

ФИЗИЧЕСКИЕ ПРОЦЕССЫ В ЭЛЕКТРОННЫХ ПРИБОРАХ

УДК 621.382

ПРИМЕНЕНИЕ СРЕДСТВ ТРАССИРОВКИ ДЛЯ АНАЛИЗА СБОЕВ МИКРОКОНТРОЛЛЕРА, ВОЗНИКАЮЩИХ ПРИ ВОЗДЕЙСТВИИ НЕЙТРОНОВ С ЭНЕРГИЕЙ 14 МэВ

© 2024 г. А. С. Пилипенко*, М. И. Тихонов

*Российский федеральный ядерный центр — Всероссийский научно-исследовательский институт
технической физики им. акад. Е.И. Забабахина, ул. Васильева, 13,
Снежинск Челябинской обл., 456770 Российская Федерация*

**E-mail: A.S.Pilipenko@vniitf.ru*

Поступила в редакцию 16.10.2022 г.

После доработки 07.06.2023 г.

Принята к публикации 25.06.2023 г.

Проанализированы возможности средств поддержки трассировки микроконтроллера с ядром Cortex-M3 для исследования сбоев, возникающих при облучении нейтронами с энергией 14 МэВ. Показано, что в большинстве случаев зависание вызвано переходом микроконтроллера в бесконечный цикл обработки неактивного исключения. Оценено значение сечения эффекта функционального прерывания и тиристорного эффекта.

Ключевые слова: микроконтроллер, трассировка, тиристорный эффект, эффект функционального прерывания, нейтрон

DOI: 10.31857/S0033849424020117, **EDN:** KMELDA

ВВЕДЕНИЕ

В настоящее время при исследованиях радиационной стойкости микроконтроллеров (МК) применяется несколько подходов для контроля их состояния. Одним из наиболее перспективных является применение встроенных средств отладки, которые входят в состав большинства современных МК. Данные инструменты позволяют как получать доступ к общей шине ядра, запоминающих устройств и периферии, так и контролировать пошагово ход выполнения программы. Если доступ к шине реализован как стандартный инструмент, то возможности пошаговой отладки (трассировки) существенно зависят от типа микропроцессорного ядра, а в ряде случаев — от реализации необязательных функций конкретным производителем МК. Тем не менее средства трассировки являются достаточно мощным инструментом анализа реакции МК при воздействии ионизирующего излучения. Как показано в [1], для ядра Cortex-A9 средства трассировки позволяют восстановить ход выполнения программы вплоть до момента зависания, возникающего при воздействии отдельных ядерных частиц. Следует отметить, что

в [1] аппаратный блок сбора и анализа данных от системы трассировки был реализован на базе системы-на-кристалле совместно с исследуемым МК. Это, на наш взгляд, сужает универсальность использования такой конфигурации, так как возникает вопрос устойчивости к сбоям блока сбора и анализа данных при воздействии импульсного ионизирующего излучения.

В [2] показана возможность получения данных из регистров МК с ядром Cortex-M3 даже в случае его зависания с помощью доступа общей шине через встроенные средства отладки. В данной работе был проанализирован доступный для одной из реализаций ядра Cortex-M3 функционал средств поддержки трассировки с целью оценки возможности анализа причин зависания МК. Для данного ядра в принципе не предусмотрено наличие модуля Program Trace Macrocell, использованного в [1] (этот модуль поддерживается ядром Cortex-A9), а в рассматриваемой реализации нет модуля Embedded Trace Macrocell. Указанные два компонента системы трассировки предоставляют наиболее полный контроль за ходом выполнения программы, вплоть до фиксирования истории изменений программ-

ного счетчика в реальном времени (на рабочей частоте ядра). В нашем случае реализованы компоненты Data Watch and Trace (DWT), Interface Trace Macrocell (ITM), Trace Interface Port Unit (TPIU). Далее кратко рассмотрены их возможности (для конкретного МК) с точки зрения применимости к рассматриваемой задаче.

В DWT предусмотрены возможности считывания содержимого программного счетчика, однако оно происходит либо по запросу от внешнего отладчика, либо периодически (но не менее чем раз в 64 такта). Также реализованы различные счетчики числа тактов, затрачиваемых для выполнения операций загрузки/сохранения, нахождения в спящем режиме, выполнения команды, а также связанных с переходом в обработчик исключения.

