Фиксация состояний происходит посредством соответствующего интерфейса передачи данных. Принятые МК2 данные передаются на ПК для обработки и анализа результатов.

3. Процесс обработки полученных данных. Сравниваются результаты работы тестовых блоков МК первого и второго этапов. Фиксируются отклонения в результате климатического и электромагнитного воздействий на исследуемый МК1.

Метод выявления и исправления ошибок в энергонезависимой памяти МК

Предложенный метод заключается в проверке корректности данных в ПЗУ МК с использованием КС объектов в ПЗУ, одним из доступных способов для вычислительной системы целевого устройства. Метод использует следующие данные: полезные данные; КС ПЗУ МК; КС данных; объект структуры; резервная копия объекта структуры; служебная структура/дескриптор. Поясним каждый вид.

К *полезным данным* относится информация, которая длительное время хранится в ПЗУ и используется в процессе работы РЭС, например, калибровочные коэффициенты; параметры режима работы; результаты работы РЭС; диагностическая информация и т.д.

КС данных вычисляется одним из аппаратных блоков МК для вычисления КС (SHA, CRC, MD5 и др.).

Объект структуры является составным типом данных (рис. 2), предназначенным для хранения полезных данных и их КС в полях структуры.

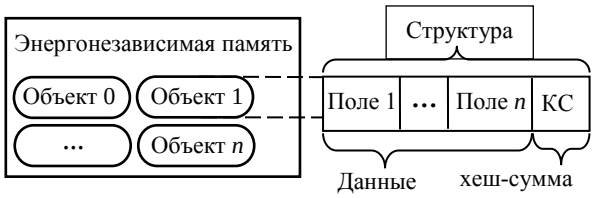

Рис. 2. Хранение объекта структуры с данными в энергонезависимой памяти

Резервная копия объекта структуры представляет собой копию исходной структуры, служащую для восстановления данных в случае повреждения информации в ПЗУ.

КС ПЗУ МК вычисляется одним из аппаратных блоков МК для вычисления хеш-суммы всей информации, находящейся в ПЗУ МК, после окончания формирования всех объектов структур и подсчета их КС. КС энергонезависимой памяти МК обновляется каждый раз при выполнении операции записи в память либо при изменении данных в ПЗУ. Она находится в поле служебной структуры и является эталоном (контрольным значением) в процессе сравнения с вычисленной КС ПЗУ.

Служебная структура содержит информацию обо всех объектах структур с данными: название структуры; адрес в памяти; количество выявленных ошибок; количество успешных восстановлений; количество исправленных битов; количество выполненных циклов чтения/записи. При каждом изменении данных в ПЗУ информация в служебной структуре обновляется. Таким образом, она содержит актуальную информацию об изменениях и состоянии данных в ПЗУ.

Предложенный метод предусматривает различные варианты реализации в зависимости от решаемой задачи, что влияет на организацию связей между данными, представленными выше. В общем виде метод состоит из этапов, представленных в обобщенном алгоритме на рис. 3.

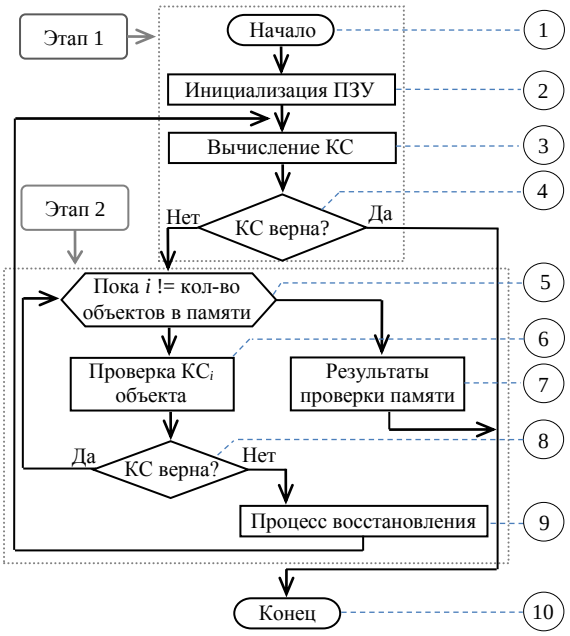

Рис. 3. Обобщенный алгоритм выявления и исправления ошибок данных в ПЗУ

В основу алгоритма проверки памяти заложен метод избыточного кодирования для вычисления КС. Данный способ кодирования отличается простотой реализации за счет наличия блоков в МК и обладает гибкостью расчета (длины результата) при выборе конечной архитектуры расчёта КС с возможным применением для МК с 8-, 16-, 32- и 64-битной вычислительной архитектурой. Обобщенный алгоритм поиска и исправления ошибок в ПЗУ представлен на рис. 3. Работа алгоритма состоит из двух этапов.

