Aeroflex Colorado Springs Application Note AN-MEM-004

SEFI Work-Arounds for MRAM Devices

Table 1: Cross Reference of Applicable Products

PRODUCT NAME	MANUFACTURER PART NUMBER	SMD #	DEVICE TYPE	INTERNAL PIC#
16Mb MRAM Device	UT8MR2M8	5962-12227	01,02	WP01
64Mb MRAM Device	UT8MR8M8	5962-13207	01,02	MQ09

*PIC = Product Identification Code

1. Overview

Many terrestrial applications, as well as space applications, use Aeroflex's volatile and non-volatile memories. Non-volatile memory is critical to the success of military, civilian, and commercial space applications. Applications include processor or field programmable gate array (FPGA) boot memory, program memory, and mass storage. In addition, applications in space include checkpoint memory, telemetry and attitude control, signal processing, and post-launch program updates. The critical nature of some of these applications may require superior SEE performance. The industry is highly accustomed to handling memory errors. Error detection and correction (EDAC) techniques and systematic deployment of fault recovery schemes is evidence that memory integrity, terrestrially and in space, is never guaranteed and needs to be considered by the system designer.

Both total ionizing dose (TID) and single-event effects (SEE) need consideration when examining the effects of space radiation on memory devices. SEE's in digital devices manifest when high-energy particles travel through a sensitive node in a micro-electronic device or storage element. The state change is a result of the free charge created by ionization. Such ionization may lead to destructive (single-event latchup [SEL] or single-event dielectric rupture [SEDR]) or non-destructive events. Non-destructive events are either transient (single-event transients [SET]) or stable events, such as single-event functional interrupt (SEFI), single-event upset (SEU) or multiple-bit upset (MBU). SEFI rates are low and may occur approximately once per century or millennia, depending on the device chosen. The focus of this document is to provide insight into simple application specific SEFI detection and recovery schemes for Aeroflex's MRAM devices.

2. MRAM Functionality and Radiation Performance

The MRAM devices are high-performance, non-volatile, memories compatible with traditional asynchronous SRAM interfaces.

2.1 Product Features

The MRAM devices have several control pins which includes chip enable (/E), write enable (/W), output enable (/G), and a sleep/reset mode (ZZ/RST) pins, allowing for significant system design flexibility without bus contention.

The magneto-resistive bit cells are immune to single event effects (SEE). To guard against transient effects, an error correction code (ECC) is included within the device. The device generates and stores ECC check bits within the MRAM array during writes. If

a single bit error occurs during a read cycle, it automatically corrects the data presented to the user.

The device operates with a nominal 3.3V power supply and supports >20MHz read/write access rates. Automatic data protection with low-voltage inhibit circuitry prevents writes on power loss. The operating temperature range for the device is -40°C to +105°C.

2.2 Memory Cell Architecture

The memory cell of this MRAM device has a number of benefits. Its design uses magnetic tunnel junction (MTJ) technology. The bit information, stored as a magnetic polarization, is inherently SEE and TID hard. The data writes to the cell by polarizing the MTJ material between two perpendicular metal lines, thus creating a magnetic field. A read or write of the cell is non-destructive and has an exceptionally high endurance (> $1x10^{14}$ cycles over temperature). Fig. 1 shows a cross-section diagram of the memory cell.