Компонент ITM является промежуточным модулем, передающим пакеты от DWT в порт трассировки для передачи внешнему отладчику. ITM может генерировать пакеты временных меток, вставляемые в поток данных от DWT, что помогает отладчику вести хронометраж событий.

Компонент TPIU применяется для вывода пакетов трассировки во внешний отладчик. Протокол передачи является последовательным (JTAG/SW), что замедляет обмен данными и априори не позволяет проводить сбор данных в реальном времени. TPIU содержит промежуточный буфер данных, однако его объем составляет всего 32 бита (одно слово).

Таким образом, рассмотренный функционал блоков трассировки ядра Cortex-M3 не позволяет выполнять контроль в реальном времени и определять предысторию перехода в состояние зависания. Однако представляется возможным получение дополнительной информации о состоянии “зависшего” МК в виде адреса последней выполняемой инструкции и количестве тактов, которое потребовалось для обработки исключительной ситуации в случае, если зависание связано с прерыванием выполнения хода программы.

1. ОБРАЗЦЫ И МЕТОДИКА ПРОВЕДЕНИЯ ЭКСПЕРИМЕНТА

В качестве объекта исследований использовался МК с ядром ARM Cortex-M3, изготовленный по технологии “объемный кремний” 0.18 мкм. МК облучали нейтронами с энергией 14 МэВ и плотностью потока порядка 10^9 н/(с·см²). Общий флюенс нейтронов за время экспери-

мента составил 6×10^{12} н/см², его определяли с помощью активационных детекторов с погрешностью 20 %.

Микроконтроллер исполнял программу из встроенной FLASH-памяти, функционал программы заключался в формировании на одном из выводов МК периодического сигнала (меандра). Тактовая частота работы ядра составляла 80 МГц, источником тактового сигнала являлся встроенный RC-генератор. В программе задействованы следующие функциональные блоки: блок умножителя частоты PLL, порт ввода-вывода PORTA, блок управления тактовыми частотами, таймер общего назначения. В качестве контролируемых параметров были использованы выходной сигнал (регистрировался на осциллографе) и ток потребления, фиксируемый по показаниям программируемого источника питания. Изменение параметров выходного сигнала или прекращение генерации рассматривалось как одиночный эффект функционального прерывания (single event functional interrupt, SEFI) – эффект, возникающий в программно-управляемых цифровых устройствах вследствие воздействия отдельной ядерной частицы, при котором работоспособность устройства восстанавливается после перезагрузки управляющей программы [3] (в нашем случае, после выключения/включения питания).

Перед началом облучения считывалась исходная информация из регистров процессорного ядра, оперативной памяти, периферийных блоков, служебного блока управления системой. Информация считывалась периодически или при проявлении SEFI, после чего производился контроль изменений в данных и их анализ, в том числе с использованием модели исключений ядра ARMv7 [4].

Информацию считывали через средства отладки посредством доступа к шине обмена данными между функциональными блоками МК с добавлением данных из модуля трассировки DWT (согласно описанному во введении).

2. РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

2.1. Одиночный эффект функционального прерывания

За время эксперимента зарегистрировано 31 событие, классифицируемое как SEFI. В двух случаях изменилась частота выходного сигнала, так как поменялся множитель частоты ядра в ре-

гистре блока управления тактовыми частотами вследствие одиночного сбоя (single event upset, SEU) – инверсии ячейки памяти, возникающей при воздействии отдельной ядерной частицы. Остальные события проявлялись как прекращение генерации выходного сигнала. При этом следует отметить, что:

- в трех случаях зарегистрирован SEU в регистрах управления работой порта ввода-вывода, вследствие чего режим работы порта изменился (он перестал функционировать как цифровой выход);

- 19 раз МК перешел в бесконечный цикл обработки исключения;

- для семи SEFI причина прекращения генерации не установлена, так как в анализируемых данных отсутствуют указания на обработку исключений или SEU в регистрах используемых в программе периферийных блоков.

