SEAKR ENGINEERING, INC.
AEROSPACE MEMORY SYSTEMS
23763 Madison St.
Torrance, CA 90505
(213) 375-2972

FAULT TOLERANT TECHNIQUES

FOR

SPACECRAFT DATA RECORDERS

SCOTT R. ANDERSON
VICE PRESIDENT

FAULT TOLERANT TECHNIQUES FOR SPACECRAFT DATA RECORDERS

ABSTRACT

This paper presents the techniques for improving system reliability which SEAKR Engineering employs in the design of their spacecraft solid state data recorders. Briefly, these techniques include Hamming code error correction, periodic memory scrubbing, latch-up protection, excessive capacity, redundant power supplies/control/bus circuits, microcode protection, and shielding.

INTRODUCTION

The frequent failures of mechanical tape recorders in space applications have shown the need for improved data storage products. In addition, the cost of a Flight quality tape unit and the problems associated with its torques and momentums contribute to the desire for alternatives. Fortunately, the capabilities of todays semiconductor memories provide the means for resolution of these problems.

Earlier studies[1-4] indicated potential methods for employing non-rad hard memory technologies in the construction of memory systems tolerant of the natural radiation environment of space. Building upon the strategies suggested in these papers SEAKR Engineering has constructed and delivered a Flight Qualified solid state memory system to a DoD program. This paper presents the design philosophy used in this system design and the techniques used to increase reliability.

SYSTEM DESIGN PHILOSOPHY

There are two approaches to providing radiation tolerant solid state memory systems. The first and most expensive is to custom design and manufacture the system's memory components in a radiation hard process. Much effort and funds have been allocated to this goal resulting in the availability, at time of this paper, of volume quantities of 64 Kbit static RAMs and smaller quantities of 256 Kbit static RAMs.

For small capacity systems, under a few MBytes, these densities are workable and can produce competitive data recorders. However, with these devices costing more than several hundred dollars each, large capacity recorders become prohibitively expensive. A more attractive alternative

is to use relatively inexpensive bulk CMOS devices and clever system design to provide system level radiation tolerance.

This approach has been discussed in earlier papers and is being employed in the Mars Observer Camera[5]. SEAKR Engineering's data recorders apply a hybrid of this approach using bulk CMOS devices for the memory array and radiation hard CMOS SOS for the system control circuits. Since the majority of devices in a solid state recorder are memory devices, this provides a significant cost reduction over a full rad hard design while providing the most crucial nodes of the system with guaranteed radiation immunity.

The memory technologies of choice for a spacecraft recorder design today are Dynamic Random Access Memories (DRAMs), Static Random Access Memories (SRAMs), and Electrically Erasable Programmable Read Only Memories (EEPROMs). Due to the need for a periodic refreshing of the data stored in a DRAM and the higher susceptibility of DRAMs to ion induced SEUs, DRAMs are the more difficult to use and present greater problems in the natural radiation of space. However, their lowest cost and highest capacity, typically four times that of the highest density SRAM or EEPROM, make their use attractive - provided that their problems can be overcome. In addition, since the other two technologies are easier to use than DRAMs are, a system design supporting DRAMs can be easily switched over to support the other two technologies.

RADIATION AND FAULT TOLERANCE

TOTAL DOSE IONIZING RADIATION

As demonstrated by JPL[5] some DRAMs are very tolerant to total ionizing radiation. Proper selection of the DRAM used in the memory array plus the exclusive use of radiation hard components for the rest of the system's microelectronics provides significant confidence in the survivability of the system. The inclusion of shielding in the recorder housing can provide functionality up to several hundred kilo rads of ionizing radiation.

IONIC PARTICLE INDUCED UPSET

System tolerance to ionic induced SEUs is more difficult to obtain. Since SEUs have different effects when they occur in different parts of the system, the system design will require different strategies to survive them. Removal of SEUs from the memory array section of the system

is achieved through the use of EDAC circuits, redundancy, periodic memory scrubbing, and thoughtful memory array architecture.

The EDAC design employed uses a common 16/6 modified hamming code which can detect multiple erroneous bits plus correct one single bit error in a 16 bit data word. As data is written into the memory array the EDAC circuitry generates 6 check bits per 16 data bits which become part of a 22 bit code word. These check bits assist the EDAC circuitry in identifying any erroneous data in a code word.

