Programmatic Impact of SDRAM SEFI

Steven M. Guertin, *Member, IEEE*, Gregory R. Allen, *Member, IEEE*, and Douglas J. Sheldon

***Abstract*-- The Elpida EDS5104(08)ABTA 512Mb SDRAM is examined for programmatic impact of SEE. Use cases for the devices including EDAC and mode register reload are examined. Results indicate some SEE mitigation methods require careful application to achieve system-level benefits, while some event types are essentially mitigated by the application use. In the studied devices MBE and SEFI are identified and investigated as mechanisms requiring special consideration.**

I. Introduction

Synchronous Dynamic Random Access Memories (SDRAMs) are very important for modern space missions because they provide large amounts of highly integrated fast memory [1]; however they are very susceptible to single event effects (SEE). These devices and their descendants such as Double Data Rate (DDR) and DDR2 present a challenge to space missions due to their various Single Event Functionality Interrupt (SEFI) modes [2], [3]. Stored data and device operation can sometimes be recovered after a SEFI event by performing key device operations, but these are not standard in non-space use, do not completely eliminate SEFIs, and are not always designed into space applications.

Space applications that use these devices employ single error detection double error correction (SECDED) or more robust error detection and correction (EDAC) algorithms to protect against bit errors. Because SECDED is very common, systems are also challenged by multiple bit errors (MBEs) where a single ion upsets two or more bits in the same logical word.

Manuscript received Month, Day YEAR. The research in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. Reference herein to any specific commercial product, process, or service by trade name, manufacturer, or otherwise, does not constitute or imply its endorsement by the United States Government or the Jet Propulsion Laboratory, California Institute of Technology. This work was supported in part by the NASA Electronic Parts and Packaging Program (NEPP), and the Juno, MSL, and SMAP programs.

Steven M. Guertin is with the Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA 91109 (USA), phone: 818-393-6895, e-mail: steven.m.guertin@jpl.nasa.gov.

Gregory R. Allen is with the Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA 91109 (USA), phone: 818-393-7558, e-mail: gregory.r.allen@jpl.nasa.gov.

Steven M. Guertin is with the Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA 91109 (USA), phone: 818-393-5113, e-mail: douglas.j.sheldon@jpl.nasa.gov.

© 2012 California Institute of Technology. Government sponsorship acknowledged.

Based on test results in many reports, mode register reload should be used in SDRAM space applications [2-10] because it acts as a reset mechanism for the internal operational state including address decoders [11-12]. However in some cases this information is either not passed to designers or is overlooked because of mission heritage or because event rate and event impact are believed to be acceptable. Recent programmatic review of SDRAM use has highlighted situations where the benefit of reloading the mode register might be limited. This occurs sometimes because programs are already in flight and modifications are difficult and very costly. But it also occurs because detailed understanding of the structure of SEFI events and the program use of the devices indicates that rates for events with program impact are limited or are not significantly improved by reloading the mode register.

This paper reviews SDRAM device use, manifestation of SEFIs, the role of MBEs, and program use considerations for evaluating event impact. Analysis of these shows that even when following best principals, applications will be affected by SEFIs and MBEs unless utilizing EDAC that can correct all the bits for one of the system's memory devices.

This paper examines Elpida 512Mb SDRAMs (EDS5104ABTA, EDS5108ABTA and EDS5116ABTA, which share the same die) in order to extract key information necessary to assess program impact of SEFIs and MBEs.

We have extended the existing data on the Elpida 512Mb SDRAM in the literature in the following ways. We have gathered detailed error maps on 100's of SEFIs to enable assessment of programmatic impact of the actual error signatures. We have systematically examined the operation of test devices after SEFI without reloading the mode register. This includes examining device data retention issues and possible defects that a SEFI may expose [1, 6, 14]. We have also collected MBE information after removing troublesome SEFI-related upsets that easily confuse MBE results in earlier work.

II. Impact of Program Use

This work extends previous studies of the subject SDRAM SEE by considering how the available data and recommendations for operation translate into program level use cases, and by collecting data relevant to using these devices after a potentially problematic SEFI is encountered. There are two primary considerations we will address. The first is the case where a program has not implemented the aerospace-recommended periodic mode register reload (which is not standard in non-aerospace applications). And

the second consideration is the impact of MBEs which overwhelm standard SECDED EDAC systems.

A. SEFI and MBE

These Elpida SDRAMs are used in many different missions. In some cases (e.g. Juno) nearly 100 of these devices are used. This increases the likelihood that infrequent upset modes may have operational impact. It is important to have a working understanding of the impact of even rare events (on the order of 0.001 event/device-year) to be adequately prepared to handle potential flight anomalies.

Error correction is a very important element of program impact. It is important to understand the potential impact of SEFI and MBE structures when taken in conjunction with the EDAC system employed. For example, program response to double bit errors which cannot be fixed by SECDED systems range all the way from logging an uncorrectable error when it is encountered, to taking the spacecraft to a safing situation.

In the case of the SEFI, we will discuss several different types with different signatures and different ways of potential mitigation. Types previously discussed in the literature include (A) band SEFI, (B) row SEFI, (C) unrecoverable SEFI, (D) rewritable SEFI, and (E) SEFI requiring reloading the mode register [2], [4], [6]. These types are not mutually exclusive.

