

مدل سازی و ارزیابی قابلیت اطمینان موتور راکت به روش تحلیل درخت خطا

مهدی کرباسیان^۱ و احمد باقری^{۲*}

۱. دانشگاه صنعتی مالک اشتر، دانشکده مهندسی صنایع

۲. مهندسان مشاور بهبود سیستم

* تهران، خیابان مطهری، پلاک ۱۱۷

mkarbasian@yahoo.com

شناسایی انواع خرابی سیستمها به خصوص در مورد محصولات حیاتی و حساس و محاسبه قابلیت اطمینان آنها قبل از به کارگیری، نقش مؤثری در بهبود طراحی این سیستمها ایفا می کند. روش تحلیل درخت خطا (FTA) یک ابزار تشخیصی بسیار قوی برای تحلیل سیستمهای پیچیده است که به عنوان یک روش کمک کننده در اصلاح طراحی به کار می رود [۱]. بر همین اساس، در این مقاله ابتدا بلوک دیاگرام یک موتور راکت رسم گردیده و بر پایه آن درخت خطای احتراق نابهنگام موتور به دست آمده است و در نهایت قابلیت اطمینان کارکرد درست موتور راکت حین به کارگیری محاسبه گردیده است.

واژه های کلیدی: قابلیت اطمینان، تحلیل درخت خطا، بلوک دیاگرام، موتور راکت

مقدمه

محصولات مهندسی مدرن از تک تک قطعات تا سامانه های بزرگ باید به گونه ای طراحی و تولید شوند که در طول زمان مأموریت از قابلیت اطمینان لازم برخوردار باشند. در هر صنعتی و به خصوص در صنایع هوافضا هنگامی که سیستمی از کار می افتد یا دچار اختلال می شود، هم از جنبه اقتصادی و هم از جنبه انسانی خطرناک و زیان آور است [۲].

از جمله تجهیزات حساس در صنایع نظامی می توان به راکت اشاره کرد که قسمت اعظمی از تولیدات صنایع موشکی کشور را به خود اختصاص داده است. موتور راکت می تواند به علت عیب های الکترونیکی، اختلال الکترومغناطیسی در کار رادارها یا عوامل خارجی از قبیل ضربه، درجه حرارت بالا و ... با احتراق نابهنگام آتش بگیرد [۳].

در این مقاله ارزیابی قابلیت اطمینان موتور راکت با استفاده از روش تحلیل درخت خطا انجام گرفته است. این تحلیل بر پایه بلوک

دیاگرامی است که از موتور راکت به دست آمده است. روش تحلیل درخت خطا یک نمودار منطقی و گرافیکی از بالا به پایین است که خرابی و علل آن را توصیف می کند [۴]. نمودار تحلیل درخت خطا از نظر گرافیکی، نمایانگر تمامی خرابی های سامانه، زیرسامانه و مجموعه است که برای نمایش روابط بین خرابی ها و علل آن مجموعه ای از علائم و نمادها را به کار می گیرد [۵]. از جمله مزایای این روش این است که ضمن شناسایی تمامی پیشامدهای میانی و نهایی، امکان محاسبه احتمال وقوع آنها نیز وجود دارد؛ دیگر اینکه برآورد احتمالات خرابی های مرکب را درون یک سیستم پیچیده امکان پذیر می سازد و حساسیت سیستم و اقدامات متقابل با بازده پایین را شناسایی می کند و به وسیله آن آماده سازی منابع را به سمت کنترل بیشتر خطر سوق می دهد؛ همچنین، این ابزار می تواند برای پیکربندی مجدد یک سیستم به کار گرفته شود تا از حساسیت و آسیب پذیری آن بکاهد [۱].

