Application Note

SRAM 中的错误检测

Peter Ehlig and Salvatore Pezzino

摘要

本应用报告提供了有关 SRAM 电路如何发生故障以及可以采取哪些应对措施的信息。目标读者是对提高系统稳健性感兴趣的电子系统开发人员或集成商。本文档是从研究半导体 SRAM 实例故障的角度编写的。

内容

1 引言和范围....2
2 SRAM 位阵列....2
3 SRAM 故障来源....3
3.1 制造缺陷....3
3.2 电路随使用次数的增加发生漂移....3
3.3 电路过应力....3
3.4 软错误....3
4 用于管理电子系统中存储器故障的方法....5
4.1 启动测试....5
4.2 系统内测试....5
4.3 奇偶检测....5
4.4 检错与纠错 (EDAC)....6
4.5 冗余....6
5 比较和结论....6
6 C2000™ 存储器类型示例....6
6.1 TMS320F2837xD....6
7 存储器类型....7
7.1 专用 RAM (Mx 和 Dx RAM) 7
7.2 本地共享 RAM (LSx RAM)....7
7.3 全局共享 RAM (GSx RAM)....7
7.4 CPU 消息 RAM (CPU MSGRAM)....8
7.5 CLA 消息 RAM (CLA MSGRAM)....8
8 总结....8
9 参考文献....9
10 修订历史记录....9

表格清单

表 2-1. SRAM 位阵列....2
表 5-1. 检测机制和保护级别....6
表 7-1. 存储器类型....7
表 7-2. 对 LSx RAM 的主访问 (假设已禁用所有其他访问保护) 7
表 7-3. 对 GSx RAM 的主访问 (假设已禁用所有其他访问保护) 8

商标

1 引言和范围

当今世界高度依赖电子控制和管理，因此人们开始关注电子操作的安全性。一个关键的关注点是系统中 SRAM 的运行。这非常重要，从某些角度而言，这是电子产品运行安全最重要的一个方面。原因如下：

- SRAM 是整个器件中的一个大型元件，通常是最大的元件。
  - 占用面积最大
  - 包含的晶体管数量最多
- SRAM 是非常密集的电路，因此容易受到干扰或细微缺陷的影响。
- SRAM 的工作电压范围比正常电路逻辑低，因此容易受到干扰。

由于这些原因，SRAM 位单元和阵列布局对于任何新集成电路工艺开发和验证都是关键组成部分。在制造过程中，集成电路制造专家致力于寻找 SRAM 位单元和阵列布局的漂移和变化。因此 SRAM 错误检测对于安全相关电子产品而言非常重要。如果您想跳到结尾部分，请参阅节 8。

本文的内容如下：

- 节 2：SRAM 位阵列组织概述
- 节 3：SRAM 故障机制摘要（包括每种机制的关注点）
- 节 4：可用于管理电子系统中存储器故障的方法
- 节 6：特定于 TMS320C2000 产品的内容

2 SRAM 位阵列

信息以字的形式存储在 SRAM 中。字长因存储需要而异。本文中使用 32 位字。字的位存储在位阵列中。不过，各个位的物理位置都针对半导体工艺的细节进行了优化。阵列是具有行和列的矩阵。在下面的示例中有 N 行，每行包含 8 个字。如果 N = 256，则该阵列为包含 256x8x32 = 65,536 个位或 2048 个字的 SRAM。

请注意，单个字的各个位在物理上是不相邻的，但 1 个 D 输入/Q 输出的所有位都是相邻的。单个字的各个位在物理上与其他字相隔 7 位。这改善了物理阵列的大小和 D/Q 信号的路由。稍后您将看到这是如何提高多位故障机制的错误检测能力的。

下面显示了三个字中的值：

```
Word(0) = 1 … 0 1b     Row0, Column0
Word(1) = 1 … 1 0b     Row0, Column1
Word(7) = 1 … 0 0b     Row3, Column7
```

表 2-1. SRAM 位阵列

			D0					D1					D31			
行	Col															
	0	1	2	…	7	0	1	2	…	7	0	1	2	…	7	列
N-1																
…																
5																
4																
3					0					0					1	
2																
1																
0	1	0				0	1				1	1				

阵列中位单元的物理组织可能因多种原因而有所不同，但该图提供了一个很好的讨论示例。该示例显示了一个值为 8 的列多路复用器因子，这意味着对于每个 Q/D，一行中有 8 个位。在执行存储器读取时，会选择行，然后列地址提供有关哪个特定的位将从 Q 中输出的解码信息。在执行存储器写入时，列解码具体定义将对所选行中的哪些位进行写入。每个 D/Q 的子阵列 (256x8) 被称为棒。