In the case of MBE, we will examine accurate identification of MBEs. For example, without a robust analysis system capable of identifying all SEFIs and removing them from the data used to determine MBEs, then MBE cross sections will be incorrectly high. Unreasonable MBE rates lead system designers to simply ignore the problem. Accurate information can reverse this and result in more reliable space systems.

B. Recoverable SEFIs

Here we briefly describe what a “recoverable” SEFI is. This type of SEFI occurs when corrupted data is somehow recovered by reloading the mode register. The assumed explanation here is that reloading the mode register forces a reset of the device which corrects the error [10], [11].

The impact of recoverable SEFIs is determined by how the device is used (or not used) between when the SEFI occurs and when the recovery method (mode register reload) is performed. Mode register reload operation takes very little time (less than 100 ns), so this time could be made very small. However, recommended intervals range from 100 ms to 1 s, such as in [6] and in common discussion. The results from this work include improved information on recoverable SEFIs, including reload interval, as discussed in Section IV.

C. Program Types

The impact of SEE on programs depends on how the SDRAMs are used by the program. During this work we reviewed the implementation of the EDS5104ABTA and EDS5108ABTA on several JPL missions and found three primary program implementations. These implementations carry different sensitivity to MBEs and SEFIs.

1) Computer Main Memory

One standard application of the devices is as main memory for a computer. In this case speed of the memory and standard memory controller use means that it is common for these systems to only utilize SECDED EDAC. Because it is not known how important the lost memory is in the event of a SEFI or MBE, the memory controller notifies the running computer of double bit errors (note that the chances for MBEs and SEFIs to exhibit double bit and higher errors is discussed later). It is then up to the operating system to properly handle a machine exception or interrupt.

It is worth pointing out that even in space applications it is possible that the operating system may not have a graceful way of handling double bit errors.

For this application SEFIs and MBEs are both potentially problematic. It is important to know what the probability is for any critical algorithm encountering double bit errors. Furthermore, even if SEFIs are recoverable, unless they are recovered before the system ever accesses any of the impacted data, the system may still be forced into a non-graceful error handling operation. Mode register reload in this case is recommended to be fast enough that the probability of a recoverable SEFI (where reloading the mode register recovers all of the corrupted data) getting into operation is no more common than the occurrence rate of an unrecoverable SEFI.

2) Data Recording

Another application examined for this work is where the data stored in the SDRAM is mostly unused except when it needs to be accessed for transmission or use. An example is the case of instrument data. In this case the SDRAM is used as a recording device and nothing critical for the system is stored in the SDRAM.

When an MBE or SEFI is encountered in this type of application, no immediate action is likely to be taken by any critical system. The event will simply sit in memory and be monitored as an EDAC scrubber periodically goes through the memory to remove errors. Upon direct access by the system, a data error will be encountered but should not cause system response.

It may appear this type of application could benefit from recovery mechanisms after the scrubber has identified the SEFI. However, if the EDAC system has undefined behavior when the number of bit errors in the EDAC word exceeds two, it will not be possible to reliably recover data in the EDS5108ABTA device after the scrubber has “scrubbed” through a recoverable SEFI.

3) Memory Buffering

Another common use case for the SDRAMs is as a transfer buffer. One of the missions examined for this paper uses the SDRAMs primarily to store information in transit between two other systems. In this case the data is read from a source, stored in the SDRAM, and then it is read from the SDRAM and transferred to a target. The data is not resident in the SDRAM very long.

This application is similar to case (2) in that it is not part of the critical operation of the spacecraft and a double bit error upon access need not reach a system level response.

What makes this situation very different from (1) and (2) is that the live time for data is much shorter. This means that recoverable SEFIs are more likely when there is no data in the system, and the time between accesses is much smaller requiring faster mode register reload if it is being used.

III. SEFI Structures

Discussion with project designers indicated that classification of SEFIs by their footprint in the system memory was valuable. Knowing how SEFIs may alter data enables designers to ensure that their systems can handle the events when they occur, and it also enables reliable classification of spacecraft anomalies.

In this study we identify all events where many addresses are affected with data loss and we develop a method to describe the events in a way that will be beneficial to designers and users. Previous works define SEFIs by how the test hardware identifies the events, for example in [4] SEFIs are described by the number of errors observed in repeated passes of reading and writing the device. Similarly, in [6] SEFIs are classified by whether or not reloading the mode register recovers the data. Test-centric reporting such as this is common and in the absence of program input to describe how to interpret the data is likely the best approach to take. However, the use cases discussed above are relevant for examination.

In order to provide data relevant to the users, we found the best approach was to identify a memory range that contains a given SEFI and describe the impact of the SEFI based on the data bits that may be affected by the SEFI. Ultimately the best description would identify the smallest subset of the device memory and word size that would contain any bit that shows an error. For example, if a set of 200 addresses contained 100 addresses with data errors with no discernible pattern for how the 100 addresses occurred, we would identify the SEFI as being contained in those 200 addresses. Similarly, if, out of eight data bits, data errors were only observed in the two lowest bits (with some addresses having one only one of the two bits in error) we would indicate the SEFI was isolated to data bits 1 and 0.

