مجله مهندسی مکانیک مدرس، فروردین 1394، دوره 15، شماره 1، ص‌ص 257-266

ماهنامه علمی پژوهشی

مهندسی مکانیک مدرس

mme.modares.ac.ir

ارزیابی قابلیت اطمینان سیستم چندحالتی برمبنای آنالیز درخت خطا

محمّدعلی فارسی[1*]، محمّد نجفی[2]

1- استادیار، مهندسی مکانیک، پژوهشکده سامانه‌های فضانوردی، پژوهشگاه فضایی ایران، تهران
2- دانشجوی دکتری، مهندسی هوافضا، پژوهشکده سامانه‌های فضانوردی، پژوهشگاه فضایی ایران، تهران
*تهران، صندوق پستی 1465774111، farsi@ari.ac.ir

اطلاعات مقاله

مقاله پژوهشی کامل
دریافت: 11 تیر 1393
پذیرش: 20 آبان 1393
ارائه در سایت: 18 آذر 1393

کلید واژگان:
قابلیت اطمینان
آنالیز درخت خطا
سیستم چندحالتی
مجموعه- برش
دیاگرام تصمیم باینری

چکیده

در این مقاله، آنالیز قابلیت اطمینان سیستم منسجم چند حالتی تشخیص شرایط اضطراری یک فضاپیما براساس آنالیز درخت خطا مورد بررسی قرار گرفته است. این سیستم دارای پیچیدگی بالا و ترم‌های اشتراکی بسیاری است که تحلیل چنین سیستمی چه به روش حداقل مجموعه- برش و چه با استفاده از روش BDD بسیار زمان‌بر و دارای تحلیل بسیار مشکلی به لحاظ ترم‌های اشتراکی بوده و همچنین نتایج بدست آمده از دقت مناسب برخوردار نخواهند بود. برای غلبه بر این مشکل، در این مقاله یک روش ترکیبی برای تحلیل درخت خطای استاتیکی توسعه داده شده است. در این روش، حداقل مجموعه- برش با روش BDD ادغام شده و احتمال رخداد رویداد اصلی مورد محاسبه قرار می‌گیرد. برای بیان کامل این روش، از مثال سیستم تشخیص شرایط اضطراری (EDS) یک فضاپیما استفاده می‌گردد. در اینجا، آنالیز سیستم از یک دیدگاه کلی‌تر صورت می‌گیرد. به این معنی که فرض می‌شود کل سیستم شامل دو زیرسیستم: زیرسیستم مربوط به فرستنده‌های سیگنال و زیرسیستم نشاندهنده‌های داخل کابین می‌باشد. دو درخت خطای متفاوت برای هر یک از حالت‌ها ساخته شده و در نهایت، نتایجی از گام‌های آنالیز برای سیستم چند حالتی متشکل از اجزاء چند حالتی به‌کمک آنالیز درخت خطا ارائه شده و مقدار قابلیت اطمینان سیستم محاسبه شده است.

Reliability Estimation of Multi-State System Based On Fault Tree Analysis

Mohammad Ali Farsi[1*], Mohammad Najafi[2]

1- Mechanical Engineering, Astronautic Research Institute, Iranian Space Research Center, Tehran, Iran
2- Aerospace Engineering, Iranian Space Research Center, Tehran, Iran
*P.O.B. 1465774111 Tehran, Iran, farsi@ari.ac.ir

ARTICLE INFORMATION

Original Research Paper
Received 02 July 2014
Accepted 11 November 2014
Available Online 09 December 2014

Keywords:
Reliability Assessment
Fault Tree Analysis
Multi-State System
Cut-Set
Binary Decision Diagram

ABSTRACT

In this paper, the reliability assessment based-on fault tree analysis in coherent multi-state emergency detection system in a sounding rocket is evaluated. A system was built with more complexity and containing various intersection terms. Analysis of such system whether by means of minimal cut-set or binary decision diagram (BDD) approaches requires complex analysis and will be time consuming owing to intersection terms. Also, the gained results have less accuracy and contain uncertainty. To overcome these problems a combinatorial method for solving static fault tree is used. This method combines minimal cut-set with BDD, and then computes the occurrence probability of top-event in fault tree. To fully demonstrate this method Emergency Detection system (EDS) is used as a case-study. Here, system analysis is done from a general approach. So assume that the overall system consists of two sub-systems: sending signal sub-system and cabin instrumental sub-system. Two different fault trees, one for each, are constructed and conclusions of analysis steps for multi-state systems consisting of multi-state elements are presented using fault tree analysis. Finally, by means of this method, the reliability assessed value of the system is estimated.