较大的存储器阵列通常使用较高的列多路复用器因子进行组织。

3 SRAM 故障来源

本节从系统设计人员或集成商的角度总结了 SRAM 故障的多种来源。

3.1 制造缺陷

本文不打算详细介绍半导体器件制造过程中产生的缺陷。SRAM 是一种非常普遍、密集和敏感的电路，在半导体器件测试中受到了极大的关注。测试环境包括高级且通常是专有的测试算法。制造测试环境允许使用在终端系统中不可能出现的电压/温度/频率裕度进行测试。半导体器件设计包括专门的测试模式，以允许制造测试包含进一步的裕度测试。

3.1.1 时间零点故障

由于生产测试中的特殊算法导向和广泛的裕度，在器件集成到系统中之前就涵盖了时间零点缺陷机制。在成熟的半导体工艺中，大多数缺陷 (>98%) 是通过常规 March 算法（例如 March13n）捕获的。在更先进的工艺节点 (<65nm) 中，需要使用更先进的算法才能实现这一点。

3.1.2 潜在故障

潜在的制造缺陷是半导体结构中的材料弱点，该弱点可能会导致系统故障，但可能会被上述算法和裕度测试遗漏。制造压力测试专门针对这种结构性弱点，它可以在发送器件之前强制使故障显现。

3.2 电路随使用次数的增加发生漂移

半导体的性能会随着时间的推移而漂移，最终可能发生电路故障。器件数据表定义了器件的寿命。会通过具有裕度的速度路径分析对器件设计进行验证。会使用足以在指定的寿命期间正常运行的裕度对器件进行测试。裕度测试和裕度设计最佳实践专门用于解决 SRAM 的性能漂移问题。

3.3 电路过应力

数据表明确定义了器件的工作电压和温度限值。如果器件承受超出数据表中定义的应力，则指定的寿命会缩短。极端的应力会损坏器件。有时造成的损坏是容易识别的故障，但有时故障不易觉察。过压或高温应力尤其影响 SRAM 的运行。

3.4 软错误

在本报告的上下文中，软错误是指由 SRAM 阵列外部的事件引起并且不会损坏 SRAM 电路的 SRAM 故障。软错误是临时的，因为将新值写入受影响的字后，错误便不再存在。此类故障的两个来源是穿透电路的放射性粒子和读取或写入字时的动态电压噪声。

随着半导体几何尺寸的减小，软错误变得更加常见。这既是因为各个位相互靠得更近（可创建目标更丰富的环境），又因为电压电平较低，从而导致位单元存储的稳健性较差。

仅当系统在受干扰的字被写入之前读取了该字时，软错误才会影响系统。某些 SRAM 内容在本质上是静态的，例如代码或表。其他 SRAM 内容是动态的，例如传入的数据和变量。此外，许多对数据进行操作的算法对单个位错误具有很好的适应性，尤其是在错误位于较低有效位的情况下。因此，动态数据中由于软错误导致的故障率比静态使用 SRAM 时低得多。在许多系统中，代码和表存储在非易失性存储器（如 ROM 或闪存）中，而 SRAM 主要用于动态存储。

3.4.1 放射性事件

放射性事件源自放射性粒子穿透半导体材料并扰乱位单元锁存器中的电压。这些事件在正常情况下是罕见的，但在放射性医疗环境和/或非常高的海拔环境中发生的可能性较大，高海拔环境中的大气较少，不利于降低粒子数。

根据粒子的穿透角度和强度，一个或多个位的值可能会翻转。这会沿一条直线发生。如果该直线穿过多个行，则必然会在不同的字中出现多个发生故障的位。这适用于垂直方向的穿透或对角线方向的穿透。

如果穿透方向是沿着行，则必须超出多路复用器因子才能在同一个字中创建多个位。

几何尺寸越小，受粒子穿透干扰的位就越多。在 90nm 工艺节点上，穿透 5 个单元的情况极为罕见。在 65nm 工艺节点上，穿透 6 个单元的情况极为罕见。与高性能工艺节点相比，低泄漏工艺节点更不易受这些事件的影响。