Structurally, four types of SEFIs were observed on the test devices. Conceptually the way we identify the affected addresses is described in the last paragraph, but effectively the process may benefit from a specific example.

SEFI from the Juno spacecraft serves as an example. For an event with 4,365 addresses with double bit errors (DBEs), the values of the address bits for each DBE are analyzed in Table I (this is on a x4 device). This table shows that fourteen address bits change while the other 13 remain fixed. Further, of the 14 that change their values are approximately evenly split between 1's and 0's.

A little more clarification of Table I is still warranted. The fixed bits indicate those bits that every address in the SEFI shares with exactly the same value as every other address in the SEFI. So these bits clearly define the SEFI range – i.e. in this case the bank is three, the row must have the highest three bits be 0b100, and column bits eight, seven, and five down to one must be all '0', while column bit zero must be a '1'. If any of these bits were different, the address could be trusted to have no errors. The remaining bits form a subset of the device that is 2^{14} addresses in size, or 16,384 addresses. In the example, addresses can only have zero, one, or two bits in error, and only those addresses with two bits in error are included in the error set. Hence approximately one quarter, or 4,096 addresses would be expected to have DBEs (here we have 4,365 with DBEs). The data bits affected by the subject SEFI were the outer data bits. We designate this "X--X" to show that only the outer bits show errors.

Table I. Analysis of address bit values for all addresses in a SEFI with 4365 addresses with errors. Note these data come from an observed SEFI on the Juno spacecraft.

Signal		# times 0	# times 1	avg. value	Fixed?
Row12	A26	0	4365	1.00	Yes
Row11	A25	4365	0	0.00	Yes
Row10	A24	4365	0	0.00	Yes
Row9	A23	2122	2243	0.51	No
Row8	A22	2136	2229	0.51	No
Row7	A21	2122	2243	0.51	No
Row6	A20	2192	2173	0.50	No
Row5	A19	2185	2180	0.50	No
Row4	A18	2176	2189	0.50	No
Row3	A17	2160	2205	0.51	No
Row2	A16	2154	2211	0.51	No
Row1	A15	2188	2177	0.50	No
Row0	A14	2161	2204	0.50	No
Bank1	A13	0	4365	1.00	Yes
Bank0	A12	0	4365	1.00	Yes
Col12	A11	2170	2195	0.50	No
Col11	A10	2225	2140	0.49	No
Col9	A9	2101	2264	0.52	No
Col8	A8	4365	0	0.00	Yes
Col7	A7	4365	0	0.00	Yes
Col6	A6	1071	3294	0.75	No
Col5	A5	4365	0	0.00	Yes
Col4	A4	4365	0	0.00	Yes
Col3	A3	4365	0	0.00	Yes
Col2	A2	4365	0	0.00	Yes
Col1	A1	4365	0	0.00	Yes
Col0	A0	0	4365	1.00	Yes

The information in Table I along with the description of the data bits that can be affected form a complete description of the SEFI. We can also describe the address range as: bank 3, row 0x1000-0x13ff, column (0x1, 0x41) x 0x200*N* (this column notation is used to account for 0x1, 0x41, 0x201, 0x241, …). This is a specific example of a SEFI categorization that is fixed to a bank, spans 1024 contiguous rows, and is isolated to 16 columns. The columns in question can cover a maximal range of 0x0 to 0xf00 (four bits change from '0' to '1') or 3840 columns (in this specific case the range is 0x1 to 0xe41).

A graphical display of the errors, where each square portion of the graph represents an address inside the SEFI range, and a dark square indicates a DBE was observed, is provided in Fig. 1. Note that the structure of the DBE pattern is indicative of the complexity of the underlying data.

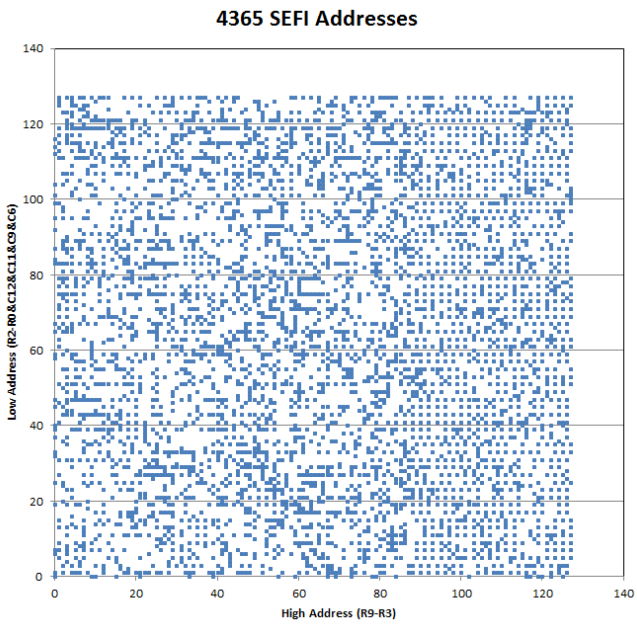

Fig. 1. Graphical display of the errors in a SEFI. Fixed address bits are stripped and the remaining bits used to form x and y values. Only MBEs are plotted. These data come from an observed SEFI on the Juno spacecraft.