На этапе 1 выполняется вычисление текущей КС ПЗУ и её сравнение с эталонным значением КС энергонезависимой памяти МК, находящейся в служебной структуре. Если оба значения КС идентичны, проверка заканчивается. В противном случае алгоритм переходит ко второму этапу проверки данных в ПЗУ.

Этап 2 заключается в поиске ошибок КС в объектах структур, находящихся в ПЗУ и их резервных копиях. Информация о них берется из служебной структуры.

Проверка блоков памяти выполняется посредством подсчета КС каждого объекта памяти (рис. 2). При достижении последнего блока значение КС сравнивается с эталонным. Если вычисленное и эталонное значения КС различаются, запускается процесс восстановления памяти. Возможен вариант, при котором КС всей памяти будет отличаться от эталонной, но ни в одном объекте не будут найдены

ошибки. Это означает, что изменения коснулись свободных ячеек памяти, которые в данный момент не используются.

Процесс проверки данных в ПЗУ в случае аппаратного либо программного сбоя в результате воздействия ЭМП состоит из 5 этапов, реализованных в обобщенном алгоритме:

1. Формирование объектов структур данных, включая запись их КС в служебное поле структуры.

2. Подсчет КС всего ПЗУ и выполнение циклической проверки КС.

3. Выявление ошибки КС всего ПЗУ и проверка всех объектов с целью локализации адреса объекта в ПЗУ, в котором возник сбой.

4. Восстановление данных поврежденного объекта из резервной копии посредством исправления битов ПЗУ, содержащих ошибку.

5. Повторная проверка КС всего ПЗУ с целью подтверждения исправления ошибок.

Поля структуры содержат данные, а их КС находится в служебном поле структуры. Затем выполняется дублирование созданной структуры (резервная копия), которая используется в случае повреждения данных. После того, как все данные помещены в структуры и созданы резервные копии, вычисляется КС всей энергонезависимой памяти, она хранится в служебной структуре либо дескрипторе вместе с информацией о количестве структур и их физических адресах в памяти. КС всей памяти – это эталонное значение, с которым будет сравниваться вычисленное значение КС памяти в процессе проверки. Оно позволит достаточно быстро определить наличие ошибок памяти, поскольку в случае изменения хотя бы одного бита тестируемой памяти гарантированно изменится и КС.

В случае несовпадения вычисленной КС с известным эталонным значением КС, полученным на этапе изменения данных в памяти, вызывается процесс проверки КС данных, хранящихся в структурах. В случае обнаружения несовпадения КС в одной или более структур выполняется сверка КС данных со значением, записанным в поле структуры, а также со значением КС резервной копии (данных и КС в служебном поле структуры). В результате этот объект имеет корректную КС данных, и она совпадает со значением КС в служебном поле структуры, эти данные считаются корректными и используются в качестве маски для сверки битов в памяти поврежденной структуры. Отличающиеся биты в поврежденной структуре будут изменены. Затем выполняется повторное вычисление КС всей памяти. В том случае, если ошибка была только в одной структуре, вычисленная КС совпадет с эталонным значением КС в служебной структуре/дескрипторе.

При формировании полей структуры рекомендуется использовать выравнивание данных для экономии памяти. Структуры могут хранить данные различного объема. При этом рекомендуется ограничить максимальный размер структуры 10% памяти для оптимизации процесса вычисления КС и снижения вероятности появления большого количества ошибок в одной структуре. Обобщенный алгоритм может применяться как для распознавания, так и для исправления ошибок памяти.

Реализация метода без возможности восстановления данных

Информация хранится в памяти, используя объекты в виде структуры (рис. 4). Поля структуры могут содержать информацию различного типа. В одном из полей структуры может находиться вычисленный результат КС данных. Тем самым обеспечивается возможность проверки данных в структуре и сравнение с полем, в котором находится «эталонный» результат, который вычисляется каждый раз при записи данных в структуру.

```
struct_eeprom_data{
        float param_1;
        float param_2;
        int param_3;
        char name_object1[44];
        char name_object2[45];
        char name_object3[45];
        uint16_treg = 0;
        uint32_tcrc = 0;
};
```