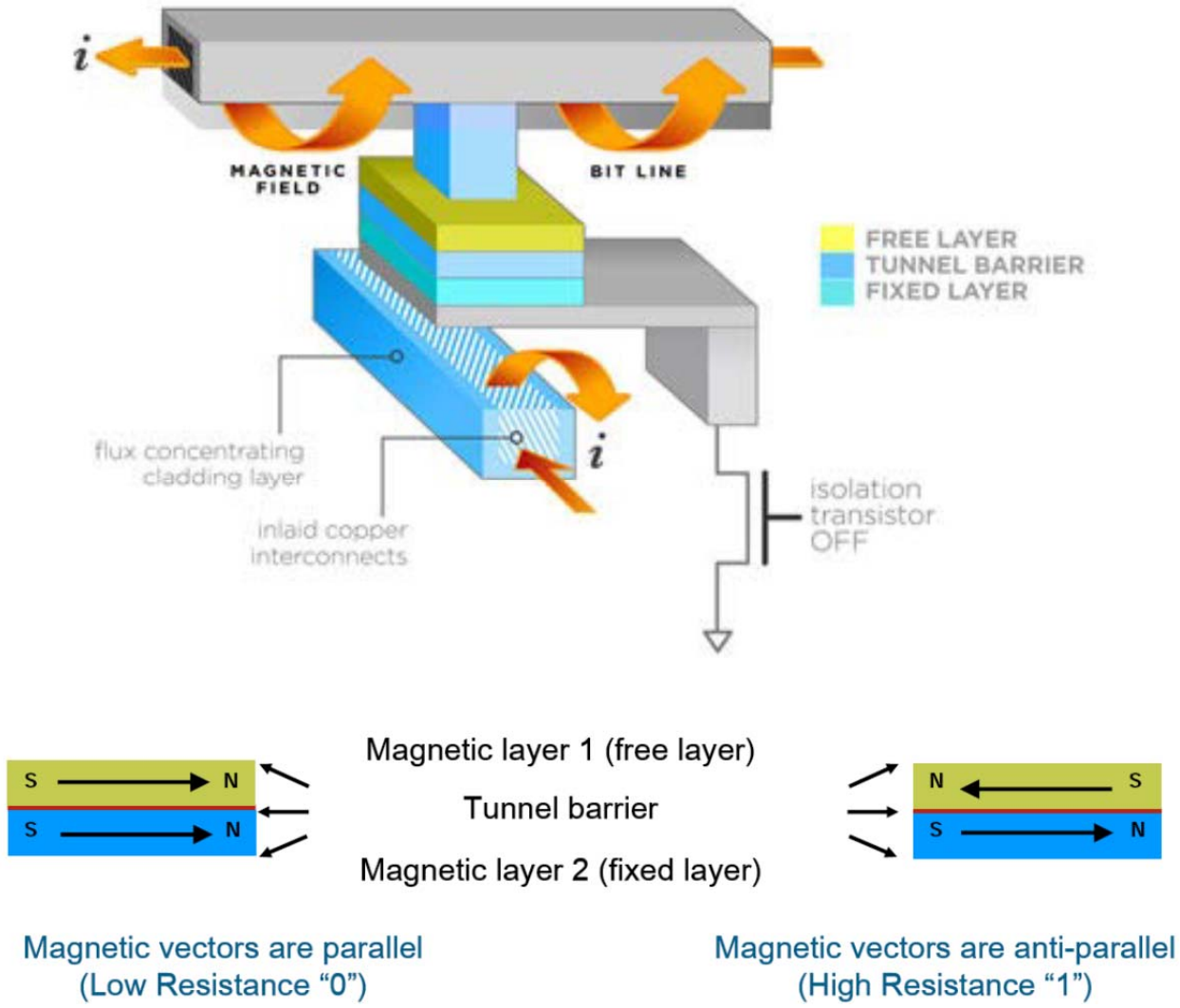

Figure 1: Cross-section diagram of the MRAM memory cell

Electrical current is passed through two perpendicular metal lines to create a magnetic field which programs (polarizes) the MTJ layer in one of two configurations for a low resistance "0" and a high resistance "1."

2.3 Radiation Performance

The MRAM devices incorporate special design and layout features that allow operation in harsh environments. Table 1 describes radiation parameters and each specification limit.