放射性粒子穿透可能会对 SRAM 单元造成物理损坏，并且这种情况时有发生。这种情况在采用结构更具创新性的几何形状的工艺节点中更为常见。

3.4.2 动态电压事件

任何涉及开关的电路都会发生动态电压事件，即使在集成电路上也会发生电压事件。例如，只要主系统时钟进行切换，许多其他晶体管都会转换，并且电源平面上会出现一些噪声。尽管半导体器件内的电压事件很小，但如果在对某个具有裕度的位单元进行读取或写入期间发生电压事件，则该位单元可能会受到干扰。不过，这些器件会使用足够的裕度进行测试，以筛选出此类位单元，因此这个问题并没有上升到系统层面。大到足以干扰具有裕度的位单元的电压事件来自芯片外部或源自器件的运行超出数据表规格。即便如此，电压事件也只会在较弱的位（由于正常和预期的过程变化而较弱）上发生。因此，单个位检测足以应对此类事件。

可能会由于显著的动态电压事件而发生多位读取或写入故障。这表明存在电压问题，最好通过电压监控而不是存储器监控加以解决。

3.4.3 错误来源总结

总之，系统内 SRAM 错误的主要问题是因节 3.4 中讨论的软事件而导致的干扰故障。

制造缺陷是通过仅在制造环境中可用的方法进行筛选的。如果未筛选出这些缺陷（这不太可能发生），则节 4 中的方法可提供额外的覆盖范围。节 4 中所述的方法还可以处理正常电路漂移导致的故障，当系统超出数据表器件寿命或出现轻微过应力时，电路漂移可能会成为一个故障因素。

4 用于管理电子系统中存储器故障的方法

本节介绍了多种可用于管理电子系统中存储器故障的方法。虽然本节的内容专门针对 SRAM，但大部分信息也适用于其他存储器，例如 ROM 和闪存。本节的内容是从系统设计人员或集成商的角度出发进行描述的，但也考虑了先前进行的与集成电路器件相关的讨论。

即使在安全注意事项的范畴内，针对存储器故障管理也存在不同的看待角度。

- 安全状态：当发现错误时，使系统进入安全状态。
- 系统可用性：在某些情况下，当发现错误时继续运行。
- 失效防护：即使已发现错误，系统也正常运行。

以上每一种角度都会增加系统成本。根据市场的要求，可以很容易证明额外的成本是合理的。或者，这些额外成本在其他目标市场中可能会令人望而却步。

4.1 启动测试

在启动时测试 SRAM 无法解决上述三个角度的问题。不过，即使在系统运行时无法进行测试，在启动时测试 SRAM 也会产生很大的附加值。

半导体行业达成共识，“在系统出现故障时，用户自行对系统进行下电已然非常糟糕，但更糟糕的是在自行下电后再对系统进行上电”。这是因为您无法完全管理系统（或系统元件）上电和下电期间的电压和电流摆动。器件在设计时已经考虑到了这个问题，但如果要发生破坏性电源事件，在上电/下电期间发生的概率更大。因此，在上电时测试 SRAM 可以解决最有可能损坏电路的问题。

此外，SRAM 在启动时更容易测试，因为系统上下文尚未加载，因此没有要保存和恢复的上下文。嵌入式 CPU 执行的 SRAM 测试需要大量的 CPU 周期，并且在与系统操作共享 CPU 资源的情况下无法轻松或有效地完成。

4.2 系统内测试

系统内测试涉及在系统完全运行时测试目标电路。这涉及占用 CPU 的一个处理时间片来测试电路的一部分。该时间片必须足够小，才不会影响 CPU 处理系统任务。在实时控制系统中，这可能具有限制性。从安全状态角度而言，必须在每个安全间隔内测试整个 SRAM 范围。

SRAM 的系统内测试涉及以下操作：

- 对目标 SRAM 进行上下文保存
- 对该 SRAM 运行 SRAM 测试算法
- 恢复该 SRAM 先前的上下文

此操作必须在系统要求访问被测 SRAM 之前完成。对于器件中的完整 SRAM 实例而言，很难做到这一点。不过，可以一次在一小片 SRAM（例如 16 或 32 个字）上执行此操作。如节 3.1.1 中所述，可以使用简单的 March 算法（March13n，或者甚至可以用 March7）来检测与缺陷相关的大多数系统内故障。在较新的工艺节点（45nm 或更小）中，需要使用更先进的算法来实现相同的覆盖范围。

该方法不会检测系统读取 SRAM 的故障，但可以在系统读取发生故障的位置之前捕获存储器中出现的错误。该方法用于没有其他检测方法来检测器件中的 SRAM 的情况。

4.3 奇偶检测

奇偶检测可识别读取访问中的单个位错误。在对 SRAM 字位置进行写入时奇偶校验电路会设置奇偶校验位，并在读回该字时验证该字中是否没有单个位错误。这是在读取/写入周期内完成的，因此不涉及 CPU 开销。如果奇偶校验电路识别出错误，会向 CPU 生成一个高优先级中断。