Рис. 4. Структура для хранения тестовых данных

В память записывается информация в виде структуры, которая содержит поля для данных и поле для хранения КС. Оно будет гарантировать целостность данных в случае сбоя или неконтролируемого сброса системы. В процессе запуска устройства вычисляется КС всей памяти. В случае, когда текущее вычисленное значение КС отличается от ранее вычисленного, регистрируется сбой в памяти и выполняется проверка всех данных, находящихся в энергонезависимой памяти МК. Если данные во всех структурах совпадут с соответствующими КС, то это означает, что сбой в памяти не повредил данные, а изменения коснулись адресов свободной памяти. Если ячейка памяти не повреждена (физически), то данный вид ошибок поддается восстановлению путем сброса всех разрядов неиспользуемой памяти. В результате данной операции повторный подсчет КС всей памяти будет совпадать с вычисленным ранее значением. В случае повреждения ячейки памяти требуется исключить операции с поврежденным блоком памяти, пометив данный блок в «карте памяти» ОСРВ и обновив данные КС.

Способ реализации метода с возможностью восстановления данных

На рис. 5 представлено программное разделение ПЗУ на 2 раздела и расположение в нем исходных структур с данными (S_1, S_2, S_3) и их резервных копий (CS_1, CS_2, CS_3). В каждом разделе имеется свой дескриптор сегмента (*DS*), он выполняет функцию *служебной структуры*, содержащей информацию о количестве сегментов памяти, количестве структур, их адреса и КС. Благодаря использованию зеркалирования данных (двусторонняя синхронизация данных в памяти МК) предоставляется возмож-

ность восстановить информацию в том случае, если повреждения не затронули области памяти резервного и резервируемого разделов памяти. В таком случае анализируется информация *DS* каждого раздела и сравнивается с данными их структур. Объекты, у которых вычисленная КС не совпадает с данными в поле КС структуры объекта, инвертируются (биты, в которых выявлены несоответствия). Таким образом, сохраняется ресурс чтения/записи в ячейки памяти (он имеет ограниченное количество циклов чтения/записи).

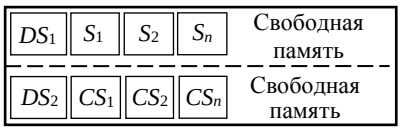

Рис. 5. Дублирование данных в общей памяти

В табл. 2 представлены все комбинации возможных вариантов ошибок в памяти с использованием зеркалирования данных. Например, вариант 1 сообщает о повреждениях, затронувших «Данные объекта *n*» (*A*). Вариант 2 сообщает о повреждениях, затронувших «Данные объекта» (*A*) и «CRC объекта» (*B*) и т.д., аналогичным образом представлены все остальные варианты ошибок. Среди них следует выделить критические комбинации вариантов ошибок, при которых отсутствует возможность восстановления данных, к ним относятся ошибки, возникшие в трех и более областях памяти (данные объекта (*A*), CRC объекта (*B*), копия данных объекта (*C*), CRC копии данных объекта (*D*)), что не исключает повреждения данных в другом блоке памяти. Для проверки целостности всей памяти предлагается снимать дамп («слепок») всей памяти и хранить результат в отдельной структуре. Данный способ проверки позволяет выполнить проверку всех данных в памяти, значительно сократив время проверки в сравнении с проверкой группы отдельных наборов данных. Серьезным недостатком способа является необходимость пересчета КС при изменении данных в каком-либо блоке памяти.

Таблица 2

Комбинации вариантов выявления ошибок в памяти

Ошибка	*A*	*B*	*C*	*D*
A	1	2	3	4
B	–	6	7	8
C	–	–	11	12
D	–	–	–	16

Способ реализации метода в составе операционной системы реального времени

Возможности различных вычислительных модулей в настоящее время позволяют запускать программный код под управлением ОСРВ, что в значительной степени упрощает процесс разработки конечного устройства. ОСРВ способна контролировать все служебные процессы и пользовательские задачи, регистрировать ошибки, используя режим псевдомногозадачности. Системная «Служба диагностики» с инструментами восстановления данных совместно с «Менеджером памяти» может контролировать целостность памяти, выполняя проверку памяти в фоновом режиме. Большинство ОСРВ распространяются в открытом доступе, предоставляя возможность внедрения стороннего кода в состав ОСРВ. Таким образом, использование в ОСРВ предложенного способа диагностики и восстановления памяти позволит автоматизировать процесс. Посредством аппаратного блока ПДП менеджер памяти может обращаться к данным в памяти в обход центрального процессора вычислительного устройства, что позволит избежать дополнительной нагрузки за счет периодического обращения к памяти ОСРВ.