Table 2: Radiation Performance Specifications

Parameter	Limit	Units
TID	1	Mrad(Si)
SEL Immunity	$\leq$112	MeV-cm^2/mg
SEU Memory Cell Immunity	$\leq$112	MeV-cm^2/mg

2.4 SEFI Characterization

The Aeroflex MRAM was tested for sensitivity to SET and SEFI events for both read and write operations. The MRAM SEE report titled "SEU, SET, and SEFI Test Results for the UT8MR2M8/UT8MR8M8 MRAM 8/27/2012" contains the summary, results, and analysis of Aeroflex's MRAM testing.

The sensitivity of the MRAM device to a write was tested by performing a write operation of the entire array immediately followed by a read of the entire array. These two operations ran in a continuous loop in the presence of the ion beam. This is not an ideal test for isolating the effects of heavy ions on the write operation since it is impossible to determine if an error observed by the read was due to an error in the write operation or an error in the read operation. An ideal test would be to write the entire array with the beam on then read the array with the beam off. However, the cross-section of the device was low enough that a single write, followed by a beam off read, did not exhibit any errors.

As in the continuous read loop testing, both the SET and SEFI results are taken into account during write/read loop testing since a SET may induce a SEFI. As was shown in the original report, the memory cell itself will not upset during heavy ion irradiation with an effective LET = 112 MeV·cm^2/mg. Several definitions follow in Table 3.

Table 3: SEE Definitions

Acronym	Term	Definition
SEFI	Single Event Functional Interrupt	Bit errors in more than one consecutive address during a read
PSEFI	Persistent SEFI	Errors remain on the second (or more) read of the same addresses; another ion strike may cause the PSEFI to clear
TSEFI	Transient SEFI	Errors are cleared on the second read of the same addresses
SET	Single Event Transient	Bit errors in one address only

Data collected during SEE testing was post processed to separate individual events. A TSEFI is identifiable by a block of failing addresses that occurs once and then does not occur on the subsequent read, while a PSEFI carries the signature of a block of failing addresses repeating on one or more subsequent reads. A PSEFI may or may not be self-clearing. As Table 4 indicates, the only PSEFI that Aeroflex found had an onset LET of 53 MeV·cm^2/mg. All other SEFI events were self-clearing. The PSEFI cleared by resetting the device through the ZZ/RST pin.

Table 4: Summary of Write/Read Loop Data

LET (Mev-cm2	Program During Test	Fluence	SET Events in Beam	SEFI during Beam	Post Beam Read Test	Post ZZ toggle Read Test
112	R/W Loop	1.00E+07	17	**YES**	pass	**NA**
53	R/W Loop	1.00E+07	21	**YES**	PSEFI (> 1000 bits)	**PASS**
29.5	R/W Loop	1.00E+07	7	**YES**	pass	**NA**
29.5	R/W Loop	1.00E+07	9	**YES**	pass	**NA**
18.1	R/W Loop	1.00E+07	1	**NO**	pass	**NA**
8.7	R/W Loop	1.00E+07	1	**NO**	pass	**NA**
8.7	R/W Loop	1.00E+07	0	**NO**	pass	**NA**
5.7	R/W Loop	1.00E+07	0	**NO**	pass	**NA**