1- مقدمه

یکی از مسائل بسیار مهم در تئوری قابلیت اطمینان، درک این است که چگونه قابلیت اطمینان یک سیستم پیچیده را از اطلاعات مربوط به اجزاء آن بدست آورد. یکی از ضعف‌های اساسی تئوری قابلیت اطمینان باینری این است که سیستم و اجزاء همیشه فقط از دو دیدگاه موفقیت یا شکست تشریح می‌گردند[1]. تحلیل قابلیت اطمینان دقیق رویداد اصلی یک درخت خطا با اجزاء چند حالتی (بیشتر از دو حالت) را ارزیابی می‌کند، نشان می‌دهد که برای تشریح صحیح یک سیستم با چند حالت، یک نوع خاصی از جبر بولی لازم می‌باشد. که این را اصطلاحاً "جبر بولی با محدودیت در متغیرها" نامیده و قوانین پایه‌ای آن همانند جبر بولی معمولی به‌همراه چند محدودیت مازاد در متغیرها می‌باشد[2]. با این‌حال، برای بسیاری از سیستم‌ها، مدل قابلیت اطمینان حالت- باینری از نظر ارزیابی سیستم کافی نیست. برای مثال، شبکه‌ها و اجزاء آنها وظایف خود را در سطوح مختلفی از عملکرد انجام می‌دهند. از این‌رو، لازم است که کاهش عملکرد شبکه به‌دلیل شکست نسبی اجزای آن در طول زمان عملیات مورد بررسی قرار گیرد[3]. برای سیستم با شبکه منسجم یا همسان چندحالته، یک طیف گسترده برای شبکه‌های چند ابعادی با اجزاء باینری مورد استفاده قرار گرفته و روابط ریاضی برای ارتباط

برای ارجاع به این مقاله از عبارت ذیل استفاده نمایید:

Please cite this article using:
M. A. Farsi, M. Najafi, Reliability Estimation of Multi-State System Based On Fault Tree Analysis, *Modares Mechanical Engineering*, Vol. 15, No. 1, pp. 257-266, 2015 (In Persian)

بین طیف‌های تجمعی و تعداد خرابی‌های سیستم توسعه یافته است[4]. روش آنالیز درخت خطا (FTA[1]) ابزاری قدرتمند برای آنالیز قابلیت اطمینان یک سیستم پیچیده می‌باشد. اما روش سنتی و معمولی FTA فرض دو حالت را قبول می‌کند یعنی، فرض اینکه سیستم و اجزاء هر دو موفق عمل می‌کنند یا دچار خرابی و شکست می‌شوند. با این‌حال، در دنیای واقعی، سیستم و متعلقات دارای چندین حالت خرابی (یا مدهای خرابی) می‌باشند. برای مثال، سیگنال خرابی قطعه/ و یا اجزائی که توسط یک ردیاب یا آشکارساز به سیستم تشخیص شرایط اضطراری یک فضاپیما فرستاده می‌شود، ممکن است به‌دلیل اتصال- کوتاه در مدار یا ناشی از قطع مدار باشد. بعلاوه، هر قطعه و هر سیستمی که فقط یک مد خرابی دارد، ممکن است دارای حالت‌های مختلفی از شکست و کارکرد باشد[5]. بدیهی است که روش‌های سنتی FTA قادر به تشریح خواص مختلفی از دنیای واقعی نمی‌باشند، و توسعهٔ یک روشی برای بررسی سیستم‌ها و اجزاء چندحالتی بسیار ضروری و لازم می‌باشد. مسألهٔ آنالیز سیستم‌های چندحالتی در دهه‌های اخیر مورد بررسی قرار گرفته است، و مفهوم توسعه یافتهٔ سیستم منسجم به اجزاء چندحالتی با معرفی یک مجموعه مرتبی از مقادیر برای هر اجزاء صورت گرفته است [7،6]. و در ادامه، توسعه یافتهٔ همان مفهوم با یک منطق غیر-ترتیبی صورت گرفت [8]. در این مقاله، روشی از FTA را به عمومی‌ترین حالت سیستم که در آن هم سیستم و هم اجزاء دارای حالت‌های خرابی متعدد و چندحالتی می‌باشند توسعه داده شده است. بطور گسترده سه رویکرد کمّی برای آنالیز درخت خطای سیستم‌های پیچیده وجود دارد: روش‌های برمبنای فضای حالت، روش‌های ترکیبی، و روش‌های مدولار (ترکیبی از دو روش فوق) که بیشتر برای درخت‌های خطای دینامیکی کاربرد دارند. برای آنالیز کمّی سیستمی با پیچیدگی بالا و ترم‌های اشتراکی بسیار، تحلیل سیستم چه به روش مجموعه (مسیر) شکست حداقلی و چه با استفاده از روش دیاگرام تصمیم باینری بسیار زمان‌بر و دارای تحلیل بسیار مشکلی به لحاظ ترم‌های اشتراکی بوده و همچنین نتایج بدست آمده از دقت کمتری برخوردار خواهند بود[5]. بر همین اساس و برای غلبه بر این مشکلات، در این مقاله برای تحلیل درخت خطای استاتیکی سیستم مورد نظر از روش ترکیبی به‌کمک مجموعه (مسیر) شکست حداقلی با روش دیاگرام تصمیم باینری (BDD[2]) استفاده خواهد شد و احتمال رخدادن رویداد اصلی محاسبه گردیده و در نهایت قابلیت اطمینان سیستم ارزیابی خواهد شد.