Процесс контроля состояния и целостности объектов в памяти выполняет служба ОСРВ «Менеджер памяти» (рис. 6). Виртуальный дескриптор выполняет контроль за доступом к объектам в памяти.

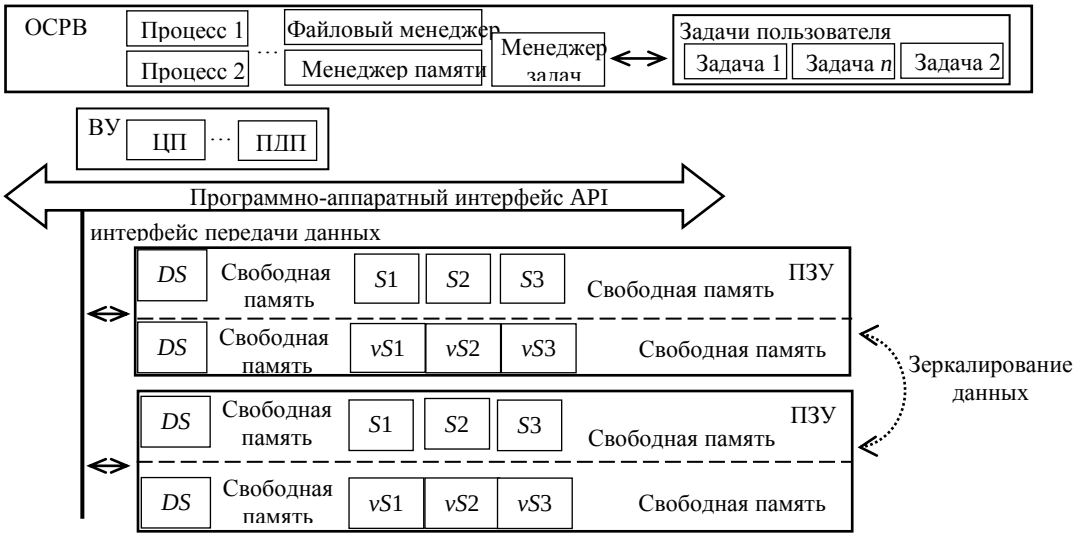

Рис. 6. Организация контроля целостности памяти средствами «Менеджера памяти» ОСРВ

Таким образом, исключается проблема множественного доступа к данным в памяти. Менеджер памяти предоставляет доступ к памяти активным процессам и содержит информацию о количестве

объектов в памяти, их адресах и КС всей памяти. В случае сброса ОСРВ проверяет целостность данных посредством службы «Менеджера памяти», функционирующего в фоновом режиме.

Тестирование алгоритма и апробация метода мониторинга и восстановления данных в памяти

Разработан программный код и выполнено тестирование разработанного метода выявления и исправления ошибок в энергонезависимой памяти МК. Работа тестовой программы выполнялась на МК ATMega2560 в соответствии с алгоритмом, представленным на рис. 3. На рис. 7 представлена структура данных, используемая в тестовой программе. Для хранения тестовых данных в структуре eeprom_data предусмотрены поля: param_1, param_2, param_3, name_object1, name_object2 и name_object3.

```
struct eeprom_data{
        float param_1 = 1.1984;
        float param_2 = 2.451;
        int param_3 = 8035;
        char name_object1[44];
        char name_object2[45];
        char name_object3[45];
        uint16_t reg = 0;
        uint32 t crc = 0;
};
```

Рис. 7. Структура для хранения тестовых данных

Результат работы тестовой программы представлен в табл. 3. Необходимо отметить, что в МК ATmega2560 отсутствует аппаратный блок вычисления КС. Для расчета КС использовался метод циклического избыточного кода.

Таблица 3

Результаты работы программы выявления ошибок в ПЗУ

Сообщения тестовой программы	Описание этапа работы
Clear EEPROM (CRC): 7DCF4209 CRC Obj1 = FB41D96C CRC Obj2 = 236B8F9B CRC Obj3 = 2365DD94	Шаг 1. Вычисление КС методом циклического избыточного кода (CRC) всей ЭСППЗУ МК и трёх структур с тестовыми данными
After write three structures to EEPROM (CRC): CB227FA0 11111111	Шаг 2. Вычисление КС всей памяти ЭСППЗУ после записи в неё трёх структур. Выводится случайно выбранная ячейка памяти из диапазона адресов, в которых расположены тестовые структуры данных
Error entered in byte #190 | bit #7 | New state bit #0 01111111	Шаг 3. В выбранную случайным образом ячейку памяти №190 вносится ошибка в бит 7
ERROR CRC EEPROM! ERROR EEPROM CRC IN OBJECT # 1	Шаг 4. Алгоритм распознал изменение КС данных в памяти и выявил ошибку в КС объекта 1
EEPROM (CRC): 7DCF4209 CRC Obj1 = FB41D96C CRC Obj2 = 236B8F9B CRC Obj3 = 2365DD94	Шаг 5. Восстановление ошибочного бита объекта 1, в котором была выявлена ошибка. После успешного восстановления отображается информация с КС всей памяти и объектов, хранящихся в ней