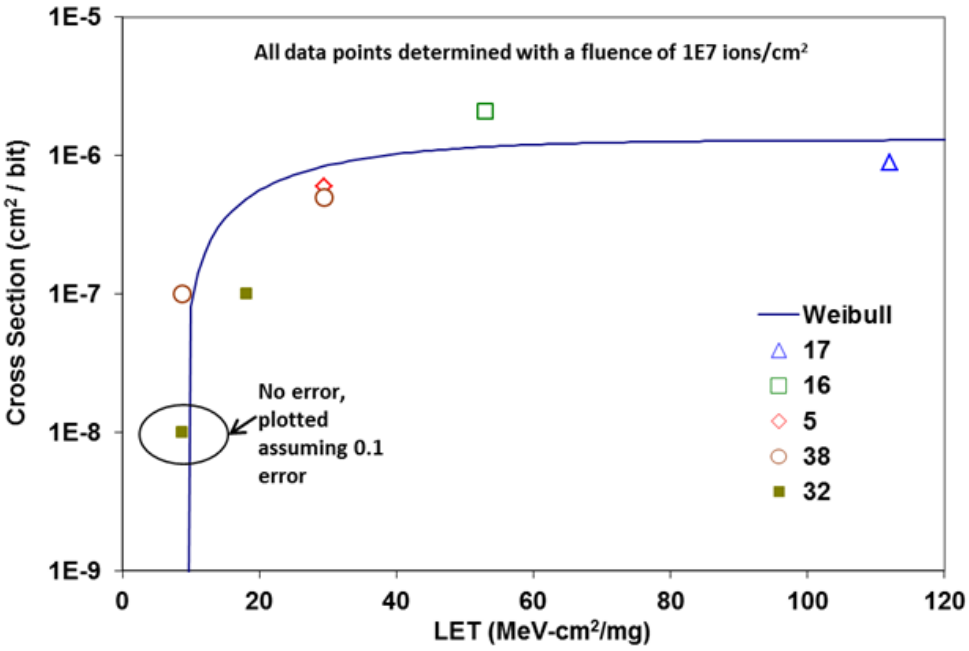

Figure 2: PSEFIs, TSEFIs, SEFIs, and the associated Weibull curve

Only SETs were observed at LET = 18.1 MeV·cm2/mg and below. Errors in the form of SEFIs occured at a LET = 29.5 MeV·cm^2/mg. The memory array data remained undisturbed during all SEFI and SET events. The lowest onset LET for all SEEs was 8.7 MeV·cm^2/mg.

Assuming a read of all 8M addresses in a four die multi-chip (MCM) 64Mb device once per minute during a 15 year mission, the probability of a SEFI event occurring is 0.0048%.

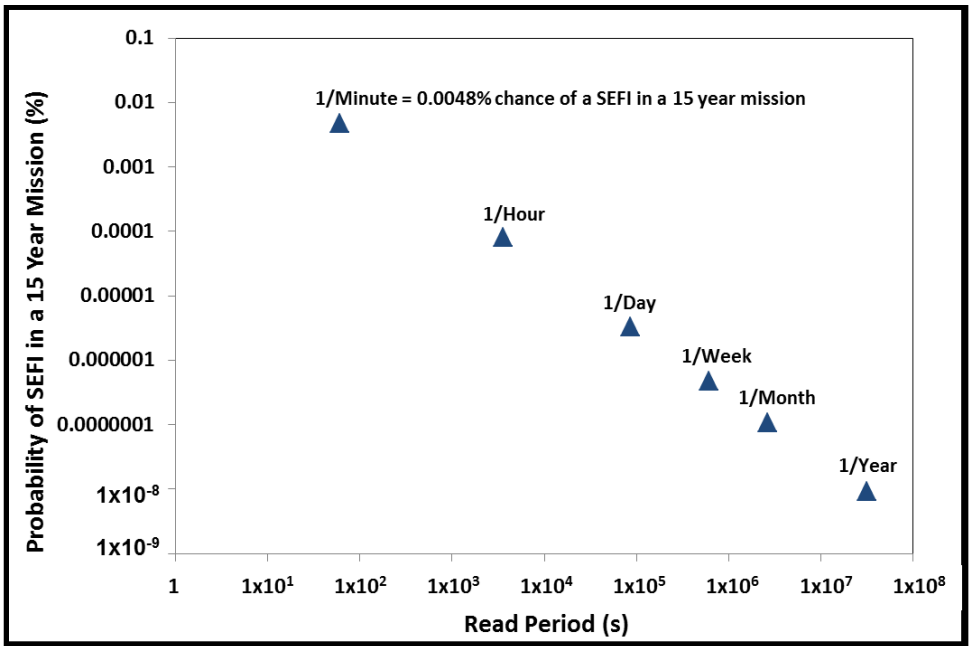

Figure 3: SEFI Probably vs Read Period

3 Device Level SEFI Recovery

The focus of this section is to provide insight into a simple, device level, SEFI recovery scheme in the rare event a SEFI event occurs. The temptation may exist among system designers to design one of many interactive detect and recovery schemes to overcome an MRAM SEFI event; however, the MRAM device has a simple feature that will overcome any SEFI event.