Table II. Structure details describing the most common SEFIs in Elpida EDS510X devices. Note that 'X' and '-' refer to bits that can and cannot show errors, respectively

Attribute	Band-Type	Row-Type 1	Row-Type 2	Region-Type
SEFI Addresses in 5104	16384	4096-16384	4096	5-500,000
SEFI Addresses in 5108	8192	2048-8192	2048	5-250,000
Error Pattern A in 5104	X--X	X--X	X--X	X--X
Error Pattern B in 5104	-XX-	-XX-	-XX-	-XX-
Error Pattern A in 5108	XX----XX	XX----XX	XX----XX	XX----XX
Error Pattern B in 5108	--XXXX--	--XXXX--	--XXXX--	--XXXX--
Isolated to One Bank	Yes	Yes	Yes	No
Affected Row Count	1024	4	1	1-128
Affected Row Range	Contiguous	768	1	Contiguous
Column Count 5104	16	4096	4096	4096
Column Count 5108	8	2048	2048	2048
Column Range 5104	3840	Contiguous	Contiguous	Contiguous
Column Range 5108	1792	Contiguous	Contiguous	Contiguous
SBU Count in 5104	8000	2000	1000	1-250,000
DBU Count in 5104	4000	500	1500	1-125,000
>DBU Count in 5104	0	0	1250	untested
SBU Count in 5108	2000	500-2000	50	1-60,000
DBU Count in 5108	3000	750-3000	200	1-90,000
>DBU Count in 5108	2600	650-2600	1750	1-75,000

A listing of the four SEFI modes observed in the EDS5104ABTA and EDS5108ABTA is given in Table II. Note that the final SEFI type, the region-type, can be a very large SEFI and is intended to contain the most extensive SEFIs that fit the general description. That is, we do not believe these devices will exhibit SEFIs whose characteristics are not contained by this list of SEFIs.

IV. Test Setup

The devices under study here have been examined numerous times in the past [4-9]. Direct examination of the EDS5104 and EDS5108 devices show that they share the same die, and it is likely the EDS5116 does as well. Test results include bit errors, SEFIs with detailed structural information, and MBEs.

A. Test Hardware

Testing was performed using the JPL modular digital test system (MDTS) which is based on commercially available field programmable gate array (FPGA) evaluation boards. A drawing of the test hardware is provided in Fig. 2. The DUT is physically separated from other active components of the test board by enough distance to enable shielding of the remainder of the circuit.

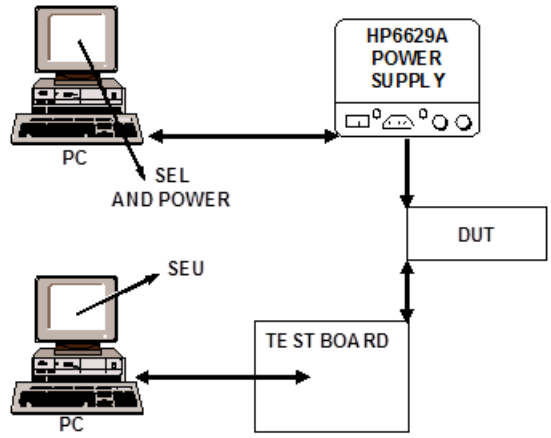

Fig. 2. Test hardware consisted of a computer to functionally operate the DUT, and another to control and monitor power.

Note the following details about DUT operation. DUTs were operated at room temperature. Bias was set to 3.3V. Irradiation data pattern was address based, with thirty-two data bits used to encode the current address. Refresh rate was 16 ms. Operating frequency was 33 MHz. Operating duty cycle was about 5%.

B. Beam Exposure

We performed both heavy ion and proton testing. The beams used are summarized in Table III. Heavy ion testing was performed at the Brookhaven National Laboratory (BNL) Tandem Van de Graff facility. Proton testing was performed at the Indiana University Cyclotron Facility (IUCF) (also now called the Integrated Science and Accelerator Technology (ISAT) Hall).

Table III. Beams used in testing of the EDS5108ABTA at BNL and IUCF

Beam	Energy/LETeff	Fluence (#/cm2)	# of DUTs
p	28 MeV	4.00E+11	2
p	55	4.29E+11	2
p	200	2.01E+12	5
C	1.4 MeV-cm2/mg	4.34E+06	1
F	3.4	3.68E+06	1
Si	8	1.19E+07	2
Ca	16.3	2.69E+06	1
Fe	24.4	1.10E+06	1
Br	37.5	3.06E+05	2

C. *Device Preparation*

Devices were prepared for heavy ion exposure by decapsulating the die and rebonding to a mounting board. Protons test devices were simply placed in a socket.

D. *Test Algorithm*

For the projects we were evaluating it was requested to collect data using the following algorithm.