2- روش درخت خطای مناسب برای اجزاء چندحالتی

آنالیز درخت خطا برای اجزاء چندحالتی به‌طور مبسوط در مرجع [5] برای سیستم‌های همسان مورد بررسی قرار گرفته است. از این‌رو، در این مقاله، ابتدا نتایج اصلی آنها معرفی گردیده و سپس، این روش برای سیستم غیرهمسان موردنظر توسعه داده خواهد شد. فرض کنید که جزء l دارای مدهای خرابی M_l باشد، و Ω_l فضای حالت آن باشد، که $M_l + 1$ شامل رویداد پایه‌ای می‌باشد (رابطه 1). در این‌صورت:

$$\Omega_l = (x_{li}, i \in (0,1,\dots,M_l)) \qquad (1)$$

که x_{l0}: حالت نرمال جزء l، و $x_{li}, i \in (1,\dots,M_l)$: iامین حالت خرابی جزء l می‌باشد، همچنین فرض می‌کنیم که هر جزء سیستم مستقل از هم می‌باشند و احتمال رخداد هر مد خرابی برابر صفر نباشد. بدیهی است که هر دو حالت یک جزء از سیستم، دوبه‌دو ناسازگار خواهد بود (رابطه 2). یعنی،

$$\begin{aligned} & x_{li} \cap x_{lj} = \emptyset \\ & i \in (0,1,\dots,M_l) \qquad i \neq j \\ & j \in (0,1,\dots,M_l) \end{aligned} \qquad (2)$$

در ادامه، مراحل آنالیز این روش تشریح می‌گردد.

2-1 ساخت درخت خطا

برای ساخت درخت خطا ابتدا رویداد اصلی سیستم شناسایی می‌شود و پس از انتخاب رویداد اصلی، تمام مدهای خرابی اجزاء سیستم به‌عنوان رویدادهای اولیه اتخاذ می‌گردند. روابط منطقی بین رویداد اصلی و رویدادهای پایه‌ای و اولیه آنالیز می‌گردد؛ سپس درخت خطای مربوط به رخدادن رویداد اصلی تشکیل می‌گردد.

2-2 ساده‌سازی FTA و بدست آوردن مجموعه شکست حداقلی

به‌منظور ساده‌سازی درخت خطا، از یک الگوریتم اختیاری توسعه یافته برای بدست آوردن حداقل مجموعه-برش برای سیستم و اجزاء دوحالته و با پیاده‌سازی بررسی انحصاری با رابطه 2، که بتواند "حداقل مجموعه-برش واقعی" را تعیین کند (مفهوم "حداقل مجموعه-برش" در اصل در سیستم‌های همسان استفاده می‌گردد) استفاده می‌گردد. و سپس با استفاده از رابطه احتمال اجتماع رویدادها (رابطه 3)، احتمال رخداد رویداد اصلی محاسبه می‌گردد. از تابع ساختار مجموع احتمالات برای رویداد اصلی داریم [2]:

$$\varphi(x) = \sum_{i=1}^{k} Y_i \qquad (3)$$

در رابطه فوق، Y_i، iامین حداقل مجموعه-برش و k مجموع تعداد حداقل مجموعه-برش‌های تابع ساختار می‌باشد. از این‌رو، رابطه 4 را برای احتمال رویداد اصلی داریم:

$$P_{\mathrm{TOP}} = \sum_{i=1}^{k} P(Y_i) - \underbrace{\sum_{i=2}^{k}\sum_{j=1}^{i-1} P(Y_i Y_j)}_{\text{ترمهای اشتراکی}} + \cdots + (-1)^{n-1} P(Y_1 \dots Y_k) \qquad (4)$$