The MRAM devices have a sleep/reset mode pin (ZZ/RST) which enables the user to either put the device into sleep mode to save power or to reset the device. In the event of a SEFI, a toggle of the sleep/reset mode pin (ZZ/RST) clears the SEFI event, allowing complete recovery of device operation.

4 System Level SEFI Detection Schemes

The purpose of this section is to provide the reader with high-level, simple methodologies for system level SEFI detection and recovery. Although many techniques exist, Aeroflex proposes four simple solutions. These solutions include utilizing a watchdog timer, Reed-Solomon architecture, checksum, and/or redundancy. The selection of which scheme to use depends on the system application. Section 5 will discuss which scheme(s) best suit specific applications.

4.1 Watchdog Timer

The simplest recovery scheme is to employ a watchdog-timer. Such a system detects a system-level failure and triggers a toggle of the MRAM ZZ/RST pin in order to reset the device and clear any SEFI mode. The implementation of this recovery mode is simple in terms of hardware, and therefore, typically requires minimal power, real estate, and design complexity. A typical design includes a watchdog timer to monitor the hardware and a reset control mechanism such as a power supervisor. There are numerous devices that a user can select for monitoring purposes.

Aeroflex offers a new family of voltage supervisors. These devices have many applications; however, for MRAM SEFI recovery, the devices function as a fault monitor and power-on reset controller. These devices also easily interface with microprocessors, microcontrollers, FPGAs, ASICs, or DSPs, and many more resettable devices.

4.2 Reed-Solomon EDAC in 32-bit + 16 Check Bit Architecture

The Reed-Solomon (RS) code is able to detect and correct multiple and consecutive errors in a data structure. To detect and recover from an MRAM SEFI mode, a system designer can use an RS codec, complimentary to the x8 MRAM, that uses a 16-bit checksum with each 32-bit word making it capable of correcting an entire byte in the word (i.e. 1 MRAM experiencing a SEFI event). The RS codec detects uncorrectable error conditions so the host can make appropriate corrective actions. Again, power-on-reset circuitry or software can enable the MRAM ZZ/RST pin to toggle in order to reset the device and clear all SEFI modes.

4.3 Checksum

A variety of checksum algorithms exist with increasing fidelity, security, and complexity. The three most common categories are parity byte or parity word checksums, modular checksums, and position-dependent checksums. Unlike Reed-Solomon coding, checksum coding is a "detect only" method that does not attempt to correct the errors that occur.

The parity checksum word is the XOR of each bit position within every word stored. The simplest method of detecting errors in memory is to utilize parity checks. This method counts the number of logic one states occurring in a data path. Parity, usually a single bit added to the end of a data structure, states whether an odd or even number of ones were in that structure. This method detects an error if an odd number of bits are in error, but if an even number of errors occurs, the parity is still correct.

The modular checksum word is a 2's complement of the total sum, without overflow, of every word stored.

Position-dependent checksum is a modified summation of the binary value of each word written, but it also considers the word's position in the sequence. Popular position-dependent checksums include Fletcher's Checksum, Adler-32, and Cyclic Redundancy Checks (CRCs).

Figure 4 shows two flow charts that describe an MRAM modular checksum application. The flow on the left describes the algorithm for generating the checksum, while the checksum verification algorithm and associated error recovery method is on the right.