1. Load data into the device under test (DUT)
2. Perform repeated read-back of DUT
3. Verify DUT holds correct data
4. Begin irradiation
5. Continue repeated read-back and store DUT data images
6. Stop beam once irradiation is complete
7. Continue read-back until number of errors in DUT stabilizes
8. Re-write the DUT
9. Re-read the DUT to determine if the written data was good
10. Repeat 8 and 9 with the inverted pattern

V. Test Results

The test results for SBU and SEFI are presented here. Information was gathered to investigate device use after SEFIs without a mode register reload (device reset). We present this information by looking at the types of SEFI events observed. We also present information gathered regarding the impact of reloading or not reloading the mode register.

A. *SEFI Structure*

Four primary types of SEFIs are exhibited on the Elpida EDS5108 device. SEFI structure is reviewed in Section III with analysis details presented here. Error pattern is particularly important in the case of this device because it was observed that the majority of SEFIs in the 4-bit part would never have an event with more than 2-bits in error in one address, while in the 8-bit part it was important to establish if the bits involved could change allowing more than 2 bits in an 8-bit word.

The most common type of SEFI is the "band" SEFI, which is named after its visual presentation in the analysis software. This SEFI presents as 1024 contiguous rows with 16 addresses potentially showing errors in each row in the DUT. For the 4-bit part, only two of the data bits can show errors due to a single SEFI. The important bits would be the inner or the outer bits, or patterns "X--X" or "-XX-" where 'X' refers to a bit that can change, and '-' refers to a bit that is never in error. The data showing this event structure was developed for [6]. For the 8-bit part, it was observed in this work that up to 4 bits could be affected in any given address, and the error patterns were "XX----XX" and "--XXXX--".

An example of band SEFIs observed (and a general example of test data presentation) in the EDS5108 part is presented in Fig. 3. Information to decode the data observed in this figure can be found in Table IV. Note that in the EDS5104ABTA, a row contains 4096 columns (a column is a 4-bit data word), while in the EDS5108ABTA, a row contains 2048 columns (8-bit data words). This analysis reflects information collected on over 500 band-type SEFIs.

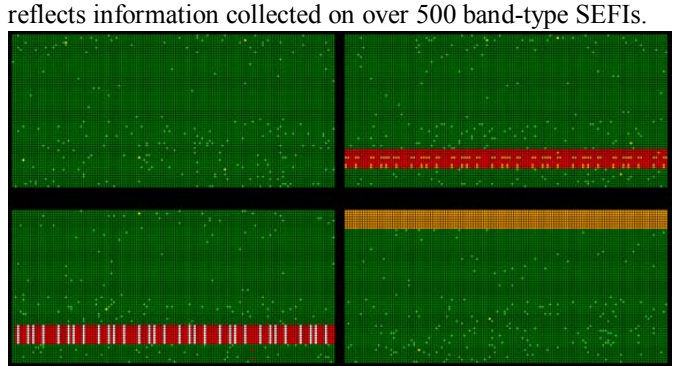

Fig. 3. Graphic display of SEU information grouped by row and bank. 3 band-type SEFIs are visible. Color decoding information is in Table IV.

Table IV. Decoding key for colors in error analysis.

Color	Bit Errors in Row
Dark Green	No error
Light Green	1 SBU only
Yellow	2 SBUs only
White	3 or more SBUs
Orange	One or more Double bit error
Red	One or more Triple+ bit error

The second most common type of SEFI is called a "row-type 1" SEFI and is identified by a row or set of rows with many errors. This type of SEFI is manifest as either 1, 2 or 4 impacted rows, with each row being susceptible to data corruption in all of its columns. In the 4-bit part, 4096 or more of the addresses in the DUT are susceptible to errors during each event, while in the 8-bit part, the number is reduced to 2048 or more. As with the band-type, the row SEFI 1 impacts only the outer or inner 2 data bits on the 4-bit part, and the outer or inner 4 data bits on the 8-bit part.

Two other types of SEFIs were seen by examination of the data, they are the unrecoverable row SEFI ("Row-Type 2") (only one row is affected and reloading the mode register has no effect on the lost data), and the region SEFI. Note that region-type SEFIs of large size were very uncommon. The relevant information on the event structure for the most common SEFI modes can be found in Table II

In systems where mode register reload is used, the band type and row-type 1 SEFIs can be cleared. Depending on the period of mode register reload, these SEFIs may still have some impact because system use or scrub operations may have already encountered the SEFI before the reload is performed.

B. Device Reliability without Mode Reload

A major topic for examination in this work is the reliable operation of devices after a SEFI without reloading of the mode register. In order to test this we exposed devices to numerous SEFIs without mode register reload. After irradiation and gathering of the SEFI data we then attempted to rewrite the device to determine if any of the SEFIs resulted in a compromised device.

In only one case in more than 750 SEFIs was a device observed to no longer be able to reliably store data. In this case approximately 100 addresses were unable to be programmed with the test pattern and its complement.

C. Heavy Ion Results

Heavy ion testing was performed to establish SEFI and MBE cross section for specific application use scenarios. Heavy ion testing was performed on two lots. Results from the two lots were consistent.

SEU results on these devices are given in Fig. 4. The 4-, 8-, and 16-bit devices share the same common die and are expected to have approximately the same SEE response.