这种检测机制在半导体器件中实施起来较为简单且相对便宜。奇偶校验可以解决旨在实现安全性的安全状态角度问题。如前面节 2 和节 4.1 所述，几乎所有系统内 SRAM 故障都可能是每个字单个位故障。这适用于物理缺陷机制和软错误。另外，还可以通过使用奇偶校验保护存储器地址位来提供额外的覆盖范围。

4.4 检错与纠错 (EDAC)

错误检测和纠正（通常称为 ECC）比奇偶校验更强大，因为该功能可以纠正单个位错误。EDAC 电路还可以检测 2 位不可纠正的错误。可以实现 2 位纠正，但根据节 2 和节 4.1 的讨论可知，这样做带来的回报与增加的成本和时间开销并不匹配。

EDAC 解决了系统可用性（用于实现安全性）的问题，因为系统可在出现单个位错误的情况下继续运行，不受任何干扰。

不过，EDAC 具有以下缺点：

- 显著增加器件的存储器部分成本
- 由于动态纠正需要额外的 SRAM 访问时间，CPU 速度会变慢
- 需要更大的系统功耗

例如，考虑以下情况：

- 器件中的 SRAM 占用大约 1/3 的成本
- EDAC 导致 SRAM 的成本增加 30%
- EDAC 需要向存储器访问时间添加一个等待状态
- 器件的价格上升约 40%

并非所有 SRAM 都一定需要 EDAC 保护，因此是否需要 EDAC 因器件设计而异。同样，可以通过一些方法将访问时间减少到少于一个等待状态。

4.5 冗余

冗余是最昂贵的方式，但也是实现失效防护解决方案的最佳方法。可以在不同的级别实现冗余：

- 器件上的冗余逻辑
- 在锁步中运行的多个处理器
- 采用投票机制的多个处理器

该方法的复杂性会迅速增加，本文中不做进一步的讨论。

5 比较和结论

表 5-1 对何种检测机制提供何种保护级别进行了总结。

表 5-1. 检测机制和保护级别

SRAM 覆盖范围	启动	系统内	奇偶校验	EDaC	冗余
每个字单个位硬故障	是	是	是	是	是
系统内每个字单个位性能下降故障	否	可能 1	是	是	是
软错误	否	否	是	是	是
每个字多位	否	否	可能	是	是
安全状态	否	否	是	是	是
系统可用性	否	否	否	是	是
失效防护	否	否	否	否	是

1. 仅当系统内测试先于系统检查有故障的字时，系统内测试才会捕获该故障。尽管存在这种可能，但并不保证一定发生。

6 C2000™ 存储器类型示例

本附录讨论了 TMS320F2837xD 双核微控制器可用的保护级别。目的是帮助读者在为特定器件提供的文档中找到所需的信息。这是一款器件的示例。

6.1 TMS320F2837xD

有关 TMS320F2837xD 存储器类型的信息，请参阅 *TMS320F2837xD 双核微控制器数据手册*。该数据手册的*详细说明*一节包含有关器件的信息。节 7 包含数据手册的*存储器类型*一节中有关何种存储器涉及何种保护级别的信息。后续各节详细介绍了每种存储器类型。

7 存储器类型

表 7-1 提供了有关每种存储器类型的更多信息。

表 7-1. 存储器类型

存储器类型	支持 ECC	奇偶校验	安全性	休眠保持	访问保护
M0、M1	支持	-	-	支持	-
D0、D1	支持	-	支持	-	支持
LSx	-	支持	支持	-	支持
GSx	-	支持	-	-	支持
CPU/CLA MSGRAM	-	支持	支持	-	支持
CPU1/CPU2 MSGRAM	-	支持	-	-	支持
引导 ROM	–	-	-	不适用	–
安全 ROM	–	-	支持	不适用	–
闪存	支持	-	支持	不适用	不适用
用户可配置的 DCSM OTP	支持	-	支持	不适用	不适用

7.1 专用 RAM（Mx 和 Dx RAM）

CPU 子系统有四个支持 ECC 功能的专用 RAM 块：M0、M1、D0 和 D1。M0/M1 存储器是与 CPU 紧密耦合的小型非安全块（即只有 CPU 可以访问这些存储器）。D0/D1 存储器是安全块，还具有访问保护功能（CPU 写入/CPU 取回保护）。