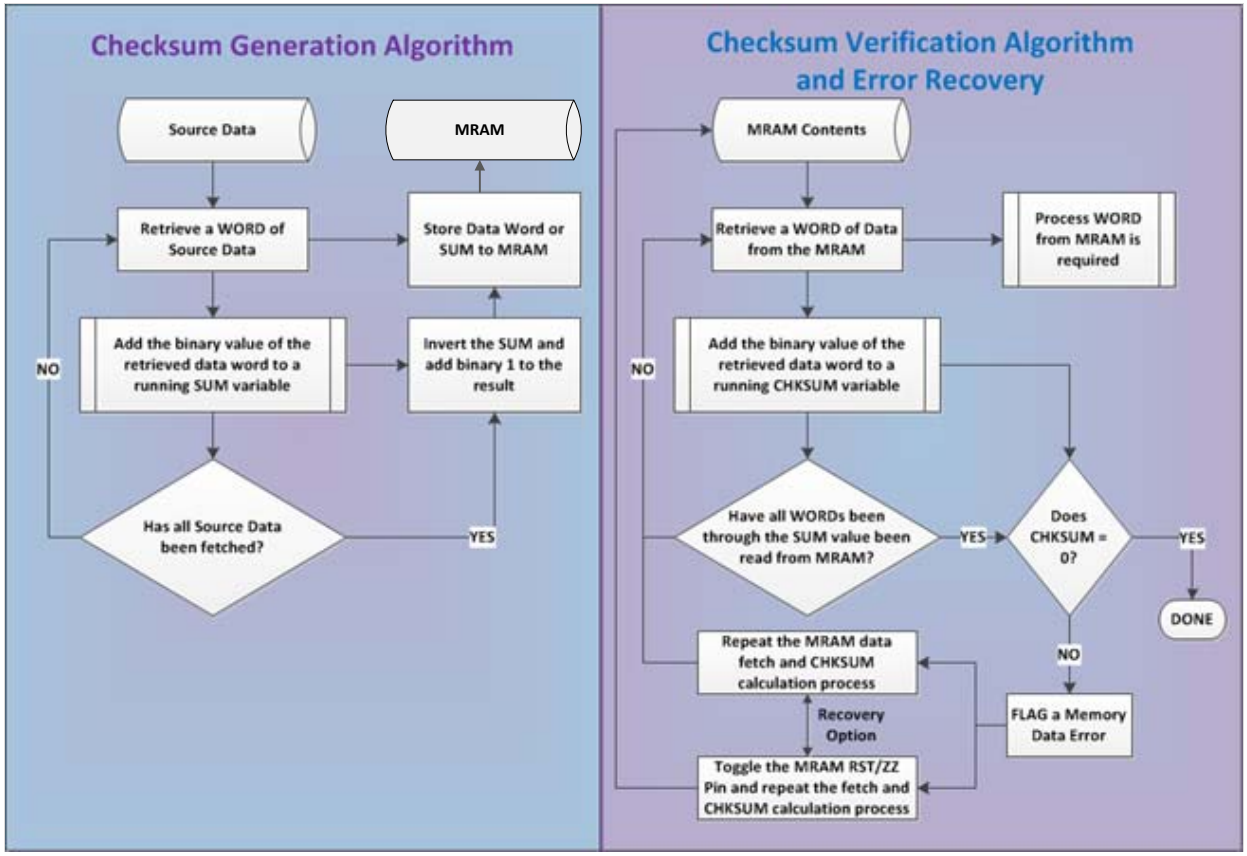

Figure 4: Modular Checksum Generation and Verification Algorithm Flow Charts

4.4 Redundancy

The final SEFI detection scheme is a simple method of error detection that uses a redundant memory of the same size as each memory used to store the primary data. The implementation of this solution is controllable entirely by software. This method is easier and less costly than triple mode redundancy (TMR), but cannot correct the error on its own. Figure 4 shows an example flow diagram of how memory redundancy works.