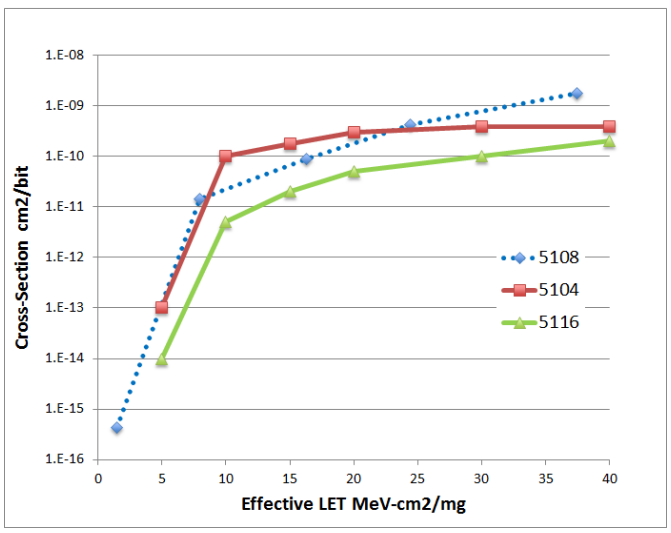

Fig. 4. The per bit SEU cross sections for the x4, x8, and x16 devices. The x4 and x16 data come from [5] and [6].

The results for SEFIs are presented in Fig. 5. Note that except for the "unclearable" curve, it is expected that the data sets show similar results.

The difference observed between the 5116 and other devices is likely due to the impact of not testing the entire device and extrapolating results from a subset of the device to predict the cross section of an entire device.

A significant result here is that the 5104 total SEFI cross section and that of the unclearable SEFIs is only a factor of ten or less different indicating that clearing SEFIs only results in a reduction in problematic SEFIs of a factor of ten. See Section V.E below.

Because heavy ion testing was performed at normal incidence, no region-type SEFIs and no MBEs were observed. Results from protons (see below) and other reports indicate the MBE and region-type SEFI cross sections at angle may be as high as the diamonds and squares (EDS5104 and 5108) shown in Fig. 5.

Testing showed that in over 500 SEFIs all resulted in a device that still reliably stored and retrieved new data.

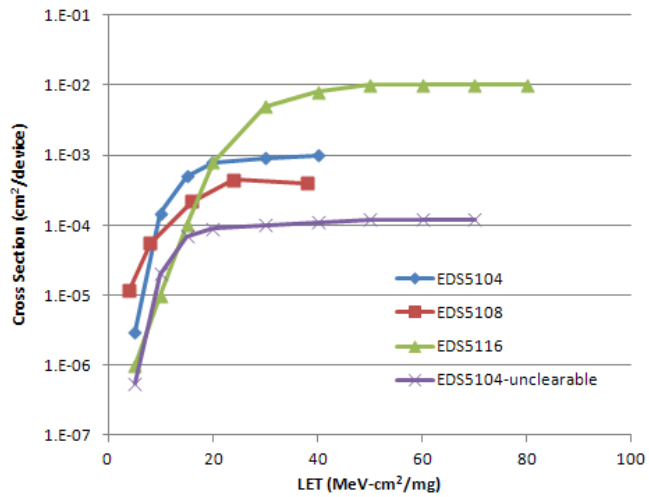

Fig. 5. Comparison of SEFIs across device versions, showing previous results from [5,6]. EDS5108 data is reported here. Reloading the mode register clears many SEFIs but not all, leaving many events.

D. Proton Results

Proton data are separated by device, reflecting a total of 5 test devices. These devices were from several different lots, so the variation in the device responses provide means to bound the potential response.

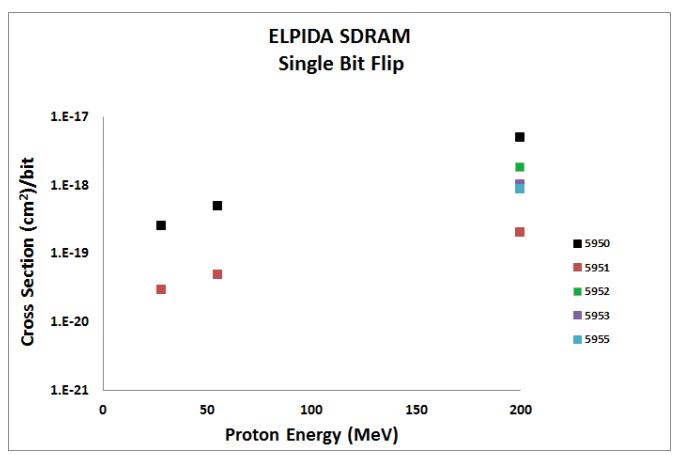

Fig. 6. The proton SBU cross section for 5 of the 8-bit devices.

The proton SEU cross section is presented in Fig. 6. These results can be compared with those of [4] which indicate a cross section of about $1x10^{-17}$/bit at 200 MeV.

Results for proton induced SEFIs are shown in Fig. 7. Compare this with [4] which has a SEFI cross section at 200

MeV of about $1.5x10^{-11}cm^2$. Here all SEFI types are bundled together.