Since multiple errors in a code word will cause the EDAC to fail and since one ionic particle has sufficient energy to upset numerous bits within the same chip it is necessary to distribute the code word throughout several unique devices, one bit per device. While this means more words will have erroneous bits per particle hit, it will limit each word to only one incorrect bit *[1]. Passing these words through the EDAC circuitry will subsequently remove all erroneous bits.

An additional benefit of this approach is the tolerance to hard failures which is obtained. Since the EDAC employed will correct all erroneous bits per word and since only one bit per word is stored in the same device, the system can continue to function even after losing an entire chip. Through software techniques (described in detail by Bob Nelson[15] and National Semiconductor Applications Note-306) SEU tolerance is still maintained providing graceful failure to the system.

This approach has a final benefit in that if a SEU or transient occurs in an on-chip address buffer or latch, then only one chip will be effected and the error will appear as single bit in nature and can be corrected *[2].

While SEAKR Engineering's memory system can be used for random access or data buffer FIFO applications its primary market is the replacement of mechanical tape recorders. It therefore must be able to maintain data integrity for lengthy periods of time before being dumped and subjected to the EDAC circuitry. This system usage raises the possibility of accumulating multiple errors in a single word due to independent events separated in time. Our solution to this problem is commonly referred to as memory scrubbing. By periodically reading all memory words in the system and correcting all SEU errors, the probability of accumulation of multiple SEUs is decreased.

*[1] NOTE: there is a finite possibility of a single particle passing through multiple chips. This may cause multiple upsets per data word and subsequently the failure of the EDAC design. However, there is very little data to support what the probability of this occurrence is. Feedback from this recorder's operation during orbit will be presented at the next annual symposium and will hopefully shed some light on this possibility.

*[2] NOTE: This is in contrast to designs which attempt to store whole words in one chip and second guess how a single particle will effect the stored word. In this competing approach the single bit error correction capability is based on the prediction of how a single particle upsets a group of bits in the vicinity of the impact. By distributing entire words throughout a single chip such that only one bit of any word is within the maximum predicted perimeter of impact, a single bit error correction scheme can be used to clear all error in the entire chip. The fallacy of the approach is that if an event occurs in any address register or buffer during a write operation good data will have been written into a wrong location. In this event not only will data be transmitted out of sequence but the system, and thus the user, will be ignorant of the fault.

IONIC PARTICLE INDUCED LATCHUP

While the prospects of a Single Event Latchup (SEL) due to the nuclear particle environment of space are remote, laboratory tests have indicated the possibility. Predicted SEL rates for AT&T 1 Mbit DRAMs in the radiation environment around MARS have been obtained which indicate that at worst this is 8.34x10E-5 SEL/device-day.[6] A system comprising 1000 devices in a Martian orbit can be expected on average to experience a SEL once every 12 days.

To prevent catastrophic failure due to the elevated ICC current associated with a latchup condition, SEAKR Engineering employs the common technique of current limiting and power strobing. Current limiting resistors on each chip hold any ICC current to below the level of damage while solid state relays provide the ability to remove power to any suspect memory board.

Activation of the power strobing is initiated by the memory system's embedded computer. If during the operation of the memory system a fault indicative of a latchup is identified on a memory board, then the system will transfer the contents of this board via the EDAC circuitry to an empty board reserved for this purpose. The power to the board in question is now cycled resetting any latchup condition. The contents of this board are now reloaded removing any effect of the latchup.

MEMORY ARRAY RELIABILITY

The reliability calculations of the memory array are dependent on the assumption that all single event upsets are a Poisson process. Namely, they are constant and independent of past history. Using the definition of the failure of the memory array to be when it transmits a single bit error, the reliability P(t) becomes the probability that no single word in the memory array has a multiple incorrect bit at time t.

