

# قابلیت اطمینان در حافظه‌های مقاوم‌سازی شده با تکنیک‌های SEC نسبت به SEU بر اساس زنجیره مارکوف

رضا امیدی<sup>1</sup> و کریم محمدی<sup>2</sup>

دانشگاه علم و صنعت ایران<sup>1</sup>

دانشگاه علم و صنعت ایران<sup>2</sup>

## چکیده

تعیین قابلیت اطمینان در بخش‌های مختلف ماهواره‌ها از مهم‌ترین فاکتورها در طراحی ماهواره می‌باشد. در ماهواره‌های مستقر در اطراف زمین، واژگونی بیت‌های حافظه شایع‌ترین پدیده‌ای است که قابلیت اطمینان ماژول‌های حافظه را تحت تاثیر قرار می‌دهد. این واژگونی‌ها بر اثر برخورد پروتون‌ها و یون‌های سنگین رخ می‌دهند اخیراً سه شکل از SEU - مرسوم، انباشتگی و خودبازسازی - مد نظر قرار گرفته است. در این مقاله تجزیه و تحلیل قابلیت اطمینان این مدل‌ها بر اساس زنجیره مارکوف ارائه و با نتایج روش‌های آمار و احتمالی سایر مقالات مقایسه گردیده است. شبیه‌سازی‌ها نشان می‌دهد که نتایج زنجیره مارکوف نسبت به روش‌های آمار و احتمالی دقیق‌تر می‌باشد. بر این اساس با معیار قرار دادن نتایج زنجیره مارکوف دو روش مقاوم‌سازی افرونگی سه ماجولی و همینگ (8،4) نیز با هم مقایسه شده‌اند.

واژه‌های کلیدی: واژگونی بیت‌های حافظه (SEU)، قابلیت اطمینان، حافظه‌ها، کدهای تصحیح تک خطا

## 1- مقدمه

ماهواره‌هایی که در اطراف زمین قرار گرفته‌اند تحت تاثیر تشعشعات کمربندهای اطراف زمین و یا تشعشعات ناشی از پرتوهای کیهانی و فعالیت‌های خورشیدی می‌باشند این تاثیرات به طور لحظه‌ای و یا در طولانی مدت، اثراتی بر عملکرد بخش‌های الکترونیکی دارند [1] واژگونی بیت‌های حافظه (SEU<sup>1</sup>) شایع‌ترین تاثیر محیط تشعشعات فضایی می‌باشد [2-4] که بر اثر برخورد پروتون‌ها و یا یون‌های سنگین در سلول‌های حافظه رخ می‌دهد بسته به نوع و محل کاربرد حافظه، تاثیر SEU ممکن است مخرب بوده و استفاده از تکنیک‌های مقاوم‌سازی ضروری باشد. به عنوان نمونه در افزاره‌های برنامه‌پذیر میدانی (FPGA<sup>2</sup>) برای مقاوم‌سازی از افزونگی سه ماجولی به شکل کلی یا انتخابی، جاروب مداوم بیت‌های پیکربندی و غیره [2-6] استفاده می‌شود. برای مقاوم‌سازی ماژول‌های حافظه که کنار پردازنده قرار گرفته‌اند، روش‌هایی مانند افزونگی سه ماجولی، انواع کدهای تشخیص و تصحیح خطا یا جاروب حافظه استفاده می‌شود [7]. تکنیک‌های مقاوم‌سازی از نظر فضای لازم، انرژی و هزینه سربارهایی دارند اما میزان کارایی هر یک از آنها با معیارهایی همچون قابلیت اطمینان یا در دسترس بودن، متوسط زمان تا خرابی یا متوسط زمان تا واژگونی بیت‌های حافظه سنجیده می‌شوند. اخیراً سه مدل و یا سه شکل از واژگونی بیت‌های حافظه یعنی شکل مرسوم<sup>3</sup>، انباشت<sup>4</sup> و خودبازسازی<sup>5</sup> مد نظر قرار گرفته است [8]. روابط MTTF در مرجع [8] بر اساس

<sup>1</sup> Single Event Upset

<sup>2</sup> Field Programmable Gate Array

<sup>3</sup> Traditional

<sup>4</sup> Cumulative

<sup>5</sup> Self Clearing



روابط و تقریب‌های آمار و احتمال ارائه شده است؛ در این مقاله روابط MTTF بر اساس زنجیره ماکوف برای هر سه شکل از تاثیر SEU ارائه خواهد شد. نتایج محاسبات MTTF در هر دو رویکرد، برای یک رجیستر یکسان می‌باشد اما در سیستم‌های حافظه بین نتایج دو روش اختلاف‌هایی وجود دارد. برای اعتبار سنجی نتایج در این مقاله الگوریتمی ارائه گردیده است، شبیه-سازی تزریق خطا با الگوریتم ارائه شده موید درستی نتایج زنجیره ماکوف می‌باشد. در ادامه مقاله، با مبنا قرار دادن زنجیره ماکوف روابطی برای حافظه‌های مقاوم‌سازی شده با افزونگی سه ماجولی ارائه و نتایج آن با روش مقاوم‌سازی همینگ (8،4) مقایسه شده است.