Поле «reg» предназначено для хранения состояния регистра порта общего назначения. Данная задача представлена ранее в табл. 1, в которой приведены тестовые задачи. Поле «crc» предназначено для хранения КС данных в структуре.

В отечественных МК 1986ВЕ9х имеется блок батарейного домена, в котором доступны 14 32-разрядных регистров, в которых рекомендуется хранить долговременные данные. Функция записи данных в регистрах батарейного домена представлена на рис. 8.

```
void SaveStruct (void) {
    eeprom_data object1, object2, object3;
    BKP_RTC_WaitForUpdate ();
    MDR_BKP->REG_02 = object1;
    MDR_BKP->REG_03 = object2;
    MDR_BKP->REG_04 = object3;
}
```

Рис. 8. Функция записи данных в регистры батарейного домена МК 1986ВЕ91Т

В основе отечественных МК серии 1986ВЕ9х используется ядро ARM Cortex-M3. В качестве ближайшего аналога отечественного МК в технической документации указан МК STM32F103. Данный МК обладает тем же ядром Cortex-M3, в котором реализован аппаратный блок CRC для подсчета КС. Таким образом, представленный метод выявления и исправления ошибок в памяти МК может применяться как в отечественных, так и зарубежных МК.

Заключение

Представленный метод выявления и исправления ошибок в памяти МК может применяться как в отечественных, так и зарубежных МК и не требует использования дополнительных аппаратных компонентов. Также метод позволяет локализовать область повреждения данных в памяти и восстановить их в том случае, если ИС памяти не была повреждена. В противном случае поврежденные страницы памяти помечаются как неиспользуемые, затем резервные данные переносятся в свободные страницы памяти.

Предлагаемые метод и алгоритмы диагностики данных в памяти МК позволяют эффективно восстановить данные в случае появления множества битовых ошибок как во внешней, при использовании дополнительной микросхемы памяти, так и во внутренней памяти МК.

Таким образом, использование предложенного метода позволяет эффективно выявлять и исправлять ошибки в памяти при эксплуатации МК в сложных условиях, в т.ч. при внешних климатиче-

ских и электромагнитных воздействиях. Предложенный метод обладает рядом преимуществ по сравнению с аналогами:

1. В процессе работы используется аппаратный блок подсчёта, что позволяет снизить объем программного кода и получить результат за 1–3 системных такта, в зависимости от объема памяти, метода вычисления КС и аппаратных возможностей МК.

2. Реализация метода не требует использования сложных и затратных вычислительных функций, а также специализированных внешних библиотек.

3. Использование инструментов МК для организации прямого доступа к памяти позволяет обращаться к данным в памяти, минуя ядро МК, что позволяет повысить скорость проверки данных на наличие ошибок, снизив расходы вычислительных ресурсов МК.

4. Возможно выявлять и локализовать область памяти, содержащую ошибки, и исправить их посредством зеркалирования.

5. Использование зеркалирования данных позволяет сохранить данные в случае физического повреждения ИС памяти.

Внедрение предложенного метода восстановления контекста рабочего процесса МК средствами ОСРВ позволит повысить надежность и отказоустойчивость разрабатываемых устройств, содержащих МК, а также сократить время поиска неисправности в МК.

Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации по проекту РНФ 19-79-10162.

Литература

1. Воздействие импульсных электромагнитных полей на микросхемы АЦП и ЦАП / Е.В. Григорьев, В.В. Старостенко, Е.П. Таран, Д.А. Унжаков // Радиоэлектроника и информатика. – 2007. – № 4. – С. 22–24.

2. Воздействие импульсных электромагнитных полей на интегральные микросхемы памяти / Л.Н. Ахрамович, М.П. Грибский, Е.В. Григорьев, С.А. Зуев, В.В. Старостенко, Г.И. Чурюмов // Радиоэлектроника и информатика. – 2006. – № 4. – С. 15–17.