زمانی که رابطه 4 محاسبه می‌گردد، رابطه 5 باید مورد استفاده قرار گیرد.

$$\begin{aligned} & P(x_{li}) = \alpha_{li} F_l \\ & \sum_{i=1}^{M_l} \alpha_{li} = 1 \end{aligned} \qquad (5)$$

$P(x_{li})$: احتمال رخداد iامین مد خرابی جزء l می‌باشد. α_{li}: ضریب مد iامین مد خرابی جزء l و F_l: احتمال خرابی جزء l می‌باشد.

برای مثال، سیستم تشخیص شرایط اضطراری (EDS[3]) یک فضاپیما را درنظر بگیرید که به صورت "اتوماتیک" بر وضعیت اجزاء و متعلقات فضاپیما نظارت داشته و در شرایط بحرانی، سیگنال‌های هشدار و فرمان پرتاب سیستم فرار فضاپیما را صادر می‌کند[9]. راه‌اندازی خودکار درصورتی وارد عمل می‌شود که یکی از حالت‌های: ازدست دادن نیروی پیشران اصلی، وارد شدن نرخ‌های زاویه‌ای بسیارزیاد به وسیله، و سیگنال ایراد الکتریکی تشخیص داده شود[10]. دیاگرام ساده‌سازی شده برای EDS در شکل 1 نشان داده شده است. با توجه به شکل 1، رویداد اصلی این‌طور تعریف می‌شود که سیستم قادر به تشخیص و انتقال سیگنال‌ها از بخش‌های مربوطه (از دست رفتن نیروی پیشران، خرابی الکتریکی، و نرخ‌های زاویه‌ای بالا) به نشاندهندهٔ داخل

1- Fault tree analysis
2- Binary Decision Diagram
3- Emergency Detection System

ماژول خدمه نباشد (به‌عبارت دیگر، نشاندهنده[1] EDSI هیچ هشداری را نشان ندهد). درخت خطای مربوط به این سیستم در شکل 2 نمایش داده شده است.

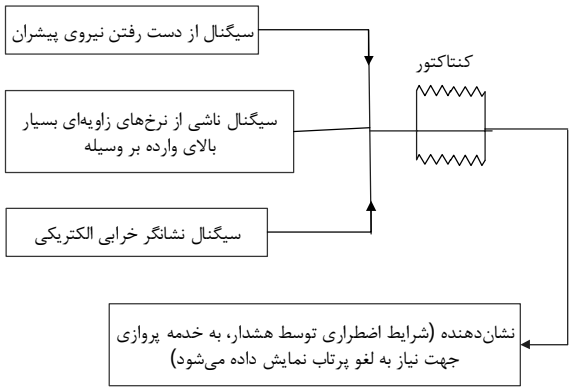
رویدادهای پایه‌ای سیستم عبارتند از x_1: سیگنال خرابی مربوط به از دست دادن نیروی پیشران، x_2: سیگنال خرابی مربوط به خرابی الکتریکی، x_3: سیگنال خرابی مربوط به نرخ زوایای بالا برای کل سیستم، x_{41}: خرابی سوئیچ الکتریکی (کنتاکتور) که در حالت- بالا بسته شود، و x_{42}: خرابی کنتاکتور که در حالت-پائین بسته بماند. براساس درخت خطای شکل 2، مجموعه (مسیر) شکست حداقلی طبق روابط زیر عبارتند از:

$$C(1): Y_1 = (X_1, X_2, X_3)$$
$$C(2): Y_2 = (X_1, X_2, X_{41})$$
$$C(3): Y_3 = (X_1, X_2, X_{42})$$
$$C(4): Y_4 = (X_1, X_{41}, X_3)$$
$$C(5): Y_5 = (X_1, X_{42}, X_3)$$
$$C(6): Y_6 = (X_{41}, X_2, X_3)$$
$$C(7): Y_7 = (X_2, X_3, X_{42})$$
$$C(8): Y_8 = (X_{41}, X_{42})$$