With the following definitions

R = failures/bit-day
f = failures/bit-sec = R/24*3600
t = time data is stored in seconds
T = scrubbing interval in seconds
w = data bits/word = 16
c = check bits/word = 6
m = memory size in number of words, an integer
n = number of scrubbing cycles during t, an integer
r(t) = reliability of a single word at time t
P(t) = reliability of the memory array at time t

The reliability of a single bit error correcting word with (w+c) bits is the probability that either all (w+c) bits are correct, or that only one bit is incorrect. For a Poisson process with the reliability of a single bit defined as e^{-ft} a word reliability is[1]:

$$r(t)=e^{-(w+c)ft}+(w+c)(1-e^{-ft})e^{-(w+c-1)ft}$$

and the entire memory reliability becomes $[r(t)]^m$. The function of memory scrubbing is to effectively make the memory array error free at the conclusion of the scrub action. Thus, the reliability of the memory array during the first scrub period is the same as the reliability of the system in the second scrub period. Therefore, the reliability of the system at time nT is the probability that it survives each of the n scrub periods. For t=nT the entire memory array reliability becomes:

$$P(nT)=[(r(T))^m]^n$$

and for all time,

$$P(t) = [(r(T)^m]^n[(r(x))^m]$$
for $t = nT + x$, $0<x<T$; $n>0$; and n an integer

Any failure of the memory system EDAC due to SEU is not permanent and will become visible as a temporary transmission of erroneous data measurable as a bit error rate (BER). Unlike mechanical tape recorders whose BER is dependent on the amount of data transmitted, a solid state recorder BER will be dependent on size, SEU rate, memory scrub period, and the length of time during which data is stored.

As an example, consider a solid state system with a 10E9 bit memory capacity and a data storage period of one day. t therefore becomes 86,400 seconds and the system capacity in words is m = 4.55x10E7. SEAKR Engineering's current design of the memory system will allow this capacity to be scrubbed in approximately 32 seconds, thus T becomes 32 seconds.

An expression published by Petersen et al. for the prediction of a bit error at geosynchronous orbit for a microelectronic circuit, in upsets per bit-day is R=5x10E-10 x $Q/(L)^2$.[8]

Q is the experimental upset cross section [um^2/bit]; and L is the linear charge deposit threshold [pC/um]. Relying on the results obtained by JPL for the AT&T 1 Mbit DRAM a cross section is found to be .353cm^2/bit and a LET of

2MeV/(mg/cm^2).[6] These are converted to 56um^2/bit and .02pC/um through a change of units. This gives R=7x10E-5 SEU/bit-day and f=8.1x10E-10 SEU/bit-sec.

Inserting these figures into the equation above, the reliability of the memory array becomes P(t)=P(day)=0.9811147413. This figure is the reliability of the memory system dumping its entire contents without one single bit in error due to cosmic particle induced upset. Since this reliability figure is calculated for one day, the reliability of the system for several years becomes $P(t)=[P(day)]^X$ with X being mission duration in days. This equation shows that for any mission duration longer that a few days the probability that the memory array will fail becomes significant.

However, the reliability of the system can be improved by lowering the criteria for system failure, namely the BER. If we approximate the effective failure of the EDAC circuit to be the transmission of two erroneous bits per failure, then one failure will give the system a BER rate of 2x10E-9 or less. A BER of 4x10E-9 would allow the EDAC circuit to fail twice and a BER of 6x10E-9 would allow three failures. For a BER of 1x10E-8 the EDAC could fail 5 times and has the probability of occurrence in one day of approximately:

$$P_{fail}=[1-P(day)]^5$$

This leads to a probability of successful operation of the memory array (BER $\leq$ 1x10E-8) for a one year mission of:

$$P_{sucess}= (1-[1-P(day)]^5)^{365} = 0.99999912$$

for a six year mission the probability becomes:

$$P_{6\ years} = 0.9999947$$

CONTROL CIRCUITS

Up to this point this paper has been focused on the error prone, radiation soft, memory array. All reliability calculations have been based on the assumption that the control circuits will function as intended. Strategies taken to assure this include thoughtful part selection, an SEU immune address protection scheme, microcode protection techniques, and majority triplication circuits for all command and control registers.

PART SELECTION

To guarantee the successful operation of the memory system's control circuits to the natural ionizing radiation of space, all control circuits have been carefully selected. These parts have all been chosen from the limited selection of specifically designed, radiation hard, CMOS parts or from approved NASA standard parts lists. All of these parts, without any shielding, have been shown to be insensitive to the exposure of over 100,000 rad of ionizing radiation. BERs are 10E-10 SEU/bit-day or less except for the ASICs which are 10E-6 SEU/bit-day.

The control circuits include the system's microprocessor, data buffers, program memory, scratch pad RAM, EDAC circuits, I/O circuits, gate arrays, all address bus drivers, and all data bus transceivers. These devices are all manufactured on a latchup immune process such as SOS or EPI layer isolation.