As with the heavy ion testing, most of the SEFIs were tested by rewriting the data to determine if the device functions well for storing and retrieving new data. Only one out of about 250 SEFIs resulted in a device that could not reliably store and retrieve new data. In this case approximately 100 addresses were unable to store reliable data.

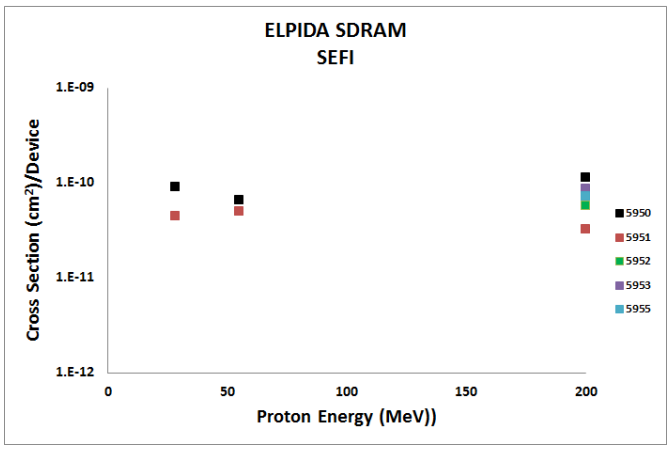

Fig. 7. The proton SEFI cross section for 5 of the 8-bit devices. The includes all types of SEFIs.

E. Differences from Other Reported Results

In our testing there were not very many individual row-type 2 SEFIs compared to [6]. It is believed this may be due to operating speed or duty cycle. This suggests that the ratio of ten indicated between all SEFIs and unclearable SEFIs indicated in Fig. 5 cannot be supported by our data (note that this ratio is driven by the ratio of individual row-type 2 SEFIs to all SEFIs). For this reason we estimate that approximately 1% of SEFIs will be unclearable instead of 10%.

Testing at angle has suggested SEFI modes where corrupt rows are repeated in different blocks. This mode was not observed in the present testing, but we have included the chance for this happening in the region-type SEFI category.

Once the SEFI errors were removed from the data collected here, we only saw very limited MBEs, and only during proton testing. The cross section for these was approximately the same as for SEFIs. In heavy ion testing there were no observed MBEs after removing all SEFIs, but again our testing was only at normal incidence.

VI. Mode Register Reload

The actual usage of the memory devices will play a very important role in how beneficial reloading can be. As found in the heavy ion and proton results, in the majority of cases SEFIs can be overwritten and the memory used as good memory. So if the memory is not storing critical information, the SEFI impact can be limited based on system response to corrupt data (i.e. ignoring or overwriting corrupt data).

On the other hand if the memory has critical information and mode register reload will be used, an appropriate reload period must be selected. Four key factors contribute to selection of reload interval. The first is the ratio of SEFIs that can be fixed to those that cannot, which we take to be R. The second is the EDAC scrub period, which we take to be T_S. The third is a memory use interval M which is the time between subsequent uses of the same section of memory. Realistically, this must be at least the number of addresses divided by the frequency, so a good estimate is $5x10^8/3.3x10^7$, or 20s (for a 512MB system).

The fourth and final component is the footprint of the SEFI in the memory, which we call F. F is the inverse of the portion of memory spanned by the SEFI. Aside from very large region-type SEFIs (which were not seen in this testing but appear to require ions with high LET and angle), F is determined by the addressing mode. If the bank bits are the highest ones, then two bank bits and three row bits are unchanged for all other SEFIs resulting in the maximal SEFI extent being 1/32 – so F is 32. If the bank bits are not the highest order address bits, the maximal extent drops to 1/8 – so F is 8.

An appropriate reload time is described by Equation 1.

$$\tau_R = \frac{F}{R}\min\{T_S, M\} \quad (1)$$

Reasonable example values are F ranges from 8 to 32, R is approximately 100, T_S could range from 0.1 to 10s. This gives a range for τ_R from 0.01s to 3s for the reload interval. For specific missions, an appropriate interval can be chosen.

VII. Program Impact

After examining the individual SEFI and MBE structures in the 4- and 8-bit versions of the SDRAM, and discussing what mode register reload does and how to pick an appropriate interval, we can address the impact of EDAC and mode register reload on the various program use cases of interest.

Each case is addressed here, and the overall results tabulated in Table V.

Table V. Impacts of SEFIs based on system use of SDRAMs

System Use of EDS51XX	Impact(s) of SEFI
Main Computer Memory	Corrupt Data or Interrupt of Execution
Solid State Recorder	Corruption of Data
Buffer or Transfer Memory	No Impact Unless SEFI Occurs During Use

A. Computer Main Memory

For systems that use the subject SDRAMs as computer main memory, both MBEs and SEFIs can have important effects. Additionally, proper use of mode register reload can be useful, provided the reload interval can be set appropriately for the application. Due to the nature of these applications, standard memory controllers may be desired.