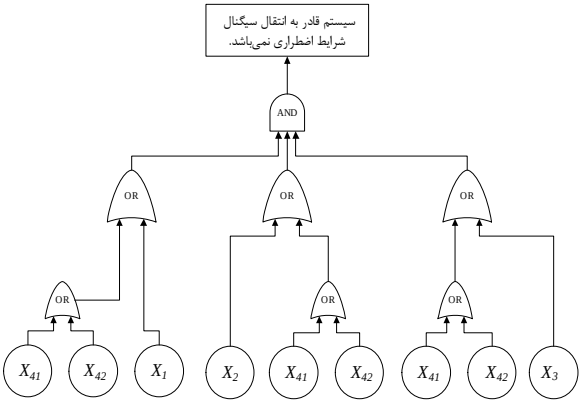
فرض کنید که احتمال خرابی هر یک از بخش‌های ازدست‌رفتن نیروی پیشران، خرابی الکتریکی، و نرخ‌های زاویه‌ای بالا در حین پرواز فضاپیما، برابر 0/02 باشد. یعنی، $P(x_1) = P(x_2) = P(x_3) = 0.02$، و احتمال خرابی کنتاکتور در هر دو حالت یکسان و برابر $F(x_{41}) = F(x_{42}) = 0.01$ باشد. همچنین ضریب حالت برای iامین حالت خرابی جزء چهارم، مقادیر زیر باشند.

$$\begin{cases}\alpha_{41} = 0.8 \\ \alpha_{42} = 0.2\end{cases} \Rightarrow \sum_{i=1}^{M_l} \alpha_{li} = 1$$

مقادیر $P(x_{41})$ و $P(x_{42})$ از رابطه 5 قابل محاسبه می‌باشد.



شکل 1 دیاگرام ساده‌سازی شده برای سیستم تشخیص شرایط اضطراری



شکل 2 درخت خطای سیستم تشخیص شرایط اضطراری

1- Emergency Detection System Instrument

$$P(x_{41}) = \alpha_{41}F(x_{41}) = 0.8(0.01) = 0.008$$
$$P(x_{42}) = \alpha_{42}F(x_{42}) = 0.2(0.01) = 0.002$$

در این‌صورت، اگر فرض شود که رویدادها دوبه‌دو ناسازگار باشند، فقط ترم اول رابطه 4 برای محاسبه P_{TOP} مورد استفاده قرار گرفته و مقدار زیر برای P_{TOP} بدست می‌آید.

$$\begin{aligned}P_{\text{TOP}} = \sum_{i=1}^{k} P(Y_i) &= P(X_1,X_2,X_3) + P(X_1,X_2,X_{41}) \\ &+ P(X_1,X_2,X_{42}) + P(X_1,X_{41},X_3) \\ &+ P(X_1,X_{42},X_3) + P(X_{41},X_2,X_3) \\ &+ P(X_2,X_3,X_{42}) + P(X_{41},X_{42}) \\ &= (0.8 + 0.32 + 0.08 + 0.32 + 0.08 \\ &+ 0.32 + 0.08 + 0.0256) \times 10^{-5} \\ &= 2.0256 \times 10^{-5}\end{aligned}$$

و اگر فرض شود که رویدادها دوبه‌دو مشترک باشند، طبق رابطه 4 مقدار زیر برای P_{TOP} بدست می‌آید.

$$P_{\text{TOP}} = \sum_{i=1}^{k} P(Y_i) - \underbrace{\sum_{i=2}^{k}\sum_{j=1}^{i-1} P(Y_iY_j)}_{\text{ترمهای اشتراکی}} + \sum_{i=3}^{k}\sum_{j=2}^{i-1}\sum_{n=1}^{j-1} P(Y_iY_jY_n)$$

که

$$\begin{cases}\underbrace{\sum_{i=1}^{k} P(Y_i)}_{8\text{ ترم}} = (2.0256 \times 10^{-5}) \\ \underbrace{\sum_{i=2}^{8}\sum_{j=1}^{i-1} P(Y_iY_j)}_{28\text{ ترم}} = (1.5680 \times 10^{-5}) \\ \underbrace{\sum_{i=3}^{k}\sum_{j=2}^{i-1}\sum_{n=1}^{j-1} P(Y_iY_jY_n)}_{56\text{ ترم}} = (0.6097 \times 10^{-5})\end{cases}$$

$$\Rightarrow P_{\text{TOP}} = [(2.0256) - (1.5680) + (0.6097)] \times 10^{-5} = 1.0673 \times 10^{-5}$$

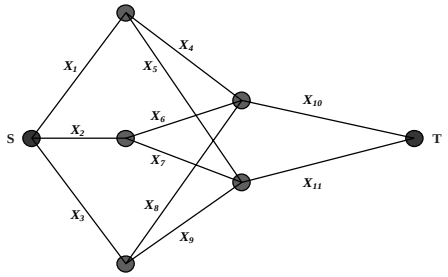
نوع خرابی و مقادیر مربوط به احتمال وقوع هر خرابی برای زیرسیستم‌های تشخیص شرایط اضطراری در جدول 1 آورده شده است.