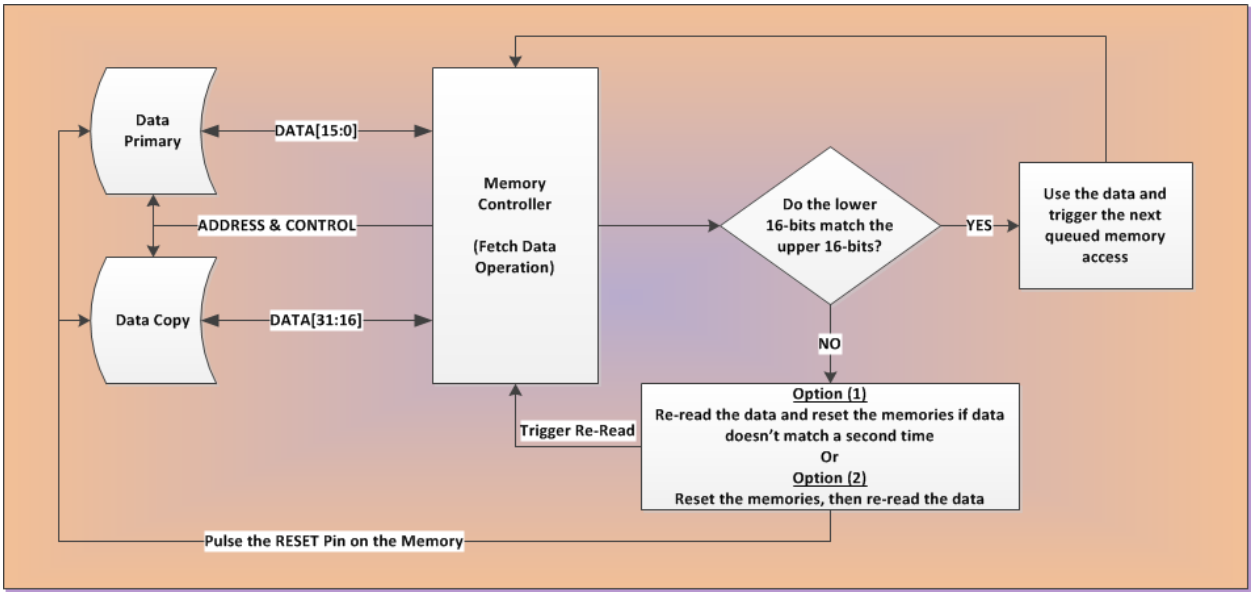

Figure 5: Memory Redundancy Flow Diagram

5 SEFI Detection and Recovery Solution(s) by Application

To determine the optimal SEFI detection scheme for the MRAM device, the user must ask the following questions:

- How will the memory be used?
  - Code, Static Data, Variables, Lookup Table, etc.
- How will the SEFI manifest itself within the system?
- What error handling facilities are available to the system designer?
  - Hardware, Software, Architecture, etc.

Table 5 cross-references the three most common application spaces to the various SEFI detection and recovery solutions. Only one SEFI solution is necessary for any given application. The system design should determine which approach is best suited to their application.

Table 5: SEFI Detection Solution(s) by Application

	Processor / FPGA Boot-Up and Code Execution	Configuration / Calibration / Large Data Sets	Random / Highly Variable / Small Data Sets
Watchdog Timer	**X**		
Reed-Solomon EDAC Architecture	**X**	**X**	**X**
Checksum		**X**	
Redundancy		**X**	**X**

6 Conclusion

Data errors that will overcome basic parity and BCH level error detection schemes are very common throughout the electronics industry. Every reliable system must include accommodations for information errors; therefore, a systematic error handling liability exists regardless of the memory selected.

The occurrence of a SEFI is extremely low with Aeroflex MRAM devices. In the event that a SEFI occurs, there is a simple device-level recovery solution and four system level detection schemes to assist in clearing all SEFI modes. Many more fault detection and recovery techniques exist. The essential issue is that system designers should always consider how their systems would detect and recover from a large data error.