چگونگی عملکرد سیستم احتراق موتور راکت

به منظور در نظر گرفتن کلیه حالت های سطح بالای خرابی در موتور

ترسیم درخت خطا و محاسبه قابلیت اطمینان

درخت خطا با توجه به تمام حالات خرابی‌های ممکن برای موتور راکت ترسیم می‌شود. در ترسیم درخت خطا اینکه هرکدام از خرابی‌های سطح بالایی ممکن است با وقوع چه رخدادهایی ایجاد شوند مد نظر قرار می‌گیرد چراکه این عوامل شاخه‌های درخت خطا را تشکیل می‌دهند. پس از رسم درخت خطا، احتمال وقوع هرکدام از عوامل ارزیابی شده و با روابط محاسبه قابلیت اطمینان، قابلیت اطمینان سیستم در مواجهه با این پیشامد نهایی به دست خواهد آمد. برای نمایش درخت خطا از پیشامدها و نمادهای منطق درجه‌ای متفاوتی استفاده می‌شود که در (جدول ۱) تعریف شده‌اند. اگرچه پیشامدها و نمادهای درجه‌ای بسیاری وجود دارند، اما اغلب درخت‌های خطا می‌توانند به واسطه چهار نماد: (۱) پیشامدهای میانی یا تاپ، (۲) درجه OR، (۳) درجه AND، و (۴) پیشامد ورودی ساخته شوند.

و در نتیجه رسم دقیق درخت خطا، باید از نحوه عملکرد موتور راکت اطلاع حاصل شود. البته باید توجه داشت که برای نمایش عملکرد سیستم از بلوک دیاگرام عملیاتی (FBD) ایده گرفته شده است. این نحوه عملکرد یا بلوک دیاگرام موتور راکت در شکل (۱) مشاهده می‌شود.

با برقراری اتصال، سوئیچ S_1 باز شده و پرتاب‌کننده قادر به آزادسازی و احتراق می‌شود.

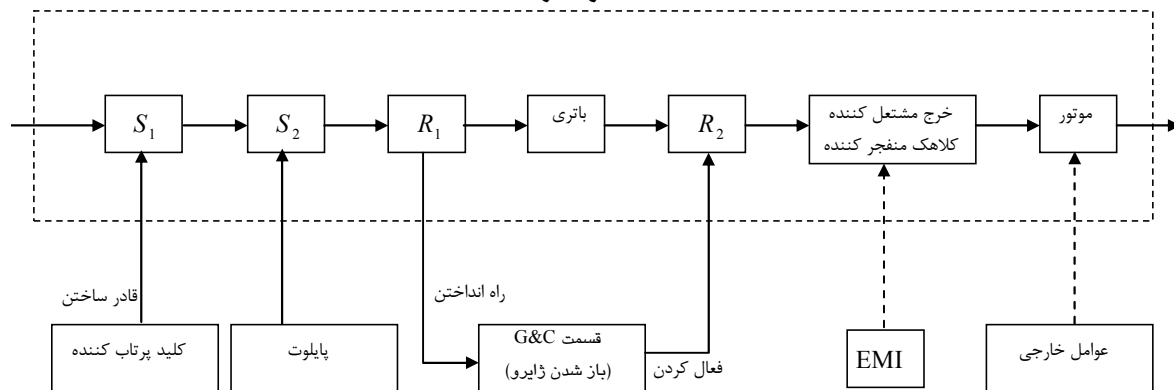
با احتراق، سوئیچ S_2 توسط پایلوت بسته می‌شود تا قدرت به رله R_1 برسد.

رله R_1 بخش هدایت و کنترل (G&C) را فعال می‌کند.

رله R_2 با سیگنالی که از بخش G&C دریافت می‌کند

فعال شده و مدار احتراق را که موتور راکت را راه‌اندازی می‌کند می‌بندد.