7.2 本地共享 RAM (LSx RAM)

专用于每个子系统且仅可由其 CPU 和 CLA 访问的 RAM 块被称为本地共享 RAM (LSx RAM)。

所有 LSx RAM 块都具有奇偶校验功能。这些存储器是安全的，具有访问保护（CPU 写入/CPU 取回）功能。

默认情况下，这些存储器仅供 CPU 使用，用户可以通过适当地配置 LSxMSEL 寄存器中的 MSEL_LSx 位字段来选择与 CLA 共享这些存储器。

表 7-2 显示了对 LSx RAM 的主访问。

表 7-2. 对 LSx RAM 的主访问
（假设已禁用所有其他访问保护）

MSEL_LSx	CLAPGM_LSx	CPU 允许的访问	CLA 允许的访问	注释
00	X	全部	–	LSx 存储器被配置为 CPU 专用 RAM。
01	0	全部	数据读取 数据写入	LSx 存储器在 CPU 和 CLA1 之间共享。
01	1	仿真读取 仿真写入	仅取回	LSx 存储器是 CLA1 程序存储器。

7.3 全局共享 RAM (GSx RAM)

可从 CPU 和 DMA 访问的 RAM 块被称为全局共享 RAM (GSx RAM)。每个共享 RAM 块可由任一 CPU 子系统拥有，具体取决于 GSxMSEL 寄存器中各个位的配置。

所有 GSx RAM 块都具有奇偶校验功能。

当 GSx RAM 块由某个 CPU 子系统拥有时，CPUx 和 CPUx.DMA 将拥有对该 RAM 块的完全访问权限，而 CPUy 和 CPUy.DMA 将仅拥有读取访问权限（无取回/写入访问权限）。

表 7-3 显示了对 GSx RAM 的主访问。

表 7-3. 对 GSx RAM 的主访问
（假设已禁用所有其他访问保护）

GSxMSEL	CPU	指令取回	读取	写入	CPUx.DMA 读取	CPUx.DMA 写入
0	CPU1	支持	支持	支持	支持	支持
	CPU2	-	支持	-	支持	-
1	CPU1	-	支持	-	支持	-
	CPU2	支持	支持	支持	支持	支持

GSx RAM 具有访问保护（CPU 写入/CPU 取回/DMA 写入）。

7.4 CPU 消息 RAM (CPU MSGRAM)

这些 RAM 块可用于在 CPU1 和 CPU2 之间共享数据。这些 RAM 用于处理器间的通信，因此也被称为 IPC RAM。CPU MSGRAM 具有来自其自身的 CPU 子系统的 CPU/DMA 读取/写入访问权限，以及来自其他子系统的 CPU/DMA 只读访问权限。

该 RAM 具有奇偶校验功能。

7.5 CLA 消息 RAM (CLA MSGRAM)

这些 RAM 块可用于在 CPU 和 CLA 之间共享数据。CLA 具有对“CLA 到 CPU MSGRAM”的读写访问权限。CPU 具有对“CPU 到 CLA MSGRAM”的读写访问权限。CPU 和 CLA 都具有对两个 MSGRAM 的读取权限。

该 RAM 具有奇偶校验功能。

8 总结

最后阐明两个问题。

与旧工艺节点中的早期器件相比，最新半导体工艺节点中的许多较新芯片在其 SRAM 中更广泛地使用 EDAC。尽管这确实比存储器中具有奇偶校验功能或不具有自动检测功能的旧器件提供了更好的覆盖范围，但这可能更多是由于工艺要求而不是安全性。较新的工艺节点采用了结构更具创新性的几何形状，更容易受到软错误和工艺退化的影响，因此有必要添加 EDAC 以满足合理的器件寿命要求。只要较新的器件包含 EDAC，这个问题就无需担心。不过，采用这些新工艺的器件对 EDAC 的需求更大。

要考虑的第二个问题是工艺节点的可用历史记录。如果目标市场需要 10 年的寿命，那么从安全角度而言，最好是在仔细监控现场故障的同时，使用可满足市场要求的工艺节点进行 10 年以上的批量生产。这是因为每项新工艺的进步都会带来独特的新问题。

9 参考文献

- 德州仪器 (TI)：*TMS320F2837xD 双核微控制器数据手册*

10 修订历史记录

注：以前版本的页码可能与当前版本的页码不同

Changes from Revision * (November 2017) to Revision A (November 2020)	Page
• 对该文档的“摘要”进行了更新。	1
• 更新了整个文档中的表格、图和交叉参考的编号格式。	2

重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265