ADDRESS PROTECTION

Innovative features which SEAKR Engineering has incorporated into the recorder design are focused on the prevention of any SEU from causing incorrect memory system operation. Even thou circuits are employed in the control registers and address drivers which are extremely insensitive to SEU it is still possible to experience a cosmic ray induced transient.

This occurrence, when in an address register or on a write line, can result in correct data being written into the wrong storage cells; possibly overwriting previously stored data. Or, if the system is in an output mode of operation, data may be transferred out of sequence. This problem is the Achilles heel of any solid state memory system and one which is frequently overlooked. Since it is impossible to eliminate the possibility that an SEU may occur, the solution to this problem lies in detection of occurrence and then correction of the effects.

In this design, detection is accomplished by feeding the address present at the DRAMs back to the control circuits and comparing this with the address sent out. Any transient or fault encountered in any address driver, either going or returning, will be detected. By using two independently loaded address counters, one primary counter which sends out the address and one secondary counter used for comparing the fed back address, a bit flip in either one

will be detected alerting the embedded computer. Independent load requirements prevent any SEU from ever effecting both registers simultaneously and identically.

All operations to the memory array are halted at the detection of any fault in the address checking scheme. In an ideal universe with the address comparison instantaneous no data would be transferred to or from the memory array without the correct address being present. However, in our real world with finite delays in transmission and comparison circuits it is possible to have an upset and not detect occurrence until after sending a read or write pulse.

Solution of this problem is simplified by the multiplexed address design and page operation of a DRAM. In a DRAM, two address are required to select a bit the first, RAS, selects a row or page in the device and the second, CAS, selects the individual cell of this page to read or write. Since the device is unreceptive to read or write pulses during the RAS address strobe, latent detection of an erroneous RAS address presents no problem. Retransmission is initiated clearing any DRAM of an incorrect RAS address.

After a known good RAS address has been loaded into the DRAMs then an entire page of data can be transferred by incrementing the address and pulsing the CAS line. This operation is susceptible to the problem described above; however, any error is now bound to the one page in the DRAM devices identified by the previous RAS address. By designing the I/O buffers and address counters for full page block operation a retransmission of any page will remove the failure and be transparent to any user.

Due to the fact that SRAMs are not page oriented and have all addresses present at the time of a read or write operation, solution to this problem can only be obtained through the reading and writing of the device in its entirety. This seriously complicates the I/O buffer requirements of any system based on SRAMs.

MICROCODE PROTECTION

In any microprocessor based system, the proper program execution depends on the error free operation of the next instruction fetch cycle. An upset in the next instruction address calculation will cause the program to execute unintended instructions. This type of upset can be caused by one or more bit flips in a hardware register called the Program Counter (PC). These upsets can be brought about by transients and high energy particles.

Due to this possibility, it is important that the actual valid program code have built-in ways to detect and correct invalid program operation. SEAKR Engineering recognizes the susceptibility of embedded control programs to these error sources and takes the following steps to reduce the probability of malfunction:

1. Use a structured programming format which will allow individual modules to be tagged with an ID code. Periodically checking the ID code against the known correct value will give confidence that the program counter has not forced a jump to another block.

2. Triplicate operation sensitive variables in rad hard RAM. Periodically a background routine will execute to compare the main variable with one of the copies. If the copy is identical, the value is written into a third location. This third copy of the variable will be used if ever the first two do not compare. When this occurs, the first two variables are rewritten to match the third. This technique protects the program from ever using a variable that has experienced a bit flip in RAM or was incorrectly stored in the RAM.

3. Periodically repeat control instructions such as Enable Interrupts and the loading of external command registers.

4. Fill unused memory locations with a value equal to a Software Interrupt instruction. If program execution improperly strays into this region, the Software Interrupt code will be encountered and an internal interrupt processing sequence will be initiated. The routine will perform the steps necessary to determine where the program went astray and will recover to that level.

5. Protect unused address locations outside of program memory. If the data bus is equipped with the proper loading resistors to emulate the interrupt code, any illegal access to an address not decoded into either program memory or as an input will return the desired interrupt code when the bus floats during the fetch cycle. Considering that our embedded control program does not use the bulk of the available address range, this simple method plus 4. above provides a good deal of protection.