برای نمایش ارتباط بین اجزاء و المان‌های سیستم تشخیص شرایط اضطراری می‌توان از مدل‌سازی رویدادهای گسسته شبکه‌ای نیز استفاده کرد. همان‌طور که در شکل 3 نشان داده شده است شبکهٔ مربوطه دارای 7 گره و 11 لینک (انتقال بین حالت‌ها) می‌باشد.

همان‌طور که در بخش قبل اشاره شد، سیستم چندحالتی منسجم در برخی از مراجع مورد بررسی قرار گرفته است [1,11-15]. اما، همیشه شرایط نرمال برای هر یک از اجزاء در درخت خطا اتفاق نمی‌افتد. لذا برای توسعه این‌حالت به درخت خطای سیستم چندحالتی منسجم، باید انجام شود. اختلاف بین این دو حالت در این است که، نه‌تنها هر مد خرابی از اجزاء باید درنظر گرفته شود بلکه به‌همان اندازه، حالت نرمال آنها همانند رویداد پایه‌ای

جدول 1 نوع خرابی و احتمال وقوع ایراد در زیرسیستم‌های EDSI

نوع خرابی	احتمال وقوع خرابی	ضرایب مدها	
		α_{i1}	α_{i2}
سیگنال ازدست دادن نیروی پیشران اصلی	0/02	1	1
سیگنال واردشدن نرخ‌های زاویه‌ای بسیارزیاد	0/02	1	1
سیگنال ایراد الکتریکی	0/02	1	1
خرابی کنتاکتور	0/01	0/8	0/2



شکل 3 مدل شبکه‌ای معادل برای درخت خطای سیستم مذکور

باید مدّ نظر قرار گیرد. صحت این تعمیم باید قابل اثبات باشد. برای این منظور، از ترم "دلیل اصلی[1]" به‌جای ترم "مجموعه (مسیر) شکست حداقلی" استفاده می‌گردد.

3- روش درخت خطای مناسب برای سیستم چندحالتی

سیستمی متشکل از n جزء را فرض کنید. که $\tilde{\Omega}$ فضای حالت سیستم باشد، در این‌صورت، رابطه 6 را برای فضای حالت کل سیستم می‌توان استخراج کرد[5]:

$$\tilde{\Omega} = \Omega_1 \times \Omega_2 \times \dots \times \Omega_n \quad (6)$$

و رویدادهای پایه‌ای فضای $\tilde{\Omega}$ بردارهایی n بعدی، همچنین براساس رابطه 7 می‌توان X را رویداد پایه‌ای قرار داد، سپس

$$X = (x_{11i}, \dots, x_{lli}, \dots, x_{nni}) \quad l_i \in (0,1, \dots, M_l) \quad l \in (1,2, \dots, n) \quad (7)$$

فرض کنید $N_{\tilde{\Omega}}$ نشانگر تعداد کل رویدادهای پایه‌ای درفضای $\tilde{\Omega}$ باشد. در این‌صورت، رابطه 8 بدیهی است.

$$N_{\tilde{\Omega}} = \prod_{i=1}^{n}(1 + M_i) \quad (8)$$

فرض کنید X_s رویداد پایه‌ای باشد که باعث موفقیت سیستم می‌شود، و X_f رویداد پایه‌ایی باشد که باعث شکست سیستم می‌شود (اهمیتی ندارد که چه نوع شکست یا خرابی ظاهر می‌شود). همچنین، $\tilde{\Omega}_s$ و $\tilde{\Omega}_f$ نشانگر دو زیرفضا از فضای $\tilde{\Omega}$ باشند (روابط 9 تا 12) که

$$\tilde{\Omega}_s = \left(X_s \mid X_s \in \tilde{\Omega} \right) \quad (9)$$

$$\tilde{\Omega}_f = \left(X_f \mid X_f \in \tilde{\Omega} \right) \quad (10)$$

بدیهی است که

$$\tilde{\Omega} = \tilde{\Omega}_s + \tilde{\Omega}_f \quad (11)$$

$$\tilde{\Omega}_s \cap \tilde{\Omega}_f = \emptyset \quad (12)$$

براساس تعاریف فوق، می‌توان مشاهده کرد که هر حالت خرابی سیستم با زیرفضایی از فضای $\tilde{\Omega}_f$ مرتبط است. با فراخوانی این زیرفضاهای رویدادها، و با استفاده از نماد $\tilde{\Omega}_{fi}$ می‌توان نشان داد که

$$\tilde{\Omega}_{fi} \subset \tilde{\Omega}_f \quad i \in (1, \dots, k) \quad (13)$$

k تعدادکل حالت‌های خرابی سیستم می‌باشد.