در ادامه این مقاله می‌خوانید: زنجیره ماکوف برای تعیین قابلیت اطمینان نسبت به SEU در یک رجیستر و در سیستم‌های حافظه، الگوریتم اعتبار سنجی نتایج زنجیره ماکوف، قابلیت اطمینان در حافظه‌های مقاوم‌شده با افزونگی سه ماجولی، جمع‌بندی و نتیجه‌گیری.

## 2- مدل ماکوف برای تعیین قابلیت اطمینان نسبت به SEU

برای محاسبات قابلیت اطمینان و MTTF در این مقاله مشابه سایر مراجع فرض کنیم:

§ نرخ واژگونی بیت‌های حافظه دارای توزیع پواسون می‌باشد. و در تمام حافظه توزیع یکنواختی دارد. در شرایط محیط تشعشعات فرض درستی می‌باشد [8].-

§ واژگونی بیت‌ها مستقل از هم باشد یعنی واژگونی یک سلول حافظه سایر سلول‌ها را متاثر نکند.

§ هر برخورد تنها یک سلول حافظه را تحت تاثیر قرار دهد یعنی چند واژگونی هم‌زمان ( $MBU^6$ ) رخ ندهد. هر چند در محیط تشعشعات احتمال MBU صفر نیست اما احتمال آن کمتر می‌باشد [7]. این اثر در [9-10] بیشتر بررسی شده است.

§ روش مقاوم‌سازی استفاده شده کدهای SEC<sup>7</sup> فرض شده است در این حالت رخداد اولین خطا در کلمه، قابل اصلاح بوده و رخداد دومین خطا در یک بیت دیگر کلمه باعث خرابی خواهد شد. در این مقاله مقاوم‌سازی با استفاده از افزونگی سه ماجولی نیز مد نظر قرار گرفته است.-

برخورد کارا- برخورد یون سنگین و یا پروتون پر انرژی در قسمت حساس یک سلول - باعث واژگونی یعنی تبدیل منطق یک به منطق صفر و برعکس در سلول حافظه خواهد شد برخورد کارای دوم در صورتی که به یکی از بیت‌های غیر از بیت واژگون شده باشد باعث خرابی کلمه می‌شود اما ممکن است برخورد دوم به شکلی باشد تنها اثر برخورد اول را تکرار و یا اثر برخورد اول تصحیح شود حالت مرسوم این است که برخورد دوم در بیت متاثر شده از برخورد اول نباشد حالت انباشته زمانی است که برخورد دوم واژگونی جدیدی ایجاد نکند و تنها اثر برخورد اول را تثبیت نماید زمانی که برخورد دوم اثر برخورد اول را تصحیح کند تحت عنوان خودبازسازی نامگذاری می‌شود [8]. بر این اساس سه حالت، ابتدا برای یک رجیستر N-بیتی و سپس برای سیستم حافظه‌ای با M رجیستر N-بیتی، قابلیت اطمینان و MTTF در محاسبه خواهد شد.

### 2-1- یک رجیستر (M=1)

اگر رجیستر مقاوم‌شده با کدهای SEC با طول N بیت در نظر گرفته شود در مرجع [8] برای تعیین MTTF مطابق با مرجع [11] از رابطه 1 استفاده شده است.

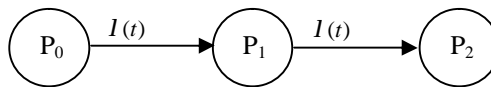
<sup>6</sup> Multi Bit Upset

<sup>7</sup> Single Error Correction

$$MTTF = \frac{METF}{\lambda} \quad (1)$$

$$MTTF = \int_0^{\infty} r_r(t)^M \times dt \quad (2)$$

در مرجع مذکور با تعیین METF برای سه حالت مختلف تاثیر SEU (مرسوم، انباشت، خودبازسازی) MTTF تعیین شده است در این مقاله MTTF با استفاده از رابطه 2 تعیین خواهد شد برای این منظور بایستی قابلیت اطمینان محاسبه و سپس انتگرال گیری انجام شود. برای تعیین قابلیت اطمینان زنجیره مارکوف برای هر یک از مدل های SEU در ادامه آمده است.