6. Include a resettable watchdog timer circuit that can interrupt or reset the processor. Because it is possible for unintended program loops to disable interrupts it is better to use a Non Maskable Interrupt or to actually toggle the RESET line and reset the entire system.

The concept is to set the delay on the timer to be slightly longer than an anticipated program sequence. At the beginning and end of the sequence, the timer is reset. If an unintended loop occurs, the timer will time out and interrupt the processor. A programmable timer can therefore be useful. The time delay can be modified for optimum response for different length program sequences. Due to the possibility of SEU in a programmable timer, however, a safer approach is to use a hardware timer with only a single RC time delay that remains fixed. The program must then make sure to reset it often enough to avoid a time out.

7. Set up the memory map so that all of the output ports/latches overlap with RAM. This way whenever the latch is loaded there will be an identical map of the data that was on the bus in RAM. This will not guarantee that the latch was loaded properly but it will detect if the data byte sent out was as intended.

HARDWARE TRIPLICATION

The last technique which is employed in the system design to reduce susceptibility to SEU induced failures is to triplicate all command registers and latches. Requiring the system microprocessor to load each redundant part of the registers three times and selecting the majority to follow will prevent any SEU from upsetting the command registers and causing improper system operation.

REFERENCES

1. Jacob A. Abraham, Edward S. Davidson, Jamal H. Patel, "Memory system design for tolerating single event upsets", IEEE Transactions on Nuclear Science, Vol. NS-30, No. 6, pp 4339-4344, Dec 83.

2. John P. Retzler, "Fault tolerant memories for single particle radiation effects", IEEE Transactions on Nuclear Science, Vol. NS-28, No. 6, pp 3998-4003, Dec 81.

3. J. B. White, Jr., "Fault-tolerant memory system architecture for radiation induced errors", IEEE Transactions on aerospace and electronic systems", Vol. AES-18, No 1, pp 39-47, Jan. 82.

4. William K. S. Walker, Carl-erik W. Sundberg, Colin J. Black, "A reliable Spaceborne Memory with a single error and erasure correction scheme", IEEE Transactions on computers, Vol. C-28, No. 7, pp 493-499, July 79.

5. D. K. Myers, A. S. Danziger, T. A. Soulanille, "Radiation tolerant memory section for the Mars observer camera", IEEE Transactions on Nuclear Science, Vol. NS-34, No 6, pp 1467-1469, Dec 87.

6. JPL interoffice communication, "Expected bit error rates for the Mars observer camera", SMB #1, pp 1-8, May 10, 1988.

7. J. A. Zoutendyk, H. R. Schwartz, R.K. Watson, Z. Hasnain, L.R. Nevill, "Single-event upset (SEU) in a DRAM with on-chip error correction", IEEE Transactions on Nuclear Science, Vol. NS-34, No 6, pp 1310-1315, Dec 87.

8. E. L. Peterson, J. B. Langworthy, S. E. Diehl, "Suggested single event upset figure of merit", IEEE Transactions on Nuclear Science, Vol. NS-30, No 6, pp 4533-4539, Dec 83.

9. K. Soliman, D. K. Nichols, "Latchup in CMOS devices from heavy ions",IEEE Transactions on Nuclear Science, Vol. NS-32, No. 6, pp 4514-4519, Dec 83.

10. D. D. Huffman, "Prevention of radiation induced latchup in commercially available CMOS devices", IEEE Transactions on Nuclear Science, Vol. NS-27, No. 6, pp 1436-1441

REFERENCES CONTINUED

11. J. G. Tront, J. R. Armstrong, J. V. Oak, "Software techniques for detecting single-event upsets in satellite computers", IEEE Transactions on Nuclear Science, Vol. NS-32, No. 6, pp 4225-4228, Dec 85.

12. B. W. Johnson, "Fault-tolerant microprocessor based systems", IEEE Micro, pp 6-20, Dec 84.

13. D. R. Ballard, "Designing fail-safe microprocessor systems", Electronics, Jan 4, 79.

14. M. Y. Hsiao, A. M. Patel, D. K. Pradhan, "Store address generator with on-line fault-detection capability", IEEE Transactions on Computers, Vol. C-26, No. 11, pp 1144-1147, Nov 77.

15. B. Nelson, "Simplification of 2-bit error correction", Computer Design, Jan 82.