Алгоритм анализа экспериментальных данных, позволяющий сделать вывод о переходе в бесконечный цикл обработки исключения, является основным в данной работе. В алгоритме рассматриваются регистры МК, используемые в модели исключений ядра ARMv7. Для определения того, находится ли МК в состоянии обработки исключения, рассматривалась информация из следующих регистров:

- стек из восьми 32-разрядных слов, используемый для хранения данных регистров МК для корректного выхода из обработчика исключения;

- регистр связи LR, указывающий на текущий режим работы МК (режим выполнения программы, режим обработки исключения либо вложенного исключения);

- регистр флагов xPSR (младшие 8 бит), содержащий поле для хранения номера активного исключения;

- регистр с информацией об адресе текущей исполняемой инструкции программного счетчика PC (Program Counter);

- счетчик числа тактов, требуемых для перехода в обработчик исключения EXCCOUNT;

- регистр состояния отказов с настраиваемым уровнем приоритета CFSR, хранящий флаги типов событий, приводящих к вызову обработчика исключений.

Данные, полученные из указанных выше регистров, приведены в табл. 1 (для эксперимен-

тов, где наблюдается переход в бесконечный цикл обработки исключения).

Как видно из таблицы, в большинстве случаев данные в регистрах совпадают (за исключением регистра флагов CFSR), следовательно, МК обрабатывает один и тот же алгоритм. Для отличающихся данных в экспериментах можно предположить возникновение SEU в отдельных ячейках регистров (например, в предпоследней строке таблицы значение EXCCOUNT отличается на один бит 0000000F – 0000001F).

Используя данные табл. 1 и информацию об алгоритме работы модели исключений ядра ARMv7 при штатной обработке исключений [4], можно сделать предположения о последовательности перехода МК в бесконечный цикл. Вначале устанавливается флаг исключительного события по одной из двух причин: либо событие действительно произошло (например, по причине SEU в регистрах ядра), либо SEU возникает непосредственно в регистре CFSR. Несмотря на разнообразие флагов событий в регистре CFSR (что свидетельствует о случайном характере их возникновения), после установления флага МК во всех случаях входит в обработку исключения с номером 3 – тяжелый отказ (номер исключения содержится в младших битах регистра xPSR). Факт входа в обработчик подтверждается корректным сохранением стека, значением регистра LR, ненулевым значением счетчика тактов EXCCOUNT и адресом из регистра PC, указывающим на область памяти, в которой расположен обработчик тяжелого отказа. Переход от любого типа исключения M, V и U к тяжелому отказу (с повышением приоритета исключения) предусмотрен моделью исключений в том случае, если исключения не разрешены к обработке (неактивны), что по умолчанию установлено в исполняемой программе. Кроме того, также по умолчанию все обработчики исключений (кроме сброса) не инициализированы, т.е. представляют собой бесконечные циклы. В данной работе мы не рассматриваем причины возникновения конкретного типа исключения и подробно не расписываем их в табл. 1 по двум причинам. Во-первых, анализ реакции МК в рамках применяемого подхода проводится по данным после воздействия, а не в режиме реального времени, что безусловно затрудняет определение причин зависания. Во-вторых, в нашем случае обработчики исключений были не инициализированы и неактивны, поэтому любой тип исключения M, V или U, приводит к тяжелому отказу.

Таблица 1. Основные анализируемые регистры МК

Стек*	PC**	EXCCOUNT**	xPSR**	LR**	Флаги регистра исключений CFSR ***								
					U1	U2	U3	U4	B1	B2	M1	M2	M3
+	08000232	0000000F	61000003	FFFFFFFF9	v								
+	08000232	0000000F	21000003	FFFFFFFF9		v							
+	08000232	0000000F	01000003	FFFFFFFF9					v				
+	08000232	0000000F	61000003	FFFFFFFF9									
+	08000232	0000000F	61000003	FFFFFFFF9									
+	08000232	0000000F	01000003	FFFFFFFF9								v	v
+	08000232	0000000F	61000003	FFFFFFFF9		v							
+	08000232	0000000F	61000003	FFFFFFFF9		v							
+	08000232	0000000F	01000003	FFFFFFFF9							v		
+	08000232	0000000F	01000003	FFFFFFFF9				v					
+	08000232	0000000F	61000003	FFFFFFFF9							v		
+	08000232	0000000F	61000003	FFFFFFFF9						v			
+	08000232	0000000F	21000003	FFFFFFFF9		v							
–	08000232	0000000B	61000003	FFFFFFFF9									
+	08000232	00000013	61000003	FFFFFFFF0			v						
+	0800023A	0000000F	6100000B	FFFFFFFF9									
–	08000232	0000000F	81000000	0C000201	v								
+	08000232	0000001F	01000003	FFFFFFFF1		v							
–	08000232	0000000F	61000003	FFFFFFFF9	v								