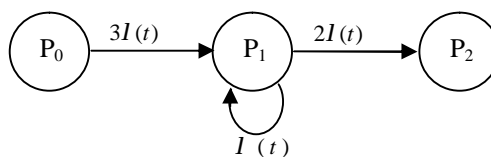
شکل 1: زنجیره مارکوف برای مدل مرسوم تاثیر SEU در حافظه ها

برای حالت مرسوم با فرض نرخ SEU ثابت در هر بیت ( $\lambda'$ ) و نرخ SEU ثابت در هر کلمه ( $\lambda = N\lambda'$ ) روابط زنجیره مارکوف عبارتند از:

$$\begin{aligned} \frac{dP_0(t)}{dt} &= -N\lambda'P_0(t) \\ \frac{dP_1(t)}{dt} &= N\lambda'P_0(t) - N\lambda'P_1(t) \\ \frac{dP_2(t)}{dt} &= N\lambda'P_1(t) \end{aligned} \quad (2)$$

با توجه به اینکه  $P_0(0)=1, P_1(0)=0$  می باشد با حل معادلات و انتگرال گیری از قابلیت اطمینان در مدل مرسوم داریم:

$$\begin{aligned} R(t) &= P_0(t) + P_1(t) = e^{-N\lambda't} + N\lambda'te^{-N\lambda't} \\ MTTF &= \int_0^{\infty} R(t)dt = \frac{2}{N\lambda'} \end{aligned} \quad (3)$$



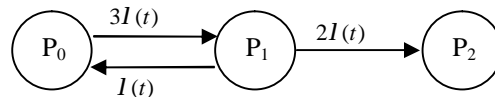
شکل 2: زنجیره مارکوف برای مدل انباشتگی تاثیر SEU در حافظه ها

در شکل انباشتگی SEU روابط زنجیره مارکوف عبارتند از:

$$\begin{aligned} \frac{dP_0(t)}{dt} &= -N\lambda P_0(t) \\ \frac{dP_1(t)}{dt} &= N\lambda P_0(t) - (N-1)\lambda P_1(t) \\ \frac{dP_2(t)}{dt} &= (N-1)\lambda P_1(t) \end{aligned} \quad (4)$$

با توجه به اینکه  $P_0(0)=1, P_1(0)=0$  می‌باشد با حل معادلات و انتگرال گیری از قابلیت اطمینان در مدل انباشت داریم:

$$\begin{aligned} R(t) &= P_0(t) + P_1(t) = e^{-N\lambda t} + N(e^{-(N-1)\lambda t} - e^{-N\lambda t}) \\ MTTF &= \int_0^{\infty} R(t) dt = \frac{1}{N\lambda'} + \frac{N}{(N-1)\lambda'} - \frac{1}{\lambda'} \\ MTTF &= \left( \frac{2N-1}{N-1} \right) \frac{1}{N\lambda'} \end{aligned} \quad (5)$$



شکل 3: زنجیره مارکوف برای مدل خودبازسازی تأثیر SEU در حافظه‌ها

در حالت خودبازسازی روابط زنجیره مارکوف عبارتند از:

$$\begin{aligned} \frac{dP_0(t)}{dt} &= -N\lambda P_0(t) + \lambda P_1(t) \\ \frac{dP_1(t)}{dt} &= N\lambda P_0(t) - (N-1)\lambda P_1(t) - \lambda P_1(t) \\ \frac{dP_2(t)}{dt} &= (N-1)\lambda P_1(t) \end{aligned} \quad (6)$$

با توجه به اینکه  $P_0(0)=1, P_1(0)=0$  می‌باشد با حل معادلات و انتگرال گیری از قابلیت اطمینان در مدل خودبازسازی

داریم:

$$\begin{aligned} R(t) &= \frac{\sqrt{N}+1}{2} e^{-(\sqrt{N}-1)\sqrt{N}I't} + \frac{\sqrt{N}-1}{2} e^{-(\sqrt{N}+1)\sqrt{N}I't} \\ MTTF &= \int_0^{\infty} R(t) dt = \frac{2}{(N-1)I'} \end{aligned} \quad (7)$$