هدایت و کنترل



شکل ۱- بلوک دیاگرام قابلیت اطمینان احتراق موتور راکت

جدول ۱- درجه‌های منطقی درخت تحلیل خطا

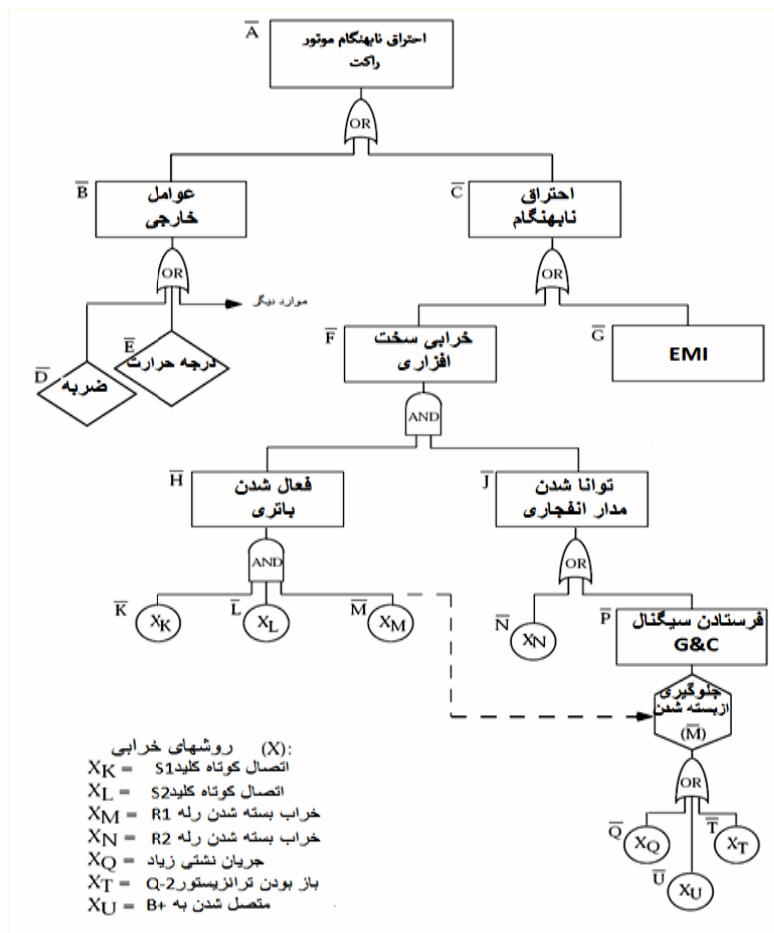
توضیح	نام	نماد
پیشامد تاپ: این پیشامد نامطلوب قابل تصور است و به سمت مسیرهای خطایابی در پیشامدهای سطح پایین‌تر پیش می‌رود. پیشامد میانی: این پیشامد وضعیت سیستمی را که توسط پیشامدهای قبلی به وجود آمده است توضیح می‌دهد.	پیشامد تاپ یا میانی ^۱	
یک خروجی به وجود می‌آید اگر یک ورودی یا بیشتر از یک ورودی وجود داشته باشد. وجود هر ورودی مجزا برای به وجود آمدن پیشامد خروجی در هریک از رخدادهای خاص لازم و کافی است.	درجه OR ^۲	

نماد	نام	توضیح
	دریچه AND ^۳	یک خروجی به وجود می‌آید اگر تمامی ورودی‌ها وجود داشته باشند. تمامی ورودی‌ها برای به وجود آمدن پیشامد خروجی ضروری و کافی هستند.
	پیشامد ورودی ^۴	یک خطا یا خرابی راه‌انداز که زیاد پیش نرفته است؛ این پیشامدها مرز دقیق تحلیل را مشخص می‌کنند. قابل بسط نبوده و در پایین‌ترین سطح تفکیک قرار دارند. با علامت X علامت می‌گردد.
	پیشامد توسعه نیافته ^۵	پیشامدی که به علت کمبود اطلاعات یا ناکافی بودن نتایج بیش از این توسعه نیافته است (یا یک خرابی که تیم قادر به اصلاح آن نباشد). با علامت W علامت می‌گردد و زیرنویس عددی ارائه می‌گردد.
	دریچه بازدارنده ^۶	در شرح ارتباط بین دو خرابی با یکدیگر استفاده می‌شود. اگر به حالت متعادل کننده اشاره کند خرابی ورودی به طور مستقیم خرابی خروجی را تولید می‌کند.

1. Event (TOP or intermediate) 2. OR gate 3. AND gate 4. basic event 5. undeveloped event 6. INHIBIT gate

نابهنگام آتش بگیرد. عیب الکترونیکی سخت‌افزاری با توانا شدن مدار انفجاری و فعال شدن باتری به وجود می‌آید که علت بروز هریک نیز در درخت خطا مشخص است.