*Знаком “+” обозначен факт корректного сохранения стека, **32-битные значения в регистрах представлены в 16-ричной системе счисления, ***флаги регистра исключений CFSR разбиты на группы: тип U (UsageFault) – отказы при выполнении программы, тип B (BusFault) – отказы доступа к шине, тип M (MemoryFault) – отказы доступа к памяти, цифрами условно обозначены различные виды исключений в каждой группе.

Таким образом, данные табл. 1 позволяют сделать вывод, что в большинстве случаев зарегистрированных SEFI МК полностью отрабатывает предусмотренный спецификацией алгоритм перехода в обработчик исключений после фиксации флага возникновения исключения. Описанная ситуация отличается от случая воздействия импульсного ионизирующего излучения [5] (в том числе нейтронного), когда при наличии явных признаков нахождения в обработчике исключения (по данным анализируемых регистров), не все регистры после воздействия содержат значения, предусматриваемые моделью исключений.

Оценка сечения SEFI σ дает значение 5.3×10^{-12} см². Значения верхней и нижней границ доверительного интервала (σ_H , см²; σ_L , см²), соответствующие заданному значению довери-

тельной вероятности P , определялись по следующим соотношениям [3]:

$$\sigma_H = \frac{t_H(P, N)(0,67 + N)}{(1 - \theta)F} \tag{1}$$

$$\sigma_L = \frac{t_L(P, N)(0,67 + N)}{(1 + \theta)F} \tag{2}$$

где t_H и t_L – коэффициенты, зависящие от значения P и числа наблюдаемых событий N ; F – флюенс нейтронов, н/см²; θ – погрешность определения флюенса нейтронов.

Итоговые значения границ доверительного интервала, определенные по формулам (1) и (2), составили $3,1 \times 10^{-12}$ см² и $9,2 \times 10^{-12}$ см² для доверительной вероятности 0.95. Следует отметить, что данное сечение SEFI существенно меньше

сечения SEU, которое составляет $1.4 \pm 0.3 \times 10^{-8} \text{ см}^2$ (здесь границы доверительных интервалов определяются главным образом погрешностью дозиметрии).

2.2. Одиночный тиристорный эффект

В эксперименте также зарегистрировано четыре события, проявляющихся в переходе источника питания в режим ограничения выходного тока (оно составляло 200 мА при номинальном токе потребления на уровне 85 мА) с просадкой напряжения питания с 3.3 до 2.14 В и невозможностью обмена данными со средствами отладки. Возврат к штатному функционированию МК происходил после переключения питания. Такой тип событий можно трактовать как одиночный тиристорный эффект (single event latchup, SEL). Сечение данного вида эффектов оценивается как $7.8 \times 10^{-13} \text{ см}^2$ с границами доверительных интервалов $2.3 \times 10^{-13} \text{ см}^2$ и $2.1 \times 10^{-12} \text{ см}^2$ для вероятности 0.95.

SEL при воздействии нейтронов с энергией 14 МэВ в интегральных схемах (ИС) может иметь место, так как

1) современные ИС имеют широкий диапазон пороговых линейных потерь энергий (ЛПЭ) для данного эффекта. Так, например, в работах [6–8] по результатам исследований большого числа типоминималов ИС при воздействии тяжелых заряженных частиц показано, что пороговые ЛПЭ SEL не зависят от функционального класса ИС и имеют значение от 2 МэВ·см²/мг;

2) результаты моделирования взаимодействия нейтронов с энергией 14 МэВ с кремнием (см., например, [9]) показывают, что ЛПЭ продуктов реакций достигают 8 МэВ·см²/мг.