در جدول 1 روابط حاصل از زنجیره مارکوف با روابط ارائه شده در مرجع مقایسه شده است - توجه داشته باشید نرخ خرابی

در یک کلمه برابر است با:  $\lambda = N\lambda'$  -

جدول 1: مقایسه نتایج روش زنجیره مارکوف و نتایج روش آمار و احتمال

روش	نتایج روش آمار و	نتایج روش
-----	------------------	-----------

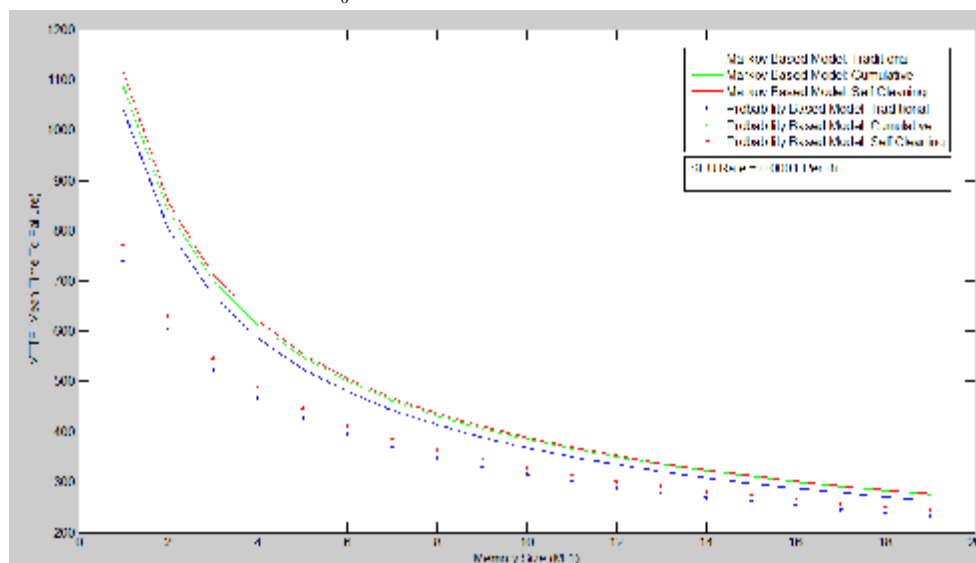
مدل	احتمال [8]	زنجیره ماکوف
مرسوم	$\frac{2}{I}$	$\frac{2}{NI}$
انباشت	$\frac{N}{I} \cdot \left(\frac{1}{N} + \frac{1}{N-1}\right)$	$\left(\frac{2N-1}{N-1}\right) \frac{1}{NI}$
خود بازسازی	$\frac{N}{I} \cdot \frac{2}{(N-1)}$	$\frac{2}{(N-1)I}$

چنانچه در جدول 1 نیز نشان داده شده است در یک رجیستر نتایج هر دو رویکرد یکسان می باشد. روش مارکوف این مزیت را دارد که رابطه قابلیت اطمینان نیز در دسترس است و در محاسبات حافظه های بزرگ تر ( $M > 1$ ) می توان از آن استفاده کرد.

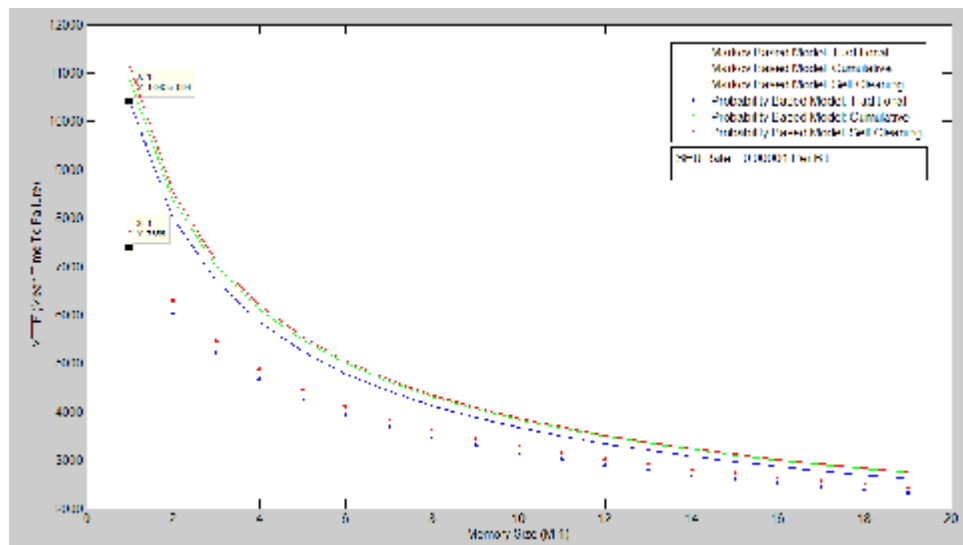
## 2-2- سیستم های حافظه ( $M > 1$ )