از آنجائی که هدف آنالیز یک سیستم چندحالته به‌کمک روش درخت خطا است، اولین گام تعیین حالت‌های خرابی برطبق نیازمندی سیستم می‌باشد، لازم بذکر است که تعریف درست و کامل از حالت‌های خرابی سیستم چندحالتی باید رابطه 14 را ارضا کند،

$$\tilde{\Omega}_f = \bigcup_{i=1}^{k} \tilde{\Omega}_{fi} \quad (14)$$

در این مرحله، دو روش ممکن است مورد استفاده قرار گیرد:

1. تعریف حالت‌های خرابی سیستم برطبق مأموریت‌ها یا پیدایش خرابی سیستم صورت گیرد. برای مثال، یک هواپیمای چند مأموریتی برای شناسایی، بمب‌افکن، و رهگیری طراحی شده باشد، در این‌صورت می‌توان سه حالت خرابی: نقص در مأموریت شناسایی، نقص در مأموریت بمب‌افکن، و نقص در مأموریت رهگیری را برای هواپیما تعریف کرد. یکی از شکل‌های قابل توجه این نوع تعریف این است که حالت‌های خرابی سیستم اغلب رویدادهای اشتراکی هستند، همان‌طور که در شکل 4 نمایش داده شده است.
2. تعریف حالت‌های خرابی سیستم برطبق درجه فرسودگی سیستم صورت گیرد. برای مثال، می‌توان حالت‌های خرابی سیستم را همانند خرابی‌های سبک، معمولی و سنگین تعریف کرد؛ یکی از شکل‌های قابل توجه این نوع تعریف این است که حالت‌های خرابی سیستم اغلب رویدادهای دوبه‌دو ناسازگار هستند، همان‌طور که در شکل 5 نمایش داده شده است.

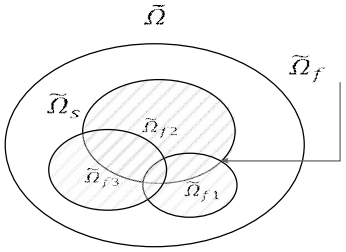
گام دوم از آنالیز یک سیستم چندحالته به‌کمک درخت خطا، انتخاب تمام حالت‌های مختلف خرابی سیستم به‌عنوان رویدادهای اصلی می‌باشد. سپس درخت خطا برمبنای رویدادهای اصلی ساخته می‌شود. پس از انجام این مرحله، آن‌را ساده کرده و احتمال رخداد هر رویداد اصلی براساس روش اشاره شده در بخش 2- محاسبه می‌گردد.

قضایای زیر برخی از خواص بسیار مفید در مورد درخت‌های خطای سیستم‌های چند حالتی را بیان می‌کنند[5].

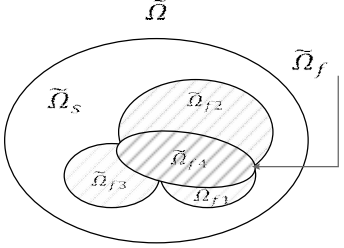
قضیه 1. اجازه دهید $(\text{TOP})_a$ و $(\text{TOP})_b$ نشانگر دو رویداد اصلی متعلق به همان فضای $\tilde{\Omega}_f$ باشند. و φ_a نشانگر تابع ساختار $(\text{TOP})_a$، و φ_b نشانگر تابع ساختار $(\text{TOP})_b$ باشند. اجازه دهید Y_{al} دلیل اصلی φ_a، $l \in (1, \dots, a_n)$، که a_n تعداد کل دلایل عمدهٔ φ_a باشد. و اجازه دهید Y_{bm} عمده دلیل φ_b، $m \in (1, \dots, b_n)$، که b_n تعداد کل دلایل عمدهٔ φ_b باشد. سپس، شرط کافی و لازم که باعث می‌شود رویدادهای اصلی $(\text{TOP})_a$ و $(\text{TOP})_b$ دوبه‌دو ناسازگار باشند عبارت است از:

$$Y_{al} \cap Y_{bm} = \emptyset \quad l \in (1, \dots, a_n) \quad m \in (1, \dots, b_n) \quad (15)$$