3. Яньков А.И. Методы обеспечения сбоеустойчивости к одиночным событиям в процессе проектирования для микропроцессоров К1830ВЕ32УМ и 1830ВЕ32У / А.И. Яньков, В.А. Смерек, В.П. Крюков, В.К. Зольников // Моделирование систем и процессов. – 2012. – № 1. – С. 92–95.

4. FlashSim: A Simulator for NAND Flash-based Solid-State Drives / Y. Kim, B. Tauras, A. Gupta, B. Urgaonkar // In Proceedings of the First International Conference on Advances in System Simulation, Porto, Portugal, 20–25 September. – 2009. – P. 125–131.

5. Yang J. Novel ECC architecture enhances storage system reliability. In Proceedings of the Flash Memory Summit, Santa Clara, CA, USA, 22–24 August 2012. – P. 1–15.

6. Tanakamaru S. Over-10x-extended-lifetime 76%-reduced-error solid-state drives (SSDs) with error-prediction LDPC architecture and error-recovery scheme / S. Tanakamaru, Y. Yanagihara, K. Takeuchi // In Proceedings of the IEEE International Solid-State Circuits Conference (ISSCC), San Francisco, CA, USA, 19–23 February 2012. – P. 424–426.

7. Park D. Safe microcontrollers with error protection encoder-decoder using bit-inversion techniques for on-chip flash integrity verification / D. Park, T.G. Kim // In Proceedings of the 2013 IEEE 2nd Global Conference on Consumer Electronics (GCCE), Tokyo, Japan, 1–4 October. – 2013. – P. 299–300.

8. Park J. VL-ECC: Variable Data-Length Error Correction Code for Embedded Memory in DSP Applications / J. Park, S. Bhunia // IEEE Transactions on Circuits and Systems II: Express Briefs. – 2014. – Vol. 61, No. 2. – P. 120–124.

9. Газарян Ю.О. Об экспериментальной оценке стойкости метода случайного кодирования к атаке многократного наблюдения частичных кодовых векторов / Ю.О. Газарян, Ю.В. Косолапов // Вычислительные технологии. – 2015. – Т. 20, № 6. – С. 5–21.

10. Методы обеспечения стойкости микросхем к одиночным событиям при проектировании радиационностойких микросхем / В.Н. Ачкасов, В.А. Смерек, Д.М. Уткин, В.К. Зольников // Проблемы разработки перспективных микро- и наноэлектронных систем // Сборник трудов / под общ. ред. А.Л. Стемпковского. – М.: ИППМ РАН, 2012. – С. 634–637.

11. Федоров С.В. Реализация потокового декодера укороченных кодов Рида–Соломона на ПЛИС / С.В. Федоров, В.И. Ромашкин, К.М. Вялых // Машиностроение и компьютерные технологии. – 2016. – № 6. – С. 184–199.

12. Subhasri G. VLSI design of Parity check Code with Hamming Code for Error Detection and Correction / G. Subhasri, N. Radha // Proceedings of the 2019 International Conference on Intelligent Computing and Control Systems (ICCS), Madurai, India, 15–17 May. – 2019. – P. 15–20.

13. Назаров Л.Е. Характеристики помехоустойчивых укороченных блоковых турбокодов итеративного приема информации / Л.В. Назаров, П.В. Шишкин // Радиоэлектроника. Наносистемы. Информационные технологии. – 2018. – Т. 10, № 2. – С. 323–328.

14. Осокин А.Н. Реализация турбокодека на программируемой логической интегральной схеме / А.Н. Осокин, А.В. Ярёменко // Векторы благополучия: экономика и социум. – 2011. – № 1 (1). – С. 382–387.

15. Теоретические основы цифровой радиосвязи: учеб. пособие / Н.И. Листопад, В.М. Козел, В.В. Дубровский, К.Л. Горбачев, К.А. Ковалев. – Минск: БГУИР, 2012. – 330 с.

16. Kim J. Low-Power Command Protection Using SHA-CRC Inversion-Based Scrambling Technique for CAN-Integrated Automotive Controllers / J. Kim, J. Cho, D. Park // In Proceedings of the 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan. 10–13 December. – 2018. – P. 1–2.

17. Cho S. Robust Intra-Body Communication Using SHA1-CRC Inversion-Based Protection and Error Correction for Securing Electronic Authentication / S. Cho, D. Park // MDPI Sensors. – 2020. – P. 1–17.