در سیستم های حافظه برای تعیین قابلیت اطمینان می توان از رابطه زیر استفاده کرد [8]:

$$MTTF = \int_0^{\infty} r_r(t)^M \times dt \quad (8)$$



شکل 4: MTTF به ازای M های مختلف ( $\lambda=0.0001$ )


 شکل 5: MTTF به ازای Mهای مختلف ( $\lambda'=0.00001$ )

3 در رابطه بالا  $I_T(t)$  قابلیت اطمینان در یک رجیستر می‌باشد. با توجه به پیچیده بودن آنالیز رابطه از یکسو و مشخص نمودن رابطه قابلیت اطمینان از سوی دیگر در [8] با یکسری تقریب‌ها روابطی برای MTTF در سیستم‌های حافظه ارائه شده است (روابط 9) در این مقاله با استفاده از روابط قابلیت اطمینان برای سه حالت - که در بخش قبلی بر اساس زنجیره ماکوف تعیین شد - MTTF با جایگذاری در رابطه 8 تعیین خواهد شد. و با نتایج فرمول‌های تقریب ارائه شده در [8] مقایسه می‌شود.

$$\begin{aligned} \text{Traditional: } MTTF|_{\text{Trad}} &\cong \frac{1}{\lambda} \sqrt{\frac{\pi}{2} \frac{1}{M}} \\ \text{Cumulative: } MTTF|_{\text{Cumul.}} &\cong \frac{1}{\lambda} \sqrt{\frac{\pi}{2} \frac{1}{M} \frac{N}{N-1}} \\ \text{Self-Clearing: } MTTF|_{\text{Self}} &\cong \frac{1}{\lambda} \sqrt{\frac{\pi}{2} \frac{1}{M} \frac{N}{N-1}} \end{aligned} \quad [8] - (9)$$

با فرض  $N=12$  (همینگ (8,4)) و به ازای Mهای مختلف MTTF محاسبه شده است - نرخ SEU داده  $\lambda'=0.00001$  و  $\lambda'=0.00001$  - نتایج در شکل‌های 4 و 5 آمده است. خطوط نقطه چین نتایج روابط 9 می‌باشد و خطوط پررنگ MTTF در سیستم‌های حافظه با استفاده از زنجیره ماکوف و رابطه 8 را نشان می‌دهد. چنانچه نتایج شبیه‌سازی نیز نشان می‌دهد بین نتایج دو روش اختلاف‌هایی وجود دارد برای اعتبار سنجی نتایج در ادامه الگوریتمی ارائه شده است.

### 3- اعتبار سنجی نتایج

چنانچه نتایج شبیه‌سازی نشان می‌دهد در سیستم‌های حافظه ( $M>1$ ) نتایج زنجیره ماکوف و روابط مبتنی بر تجزیه و تحلیل آماری [8] برای MTTF متفاوت می‌باشد جهت اعتبار سنجی نتایج الگوریتمی برای شبیه‌سازی تزریق خطا استفاده شده است جزئیات این الگوریتم در ادامه آمده است. این الگوریتم برای مدل‌سازی تزریق خطا در حالت مرسوم می‌باشد که برای حالت‌های دیگر (انباشت و خودبازسازی) نیز به سادگی قابل تعمیم است.

در سیستم حافظه‌ای که دارای M کلمه N بیتی است،  $M \times N$  بیت داریم به هر بیت یک شماره از یک الی  $M \times N$

اختصاص می‌دهیم خرابی یک کلمه به معنای خرابی سیستم تلقی می‌شود پس رخداد یک خطا قطعاً باعث خرابی نمی‌شود اما رخداد  $M+1$  خطا قطعاً باعث خرابی سیستم حافظه خواهد شد، در حالت کلی اگر حداقل دو خطا در یک کلمه رخ دهد سیستم خراب محسوب می‌شود. الگوریتمی به این ترتیب در نظر بگیرید:

بردار وزن‌ها را مساوی صفر قرار بده و مراحل زیر به تعداد دفعات تزیق اجرا کنید.