همان‌طور که پیش از این اشاره شد موتور راکت می‌تواند به علت عیوب الکترونیکی، اختلال الکترومغناطیسی در کار رادارها یا عوامل خارجی از قبیل ضربه، درجه حرارت بالا و ... با احتراق



شکل ۲- درخت عیب‌یابی مدار انفجاری موتور راکت ارتباط میان بلوک

محاسبه قابلیت اطمینان

اگر درخت خطایابی به عنوان یک ابزار کمی مورد استفاده قرار گیرد، احتمال خرابی باید برای هریک از پیشامدها یا راه‌اندازهای ورودی تعیین گردد. منابع این احتمالات خرابی از داده‌های کارخانه سازنده، استانداردهای صاحب‌نظران صنعت، استانداردهای MIL، شواهد تاریخی (برای سیستم‌های مشابه)، شبیه‌سازی یا آزمون‌سازی، برآوردهای دلفی، و روش واقع‌نگاری میانی دریافت می‌شوند. تکنیک دلفی، از برآوردهای کارشناسان اهل نظر به دست آمده است. روش ثبت عملیات میانی نیز زمانی مفید است که احتمال خرابی نتواند برآورد شود اما مرزهای قابل قبول بالاترین و پایین‌ترین را می‌توان تخمین زد [۱]. در اینجا احتمالات از استاندارد MIL-338 B به دست آمده است. به عبارت دقیق‌تر، برای احتمالات K، L، M، N و G از استاندارد Mil-217 براساس شرایط محیطی، درجه حرارت، مشخصات الکتریکی و کیفیت قطعات استفاده شده است و برای دیگر بخش‌ها از تجارب قبلی و نظرات خبرگان استفاده شده است.

جدول ۲- احتمال خرابی هریک از قطعات موتور

$\bar{K} = S_1$ = احتمال اتصال کوتاه شدن کلید $50 * 10^{-3}$
$\bar{L} = S_2$ = احتمال اتصال کوتاه شدن کلید $100 * 10^{-3}$
$\bar{M} = R_1$ = احتمال خراب بسته شدن رله $40 * 10^{-3}$
$\bar{N} = R_2$ = احتمال خراب بسته شدن رله $5 * 10^{-3}$
\bar{Q} = احتمال جریان نشستی زیاد $1 * 10^{-3}$
$\bar{T} = Q^{-2}$ = احتمال باز بودن ترانزیستور $2 * 10^{-3}$
\bar{U} = احتمال متصل شدن به سر باتری $2 * 10^{-3}$
\bar{G} = احتمال اختلال در کار رادار $5 * 10^{-6}$
\bar{D} = احتمال ضربه تحت شرایط آزمون $2.5 * 10^{-6}$
\bar{E} = آزمون $12.5 * 10^{-6}$ = احتمال احتراق نابهنگام به علت درجه حرارت شرایط

همان‌طور که در شکل (۲) نشان داده شد، احتمال آتش گرفتن تصادفی موتور راکت به علت احتراق نابهنگام به وسیله مدار انفجار بر اثر خرابی سخت‌افزاری (F) یا مداخله الکترومغناطیسی در کار رادارها (G) است؛ یعنی:

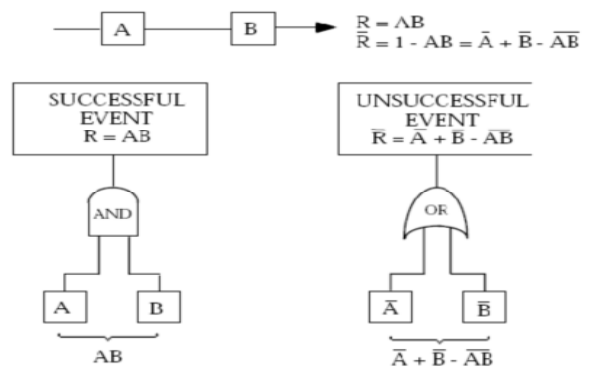
با توجه به خرابی سخت‌افزاری، احتمال احتراق نابهنگام به علت خرابی سخت‌افزاری براساس رابطه زیر بیان می‌شود:

در حالی که

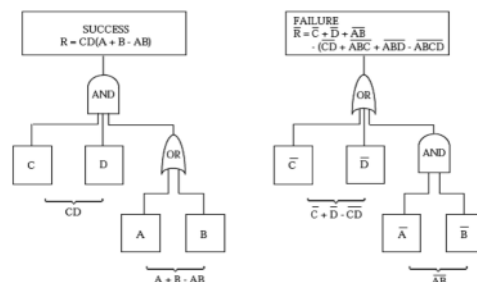
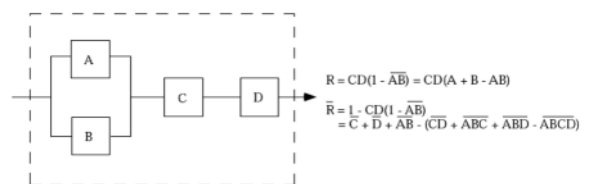
$$\begin{aligned} \bar{H} &= \overline{KLM} \\ \bar{J} &= \bar{N} + \bar{P} - \bar{NP} \\ \bar{P} &= \bar{Q} + \bar{T} + \bar{U} = (\bar{QT} + \bar{QU} + \bar{TU} - \bar{QTU}) \end{aligned}$$

ارتباط عملکردی میان بلوک دیاگرام قابلیت اطمینان (موفقیت) و هم‌ارز درخت خطای آن در شکل‌های ۳ و ۴ نشان داده شده است.

همان‌طور که در شکل (۳) دیده می‌شود، موفقیت سیستم سری که از دو جزء A و B تشکیل شده است، از رابطه $R=AB$ و احتمال خرابی سیستم (یعنی شکست یا عملکرد غیرقابل اطمینان) از رابطه $\bar{R} = (1 - R) = 1 - AB$ به دست می‌آید. به عبارت دیگر، $\bar{R} = 1 - AB = 1 - (1 - \bar{A})(1 - \bar{B}) = \bar{A} + \bar{B} - \bar{A}\bar{B}$ در شکل (۴) دو جزء A و B به صورت موازی با یکدیگر هستند که این دو جزء به صورت سری با دو جزء دیگر C و D مرتبط شده‌اند. شایان ذکر است که در پیچۀ "AND" در ترکیب موفقیت (R_S)، در پیچۀ "OR" برای ترکیب خرابی (R_S) می‌شود و بالعکس.



شکل ۳- تبدیل بلوک دیاگرام قابلیت اطمینان دو المان سری به دیاگرام منطقی درخت خطا



شکل ۴- تبدیل بلوک دیاگرام سری - موازی به هم‌ارز دیاگرام منطقی درخت خطا

$$\bar{A} \approx 21.7 * 10^{-6}$$

بنابراین، در هر ۱ میلیون پرتاب یا بارگیری موشک ۲۲ احتراق نابهنگام موتور صورت می‌گیرد. شایان ذکر است براساس این تخمین می‌توان بررسی کرد که سیستم طراحی شده با این قابلیت اطمینان، مورد قبول کارفرما هست یا خیر تا در صورت پذیرفته نشدن، نسبت به تغییر طراحی یا تغییر سطح کیفیت مواد اقدام کرد.

نتیجه‌گیری

پس از محاسبه قابلیت اطمینان سیستم و با توجه به درخت خطا می‌توان مؤثرترین عوامل بر روی قابلیت اطمینان را شناسایی کرده و ضمن بهبود طراحی سیستم به کمک راهکارهای مناسب، طراحی‌های مختلف را با یکدیگر مقایسه کرده و مناسب‌ترین گزینه را انتخاب کرد. همچنین، درخت خطا می‌تواند در شناسایی مسیرهای خرابی بحرانی و اصلاح ضعف‌های طراحی ایفای نقش کند. یکی دیگر از نتایج تحلیل درخت خطا تخصیص احتمالات خرابی بحرانی در میان سطوح پایینی خرابی سیستم است.