These memory controllers have limited flexibility in signal-level modifications necessary to employ EDAC stronger than SECDED,

B. Solid State Recorder

SDRAMs can be used to store data for later retrieval. In this case data corrupted by a SEFI are not likely to cause any other impact in the system because the recorder is a separate subsystem that is likely not tied directly into any part of the operation. In this case the average access interval is probably much larger than the scrub interval. Because of this, scrubbing will encounter most SEFIs and will either throw a large number of MBE notifications and/or may erroneously corrupt data further by scrubbing an error signature the scrubber is not designed to handle (i.e. due to three errors or more).

C. Memory Buffer

Another common use for memory in a system is as temporary memory to enable transfer of data. In this case, because only one in 750 SEFIs resulted in a situation where new data could not be reliably stored, the only SEFIs we worry about are those that occur during the memory transfer. Reloading the mode register up to 100 times faster than the average time data is buffered would improve SEFI response, but it is already significantly reduced by this use case.

VIII. Conclusion

This paper has examined existing and needed SDRAM SEFI data, mitigation strategy, and use scenarios. We have shown that the benefit of mitigation, including mode register reload and EDAC, depends on the program's use of the memory and the impact of the SEFI structure. We have found that careful examination of SEFI structure is needed but not often reported. We have also found in the case of the SDRAMs studied, MBEs are sometimes mixed with SEFI results in a way that provides unrealistic MBE rates for real missions.

Mode register reload can be used to reduce SEFI impact on a system down to the floor of SEFIs that the operation cannot fix. We have provided a method for determining an appropriate reload interval and developed recommended intervals, based on common system configuration. The recommended reload intervals are between 0.01 and 3 seconds, and can be tailored to system needs.

The overwhelming majority of SEFIs observed in the subject Elpida devices resulted in a device that could still be written and read reliably following irradiation without reload of the mode register. Because of this we have found that certain types of programs will be minimally impacted by not reloading the mode register. However, it is not a significant impact on the devices to reload the mode register and it is highly recommended that systems implement periodic mode register reload.

IX. Acknowledgment

The authors acknowledge assistance from the Juno, MSL, and SMAP projects. The authors also acknowledge direct assistance from many people including Brian Cox, Tracy Drain, Mark Katsumara, Carl Steiner, Mohammad Abid from JPL, and William Fehringer of Lockheed Martin.

The research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration. This work was partially supported by the NASA Electronic Parts and Packaging Program (NEPP), and the Juno, SMAP, and MSL projects.

X. References

[1] R. Ladbury, M. Shoga, R. Koga, "SDRAMs: Can't Live Without Them, But Can We Live With Them?", SEE Symposium, 2003

[2] R. Koga, et. al., "Permanent Single Event Functional Interrupts (SEFIs:) in 128- and 256-megabit Synchronous Dynamic Random Access Memories (SDRAMs)", IEEE Radiation Effects Data Workshop, pp. 6-13, 2001

[3] R. Ladbury, et. al., "Radiation Performance of 1 Gbit DDR2 SDRAMs Fabricated with 80-90 nm CMOS", IEEE Radiation Effects Data Workshop, pg. 41-46, 2008

[4] L. K. Reed, "Radiation Characterization of 512Mb SDRAMs", IEEE Radiation Effects Data Workshop, pg. 204-207, 2007

[5] Private communication with 3D Plus

[6] P. C. Adell, "An Approach to Single Event Testing of SDRAMs", IEEE Trans. Nucl. Sci., Vol , pg. 155-159, 2008.

[7] T. Langley, R. Koga and T. Morris, "Single-event Effects Test Results of 512MB SDRAMs," IEEE Radiation Effects Data Workshop, pp. 98-101, 2003

[8] A. B. Sanders, et. al., "Test Report for the EDS5108ABTA 3DPLUS ELPIDA SDRAM," http://radhome.gsfc.nasa.gov/, NRL100808_ NRL020209_ T110308_EDS5108ABTA.pdf, Oct. 2008

[9] R. Ladbury, et. al., "TPA Laser and Heavy-Ion SEE Testing: Complementary Techniques for SDRAM Single-Event Evaluation", IEEE Trans. Nucl. Sci., Vol. 56. pp. 3334-3340, 2009

[10] A. M. Chugg, et. al., "The Random Telegraph Signal Behavior of Intermittently Stuck Bits in SDRAMs", IEEE Trans. Nucl. Sci., Vol. 56. pp. 3057-3064, 2009

[11] A. Bougerol, et. al. "Use of Laser to Explain Heavy Ion Induced SEFIs in SDRAMs", IEEE Trans. Nucl. Sci., Vol 57., pg. 272-278, 2010

[12] A. Bougerol, et. al., "SDRAM architecture & single event effects revealed with laser," Proc. IEEE Int. On-Line Testing Symposium, pp. 283–288, 2008

[13] S. M. Guertin, et. al., "Dynamic SDRAM SEFI Detection and Recovery Test Results", IEEE Radiation Effects Data Workshop, pp. 62-67, 2004

[14] L. D. Edmonds, et. al., "Ion-induced Stuck Bits in 1T/1C SDRAM Cells", IEEE Trans. Nucl. Sci., Vol. 48. pp. 1925-1930, 2001S. Stratton, D. Stevenson, M. A. Johnson, "Rapid Development of Experimental LEON 3FT Controller Board", Small Satellites Conference 2009