1- اعداد یک الی  $M \times N$  را به صورت  $M$  مجموعه شامل  $N$  عدد در نظر بگیرید.

$$S_j \left\{ \begin{array}{cccccccc} 1 & 2 & 3 & \dots & \dots & \dots & \dots & N \\ N+1 & N+2 & N+3 & \dots & \dots & \dots & \dots & 2N \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ M(N-1)+1 & M(N-1)+2 & \dots & \dots & \dots & \dots & \dots & M \times N \end{array} \right.$$

2- در هر تکرار یک عدد تصادفی صحیح غیر تکراری بین یک تا  $M \times N$  به مجموعه  $R$  اضافه کن.

$$R = \{r_1, r_2, r_3, \dots, r_i\}$$

3- به ازای هر دو عضو دلخواه از مجموعه  $R$  اگر عضو یکی از مجموعه‌های  $S_j$  ( $1 \leq j \leq M$ ) نباشند برو به مرحله 2.

4- به ازای هر دو عضو دلخواه از مجموعه  $R$  اگر عضو یکی از مجموعه‌های  $S_j$  ( $1 \leq j \leq M$ ) باشند به شمارنده وزن خطا یک واحد اضافه کن و  $R = \{\emptyset\}$ .

اگر دفعات تکرار تمام شده باشد متوسط تعداد خطاهای لازم برای خرابی از رابطه زیر به دست می‌آید:

$$METF = [\omega_1 \quad \omega_2 \quad \dots \quad \omega_{M+1}]_{1 \times (M+1)} \begin{bmatrix} 1 \\ 2 \\ \dots \\ \dots \\ M+1 \end{bmatrix}_{(M+1) \times 1}$$

خروجی الگوریتم ارائه شده متوسط رخدادها برای خرابی در سیستم‌های حافظه مقاوم‌سازی شده با کدهای SEC می‌باشد. این مقدار برای هر یک از روش‌های زنجیره مارکوف و روش تجزیه و تحلیل آماری [8] از رابطه  $METF = \lambda \times MTTF$  تعیین می‌شود در جدول زیر به ازای چند  $M$  مختلف و یک میلیارد تزیق خطا نتایج آمده است که موید روش زنجیره مارکوف می‌باشد.

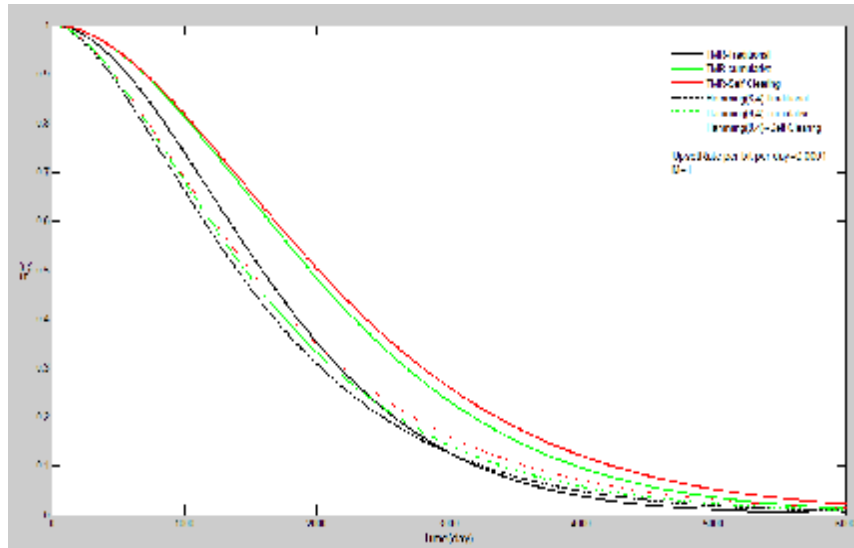
جدول 2: اعتبار سنجی نتایج روش احتمال و مارکوف

M	روش احتمال	روش مارکوف	شبیه‌سازی
2	1.7724	1.7724	08
3	2.1708	2.889	2.8889
4	3.21101	3.7571	3.75709