Исходя из сказанного выше, можно сделать вывод, что при воздействии нейтронов с энергией 14 МэВ в ИС возможно возникновение SEL за счет вторичных частиц, рожденных в реакциях на ядрах ²⁸Si, несмотря на их относительно малые ЛПЭ в кремниевых структурах.

ЗАКЛЮЧЕНИЕ

Анализ функционала блоков трассировки ядра Cortex-M3 исследуемого объекта показал, что для данного ядра полный контроль хода выполнения программы до момента зависания невозможен. Тем не менее, на основе анализа был дополнен существующий метод контроля

состояния МК в случае его зависания. Новой получаемой информацией является количество тактов, затрачиваемых на вход в обработчик исключения, а также адрес инструкции, в которой находится МК в момент обработки прерывания.

Установлено, что в большинстве случаев зависания МК переходит в бесконечный цикл, при этом он полностью отрабатывает предусмотренный спецификацией алгоритм перехода в обработчик исключений после фиксации флага возникновения исключения. Оценка сечения эффекта дает значение $5.3 \times 10^{-12} \text{ см}^2$.

В эксперименте также зарегистрировано четыре события, проявляющихся в переходе источника питания в режим ограничения выходного тока, что можно трактовать как одиночный тиристорный эффект. Сечение данного вида эффектов оценивается как $7.8 \times 10^{-13} \text{ см}^2$.

Авторы заявляют об отсутствии конфликта интересов.

СПИСОК ЛИТЕРАТУРЫ

1. Peña-Fernandez M., Lindoso A., Entrena L., Garcia-Valderas M. // IEEE Trans. 2020. V. NS-67. № 1. P. 126.
2. Пилипенко А. С. // РЭ. 2022. Т. 67. № 5. С. 514.
3. РД 134-0175-2009. Аппаратура радиоэлектронная бортовая космических аппаратов. Методы испытаний цифровых сверхбольших интегральных микросхем на стойкость к воздействию отдельных высокоэнергетических протонов и тяжелых заряженных частиц космического пространства на ускорителях заряженных частиц. Нормативный документ по стандартизации РКТ. М.: "ЦНИИ Машиностроения", 2009. №19720. 29 с.
4. ARM DDI 0403D "ARMv7-M Architecture Reference Manual" / Cambridge: ARM Limited, 2010. 1020 p.
5. Пилипенко А. С., Тихонов М. И. // Тр. 25-й Всерос. научн.-техн. конф. "Стойкость-2022". Лыткарино. 7–8 июня 2022. М.: НИИП, 2022. С. 52.
6. Протопопов Г. А., Казанцев Д. А. // Тр. 25-й Всерос. научн.-техн. конф. "Стойкость-2022". Лыткарино. 7–8 июня 2022. М.: НИИП, 2022. С. 125.
7. Irom F., Miyahira T. F. // Radiation Effects Data Workshop. 2005. P. 36.
8. Irom F., Miyahira T. F. // IEEE Trans. 2005. V. NS-52. № 6. P. 2475.
9. Weulersse C., Guibbaud N., Beltrando A.-L. et al. // IEEE Trans. 2017. V. NS-64. № 8. P. 2268.

APPLICATION OF TRACING TOOLS FOR ANALYSIS OF MICROCONTROLLER FAILURES ARISING UNDER THE 14 MeV NEUTRONS EXPOSURE

A. S. Pilipenko*, M. I. Tikhonov

*Federal State Unitary Enterprise “Russian Federal Nuclear Center – Zababakhin All-Russia
Research Institute of Technical Physics” Snezhinsk, Chelyabinsk oblast, 456770 Russia*

**E-mail: A.S.Pilipenko@vniitf.ru*

Received October 16, 2022; revised June 7, 2023; accepted June 25, 2023

The trace support tools capabilities for a microcontroller (MC) with a Cortex-M3 core are analyzed to investigation of failures arising under the 14 MeV neutrons exposure. It has been shown that in most cases, MC hang is caused by the microcontroller going into a handling an inactive exception infinite loop. The cross-section values for the single event functional interrupt and the single event latch-up are estimated.

Keywords: microcontroller, tracing, single event latch-up, single event functional interrupt, neutron