18. IEC 62132-4–2006. Integrated circuits – Measurement of electromagnetic immunity 150 kHz to 1 GHz. – Part 4. Direct RF power injection method, 2006. – URL: https://webstore.iec.ch/publication/6510 (дата обращения: 05.03.2022).

19. Integrated Circuits. Measurement of Electromagnetic Emissions. Part 2: Measurement of Radiated Emissions, TEM Cell and Wideband TEM Cell Method, IEC 61967-2, First Edition, 2005. – URL: https://webstore.iec.ch/publication/6185 (дата обращения: 05.03.2022).

Осинцев Артем Викторович
Ассистент каф. телевидения и управления (ТУ)
Томского государственного ун-та систем управления
и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0003-0888-6793
Тел.: +7-952-755-01-23
Эл. почта: kubenet@gmail.com

Комнатнов Максим Евгеньевич
Канд. техн. наук, с.н.с., доцент каф. ТУ ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
ORCID: 0000-0002-6463-2889
Тел.: +7-952-888-38-96
Эл. почта: maxmek@mail.ru

Osintsev A.V., Komnatnov M.E.

A method for detecting and correcting errors in memory circuits based on the calculation of the hash sum Method to detect and correct errors in memory circuits based on the calculation of the hash sum

A method has been developed for detecting errors in the memory of a microcontroller (MC), which is necessary for research and testing for noise immunity of the MC. The method is based on the operation of the hash function hardware unit for calculating the checksum (CS) of useful data. Based on the method, an approach is proposed for correcting erroneous bits in the memory of various computing devices. The method includes an algorithm for detecting and correcting errors, which allows to restore data in memory by calculating their CS with the organization of data storage in the form of a structure. The proposed method enables helps to recognize the object where an error occurred and to recover the erroneous memory bits. The implementation of the data verification algorithm as a system process of the real-time operating system made it possible to automate the process of searching for errors in the background and determine the cause of the failure. The software implementation of the error detection and correction method, without changing the hardware, can be used in the operation of radioelectronic equipment in difficult conditions containing any computing device.

Keywords: EMC, radioelectronic equipment, microcontroller, bit error, hash, checksum.
DOI: 10.21293/1818-0442-2021-25-1-70-78

References

1. Grigoriev E.V. Starostenko V.V., Taran E.P., Unzhakov D.A. *Vozdeystviye impul'snykh elektromagnitnykh poley na mikroskhemy ATSP i TSAP* [Influence of pulsed electromagnetic fields on ADC and DAC microcircuits]. *Radioelectronics and Informatics*, 2007, no. 4, pp. 22–24 (in Russ.).

2. Akhramovich L.N, Gribsky M.P., Grigoriev E.V., Zuev S.A., Starostenko V.V., Churyumov G.I. *Vozdeystviye impul'snykh elektromagnitnykh poley na integral'nyye mikroskhemy pamyati* [Impact of pulsed electromagnetic fields on integrated memory circuits]. *Radioelectronics and Informatics*, 2006, no. 4. pp. 15–17 (in Russ.).

3. Yankov A.I. Smerek V.A., Kryukov V.P., Zolnikov V.K. *Metody obespecheniya sboyeustoychivosti k odinochnym sobytiyam v protsesse proyektirovaniya dlya mikroprotsessorov K1830BE32UM i 1830VE32U* [Methods for ensuring fault tolerance to single events in the design process for microprocessors K1830BE32UM and 1830BE32U]. *Modeling of Systems and Processes*, 2012, no. 1. pp. 92–95 (in Russ.).

4. Kim Y., Tauras B., Gupta A. Urgaonkar B. FlashSim: A Simulator for NAND Flash-based Solid-State Drives. *In Proceedings of the First International Conference on Advances in System Simulation*, Porto, Portugal, 20–25 September. 2009, pp. 125–131.

5. Yang J. Novel ECC architecture enhances storage system reliability. *In Proceedings of the Flash Memory Summit*, Santa Clara, CA, USA, 22–24 August 2012, pp. 1–15.

6. Tanakamaru S., Yanagihara Y., Takeuchi K. Over-10x-extended-lifetime 76%-reduced-error solid-state drives (SSDs) with error-prediction LDPC architecture and error-recovery scheme. *In Proceedings of the IEEE International Solid-State Circuits Conference (ISSCC)*, San Francisco, CA, USA, 19–23 February 2012, pp. 424–426.

7. Park D., Kim T.G. Safe microcontrollers with error protection encoder-decoder using bit-inversion techniques for on-chip flash integrity verification. *In Proceedings of the 2013 IEEE 2nd Global Conference on Consumer Electronics (GCCE)*, Tokyo, Japan, 1–4 October. 2013, pp. 299–300.