### 3-1- متوسط رخداد خطا در حافظه‌های مقاوم‌سازی شده با روش افزونگی سه ماجولی

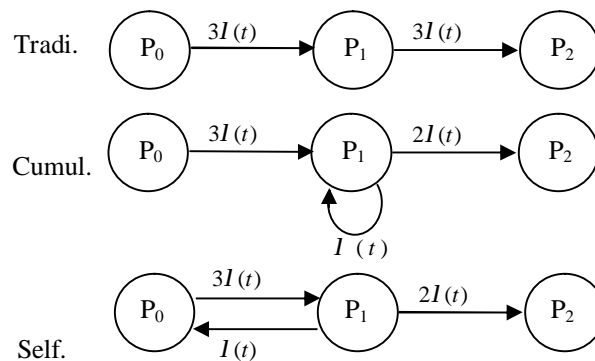
تکنیک مقاوم‌سازی افزونگی سه ماجولی هر چند نسبت به سایر روش‌های مقاوم‌سازی سیستم‌های حافظه - روش‌های استفاده از کدهای تشخیص و تصحیح خطا یا سیستم‌های RAID [12] - دارای سربار بیشتری می‌باشد اما در کاربردهای فضایی از این تکنیک نیز استفاده می‌شود [7]. در این روش قابلیت ماسک کردن خطا در هر بیت امکان‌پذیر می‌باشد بنابراین برای محاسبه MTTF قابلیت اطمینان در هر بیت معیار قرار می‌گیرد. مروری بر کارهای انجام شده در زمینه تعیین قابلیت

اطمینان سیستم‌های حافظه‌ها در مراجع مختلف نشان می‌دهد که مقایسه‌ای بین این روش با سایر روش‌های مقاوم‌سازی ارائه نشده است و همچنین استفاده از زنجیره مارکوف و شکل‌های انباشت و خودبازسازی در اثر SEU مد نظر قرار نگرفته است. در [13] مقایسه انجام شده مربوط به مدارهای دیجیتال می‌باشد.



شکل 7: مقایسه نتایج قابلیت اطمینان برای سه مدل تاثیر SEU – Traditional, Cumulative, Self Clearing – روش مقاوم‌سازی همینگ (8+4) و افزونگی سه ماژولی در یک رجیستر

از آنجایی که افزونگی در هر بیت انجام شده است زنجیره مارکوف جهت تعیین قابلیت اطمینان در سه حالت مرسوم، انباشت و خودبازسازی در شکل زیر آمده است.



شکل 8: زنجیره مارکوف در سه حالت مرسوم، انباشت و خودبازسازی برای افزونگی سه ماژولی

روابط قابلیت اطمینان هر یک از حالت‌های مختلف SEU در جدول زیر خلاصه شده است- با فرض اینکه انتخاب‌گر عاری از خطا است :-

جدول 3: روابط قابلیت اطمینان برای افزونگی سه ماژولی

روش مدل	قابلیت اطمینان (با استفاده از زنجیره مارکوف)
مرسوم	$(1+3\lambda t)e^{-3\lambda t}$
انباشت	$3e^{-2\lambda t}-2e^{-3\lambda t}$
خود بازسازی	$1.366e^{-1.268\lambda t}-0.366e^{-4.732\lambda t}$



نتایج مقایسه در یک رجیستر با دو روش همینگ (8،4) و افزونگی سه ماجولی در شکل 8 آمده است. در سیستم‌های حافظه یعنی ( $M > 1$ ) نتایج محاسبات MTTF در جدول زیر خلاصه شده است:

جدول 4: مقایسه نتایج MTTF روش مقاومسازی همینگ (8،4) و افزونگی سه ماژولی برای سه مدل تأثیر SEU

M	1024	2048	4096	8192
TMR-Traditional	46.9294	33.2742	23.6467	16.8531
TMR-Cumulative	57.3711	40.6435	28.8505	20.5293
TMR-Self Clearing	57.1470	40.3855	28.5763	20.2476
Ham-Traditional	33.6836	23.8510	16.9552	12.1073
Ham-Cumulative	35.1597	24.8896	17.6870	12.6235
Ham-Self Clearing	35.2003	24.9171	17.7079	12.6412

با توجه به منحنی‌های شکل 8 قابلیت اطمینان در روش افزونگی سه ماجولی در هر سه شکل از تأثیر SEU بالاتر از همینگ قرار می‌گیرد همچنین MTTF روش افزونگی سه ماجولی بهتر می‌باشد. نکته دیگری که از نتایج به دست می‌آید این است که در سیستم‌های حافظه نتایج MTTF سه شکل از تأثیر SEU با بزرگ‌تر شدن حافظه به هم نزدیک می‌شوند [8] اما این نزدیکی در نتایج روش افزونگی سه ماجولی در حافظه‌های بسیار بزرگ‌تر رخ می‌دهد. توجه به این نکته ضروری است که افزونگی سه ماجولی دارای سربار بیشتری است در یک کلمه 8 بیتی برای مقاومسازی با روش افزونگی سه ماجولی حداقل 16 بیت سربار داریم در حالی که در همینگ (8،4) تنها 4 بیت سربار به وجود می‌آید. در سیستم‌های حافظه هم همین سربار در تعداد کلمه‌ها ضرب می‌شوند.