مراجع

- [1] Goldberg B. E., et al, *System Engineering Toolbox for Design – Oriented Engineers*, National Aeronautics and Space Administration, Marshall Space Flight Center, 1994.
- [۲] لوین م.ا.، و ت.ت. کالال، *بهبودسازی در قابلیت اطمینان محصول: استراتژی‌ها و پیاده‌سازی*، ترجمه معاونت تضمین مرغوبیت سازمان صنایع هوافضا، ویراسته احمد مهدی‌زاده، تهران، انتشارات صنایع هوافضا، ۱۳۸۶.
- [3] MIL – HDBK - 338 B: *Electronic Reliability Design Handbook*, 1998.
- [4] Vesely W., B. Goldberg, *Fault Tree Handbook*, United States Nuclear Regulatory Commission, Washington D.C., 1981.
- [۵] کرباسیان مهدی و طباطبایی، لیلا. *آشنایی با قابلیت اطمینان*، اصفهان، انتشارات ارکان دانش، ۱۳۸۸.

با استفاده از رویکرد از بالا به پایین، ترکیب این اطلاعات در مدل احتمالی خرابی، و تخمین میزان احتمال سیستم به صورت معادلات بعدی آمده است:

$$\begin{aligned} \bar{P} &= \bar{Q} + \bar{T} + \bar{U} - (\bar{QT} + \bar{QU} + \bar{TU} - \bar{QTU}) \\ &= (2 + 1 + 0.5)10^{-3} - [(2 + 1 + 0.5)10^{-6} - (1)10^{-9}] \\ &\approx 3.5 * 10^{-3} \\ \bar{J} &= \bar{N} + \bar{P} + \bar{NP} \\ &= 5 * 10^{-3} + 3.5 * 10^{-3} - 17.5 * 10^{-6} \\ &\approx 8.5 * 10^{-3} \end{aligned}$$

این احتمال تصادفی مدار انفجاری به شرطی که رله R_1 در حالت اتصال خراب بسته شده باشد (یعنی M) در شاخه درخت خطای باتری کاربردی است. در شاخه باتری، تنها زمانی باتری می‌تواند به طور اتفاقی فعال شود که سوئیچ‌های S_1 و S_2 در حالت اتصال خراب باشند، و اگر رله R_1 در حالت اتصال خراب باشد:

$$\begin{aligned} &= (50 * 10^{-3})(100 * 10^{-3})(40 * 10^{-3}) \\ &= 200 * 10^{-6} \end{aligned}$$

احتمال احتراق نابهنگام به علت خرابی سخت‌افزاری

براساس تخمین به صورت زیر است:

$$\begin{aligned} \bar{F} &= \bar{HJ} = (200 * 10^{-6})(8.5 * 10^{-3}) \\ &= (1.70 * 10^{-6}) \end{aligned}$$

احتمال احتراق نابهنگام به علت خرابی سخت‌افزاری

یا اختلال الکترومغناطیسی از رابطه زیر به دست می‌آید:

$$\begin{aligned} \bar{C} &= \bar{F} + \bar{G} - \bar{FG} \\ &= (1.70 * 10^{-6}) + (5 * 10^{-6}) - \\ &\quad (1.70 * 10^{-6})(5 * 10^{-6}) \\ &\approx 6.70 * 10^{-6} \end{aligned}$$

احتمال احتراق نابهنگام موتور راکت به علت عوامل

خارجی از رابطه زیر به دست می‌آید:

$$\begin{aligned} \bar{B} &= \bar{D} + \bar{E} - \bar{DE} \\ &= (2.5 * 10^{-6}) + (12.5 * 10^{-6}) - \\ &\quad (2.5 * 10^{-6})(12.5 * 10^{-6}) \\ &\approx 15 * 10^{-6} \end{aligned}$$

بنابراین، احتمال تصادفی احتراق نابهنگام موتور راکت

هنگام مراحل جابه‌جایی و بارگیری سلاح عبارت است از:

$$\begin{aligned} \bar{A} &= \bar{B} + \bar{C} - \bar{BC} \\ &= (15 * 10^{-6}) + (6.70 * 10^{-6}) - \\ &\quad (15 * 10^{-6})(6.70 * 10^{-6}) \end{aligned}$$