8. Park J., Bhunia S. VL-ECC: Variable Data-Length Error Correction Code for Embedded Memory in DSP Applications. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2014, vol. 61, no. 2, pp. 120–124.

9. Gazaryan Yu.O., Kosolapov Yu.V. *Ob eksperimental'noy otsenke stoykosti metoda sluchaynogo kodirovaniya k atake mnogokratnogo nablyudeniya chastichnykh kodovykh vektorov* [On the experimental assessment of the resistance of the random coding method to the attack of multiple observation of partial code vectors]. *Computational Technologies*, 2015, vol. 20, no. 6, pp. 5–21 (in Russ.).

10. Achkasov V.N. Smerek V.A., Utkin D.M., Zolnikov V.K. *Metody obespecheniya stoykosti mikroskhem k odinochnym sobytiyam pri proyektirovanii radiatsionno-stoykikh mikroskhem* [Methods for ensuring the resistance of microcircuits to single events in the design of radiation-resistant microcircuits]. *Problems of Development of Advanced Micro– and Nanoelectronic Systems. 2012. Proceedings under the general. ed. of Academician of the Russian Academy of Sciences A.L. Stempkovsky.* Moscow, IPPM RAN, 2012, pp. 634–637 (in Russ.).

11. Fedorov S.V. Romashkin V.I., Vyalykh K.M. *Realizatsiya potokovogo dekodera ukorochennykh kodov Rida-Solomona na PLIS* [Implementation of a streaming decoder of shortened Reed-Solomon codes on FPGA]. *Engineering and Computer Technologies*. 2016, no. 6, pp. 184–199 (in Russ.).

12. Subhasri G. Radha N. VLSI design of Parity check Code with Hamming Code for Error Detection and Correction. *In Proceedings of the 2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, Madurai, India, 15–17 May. 2019, pp. 15–20.

13. Nazarov L.E., Shishkin P.V. *Kharakteristiki pomekhoustoychivykh ukorochennykh blokovykh turbo-kodov iterativnogo priyema informatsii* [Characteristics of noise-immune shortened block turbo codes for iterative information reception]. *Radioelectronics. Nanosystems. Information Technology*, 2018, vol. 10, no. 2. pp. 323–328 (in Russ.).

14. Osokin A.N., Yaremenko A.V. *Realizatsiya turbokodeka na programmiruyemoy logicheskoy integral'noy skheme* [Implementation of a turbo codec on a programmable logic integrated circuit]. *Vectors of Well-being: Economics and Society*, 2011, no. 1 (1), pp. 382–387 (in Russ.).

15. Listopad N.I. *Teoreticheskiye osnovy tsifrovoy radiosvyazi: ucheb. posobiye* [Theoretical foundations of digital radio communication]. Minsk, BSUIR, 2012, 330 p.

16. Kim J., Cho J., Park D. Low-Power Command Protection Using SHA-CRC Inversion-Based Scrambling Technique for CAN-Integrated Automotive Controllers. *In Pro-*

ceedings of the 2018 IEEE Conference on Dependable and Secure Computing (DSC), Kaohsiung, Taiwan. December 10–13. 2018, pp. 1–2.

17. Cho S., Park D. Robust Intra-Body Communication Using SHA1-CRC Inversion-Based Protection and Error Correction for Securing Electronic Authentication. *MDPI Sensors*. 2020, no. 21, pp. 1–17.

18. IEC 62132-4–2006. Integrated circuits – Measurement of electromagnetic immunity 150 kHz to 1 GHz – Part 4: Direct RF power injection method. URL: https://webstore.iec.ch/publication/6510 (Accessed: March 05, 2022).

19. Integrated Circuits. Measurement of Electromagnetic Emissions. Part 2: Measurement of Radiated Emissions, TEM Cell and Wideband TEM Cell Method, IEC 61967-2, First Edition, 2005. URL: https://webstore.iec.ch/publication/6185 (Accessed: March 05, 2022).

Artem V. Osintsev
Assistant, Department of Television and Control, Tomsk State University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0003-0888-6793
Phone: +7-952-755-01-23
Email: kubenet@gmail.com

Maxim E. Komnatnov
Candidate of Science in Engineering,
Senior Researcher, Associate Professor,
Department of Television and Control, TUSUR
40, Lenin pr., Tomsk, Russia, 634050
ORCID: 0000-0002-6463-2889
Phone: +7-952-888-38-96
Email: maxmek@mail.ru