#### 4- نتیجه‌گیری

در این مقاله سه شکل از تأثیر SEU (مرسوم، انباشتگی و خودبازسازی) از نظر شاخص‌های قابلیت اطمینان، با استفاده از زنجیره مارکوف بررسی شدند و با ارائه الگوریتمی، نتایج مورد ارزیابی قرار گرفت. با مبنا قرار دادن روابط زنجیره مارکوف دو تکنیک مقاومسازی افزونگی سه ماژولی و همینگ (8،4) با هم مقایسه گردید. در هر سه شکل از تأثیر SEU افزونگی سه ماژولی شاخص‌های قابلیت اطمینان بهتری نشان داد اما این تکنیک سربار بیشتری نیز دارد.

#### مراجع

- [1] A. Raoul Velazco and B. Pascal Fouillat, "Radiation Effects on Embedded Systems", Springer Netherlands, Page(s): 1-9, 2007.
- [2] A. S. Ramaswamy and B. L. Rockett, "Reconfigurable, High Density, High Speed, Low Power, Radiation-Hardened FPGA Technology", Proc. Military and Aerospace Programmable Logic Devices Conf., Sep. 2008.
- [3] A. K. Morgan, and B. D. McMurtrey, "A comparison of TMR with alternative fault-tolerant design techniques for FPGAs", IEEE Transactions on Nuclear Science, vol. 54, no. 6, pp. 2065-2072, Dec. 2007.
- [4] A. P. K. Samudrala, and B. J. Ramos, "Selective Triple Modular Redundancy (STMR) based single-event upset SEU tolerant synthesis for FPGAs", IEEE Transactions on Nuclear Science, vol. 51, no. 6, page(s): 2957-2969, Oct. 2004.
- [5] A. Pratt, B. and B. Caffrey, M., "Fine-Grain SEU Mitigation for FPGAs Using Partial TMR", IEEE Transactions on Nuclear Science, Vol.: 55, Issue: 4, Part 1 On page(s): 2274- 2280, Aug. 2008.
- [6] A. Sterpone, L. and B. Reorda, "A Reliability-Oriented Place and Route Algorithm for SRAM-based FPGAs", Research in Microelectronics and Electronics, Vol. 1, page(s): 173- 176, July 2005.
- [7] Christian Poivey and others, "Lessons Learned from Radiation Induced Effects on Solid State Recorders (SSR) and Memories", NASA-GSFC and SGT-Inc., December 2002.
- [8] A. J.A.Maestro and B. P.Reviriego, "Reliability of Single-Error Correction Protected Memories", IEEE TRANSACTIONS ON RELIABILITY, VOL. 58, NO. 1, MARCH 2009.
- [9] Pedro Reviriego and Juan Antonio Maestro, "Reliability Analysis of Memories Suffering Multiple Bit Upsets", IEEE TRANSACTIONS ON DEVICE AND MATERIALS RELIABILITY, VOL. 7, NO. 4, DECEMBER 2007.



- 
- [10] Pedro Reviriego and Juan Antonio Maestro, "Study of the Effects of Multibit Error Correction Codes on the Reliability of Memories in the Presence of MBUs", IEEE TRANSACTIONS ON DEVICE AND MATERIALS RELIABILITY, VOL. 9, NO. 1, MARCH 2009.
- [11] J. M. Kontoleon and J. Andrianakis, "Reliability analysis of simplex and duplex memory systems with SEC and soft-error scrubbing recovery", International Journal of Quality & Reliability Management, vol. 20, no. 5, pp. 620-636, 2003.
- [12] A. Israel Koren and B. C. Mani Kirishna, "Fault Tolerant Systems", Elsevier, Page(s): 55-108, 2007.
- [13] R. Hentschke, F. Marques, F. Lima, L. Carro, A. Susin, and R. Reis, "Analyzing area and performance penalty of protecting different digital modules with Hamming code and triple modular redundancy", in 15th Symposium on Integrated Circuits and Systems Design, 2002, pp. 95-100.

1- تهران - دانشگاه علم و صنعت ایران - دانشکده برق - [r\\_omidi@elec.iust.ac.ir](mailto:r_omidi@elec.iust.ac.ir)

2- تهران - دانشگاه علم و صنعت ایران - دانشکده برق - [mohammadi@iust.ac.ir](mailto:mohammadi@iust.ac.ir)