برای اثبات این قضیه داریم



شکل 4 رویدادهای اشتراکی سیستم چندحالتی



شکل 5 سیستم چندحالتی با رویدادهای انحصاری

1- Prime Implicant

$$\varphi_a = \bigcup_{i=1}^{a_n} Y_{al} \quad (16)$$

$$\varphi_b = \bigcup_{m=1}^{b_n} Y_{bm} \quad (17)$$

داریم

$$\begin{aligned}(\text{TOP})_a \cap (\text{TOP})_b &= \varphi_a \cap \varphi_b \\ &= \left(\bigcup_{i=1}^{a_n} Y_{al}\right) \cap \left(\bigcup_{m=1}^{b_n} Y_{bm}\right) \\ &= \bigcup_{i=1}^{a_n}\bigcup_{m=1}^{b_n} (Y_{al} \cap Y_{bm})\end{aligned} \quad (18)$$

با توجه به روابط 15 و 18 داریم

$$(\text{TOP})_a \cap (\text{TOP})_b = \varphi_a \cap \varphi_b = \emptyset \quad (19)$$

اگر اشتراکی وجود داشته باشد:

$$Y_{ai} \cap Y_{bi} \neq \emptyset \quad (20)$$

پس، از رابطه 18 داریم

$$(TOP)_a \cap (TOP)_b = Y_{ai} \cap Y_{bi} \neq \emptyset \quad (21)$$

این رابطه در تضاد با رابطه 19 بوده و در نتیجه:

نتیجه 1. در یک سیستم منسجم که اجزاء آن تنها دو حالت دارند، رویدادهای اصلی مختلف آن همیشه رویدادهای مشترک می‌باشند. صحّت این نتیجه کاملاً آشکار است. در این سیستم‌ها، هر دلیل اصلی (حداقل مجموعه-برش) از هر رویداد اصلی شامل حالت خرابی اجزاء بوده، سپس، تمام مجموعه‌های-برش بطور متقابل مشترک می‌باشند. بنابراین، نمی‌توان از درخت خطای منسجم معمولی برای آنالیز سیستم‌های چندحالتی که حالت‌های خرابی دوبه‌دو ناسازگار می‌باشند استفاده کرد.

قضیه 2. فرض کنید سیستمی متشکل از n جزء باشد، و جزء l شامل M_l مد خرابی باشد، $l \in (1, \dots, n)$، سپس، در طی آنالیز، حداکثر تعداد رویدادهای اصلی که ممکن است انتخاب شوند عبارت است از

$$N_{TOP_{max}} = 2^{(\prod_{i=1}^{n}(1+M_i)-1)} - 1 \quad (22)$$

برای اثبات این قضیه از رابطه 8 استفاده می‌شود. و برای هر سیستم، رویدادهای پایه‌ای عبارتند از:

$$X_{s0} = (X_{10}, X_{20}, \dots, X_{n0}) \quad (23)$$

که همیشه باعث می‌شود سیستم موفق عمل کند. برای تشریح این موضوع سیستم ساده‌ای موردی بررسی قرار می‌گیرد که دارای ساختار سری می‌باشد و هر جزء و مد خرابی متفاوت باشند، سپس تمام رویدادهای پایه‌ای، بجزء X_{s0} (که در این‌حالت سیستم دچار خرابی شده است) مورد بررسی قرار می‌گیرد. یعنی

$$\tilde{\Omega}_{s_{min}} = (X_{s0}) \quad (24)$$

$$\tilde{\Omega}_{f_{max}} = \left(X \mid X \in \tilde{\Omega}, X \neq X_{s0}\right) \quad (25)$$

سپس

$$N_{\tilde{\Omega}_{f_{max}}} = N_{\tilde{\Omega}} - 1 = \prod_{i=1}^{n}(1 + M_i) - 1 \quad (26)$$

فرض کنید $\wp(\tilde{\Omega}_f)$ نشان‌دهندهٔ فضای حالت کلی برای $\tilde{\Omega}_f$ باشد. المان‌های فضای $\Theta(\tilde{\Omega}_f)$ همگی زیرفضاهایی از فضای $\tilde{\Omega}_f$ می‌باشند. یعنی

$$\wp(\tilde{\Omega}_f) = \left(\tilde{\Omega}_{f_i} \mid \tilde{\Omega}_{f_i} \subset \tilde{\Omega}_f\right) \quad (27)$$

براساس قضیه مجموعه‌ها، داریم

$$N_{\wp(\tilde{\Omega}_f)} = 2^{N_{\tilde{\Omega}_f}} \quad (28)$$

بنابراین

$$N_{\wp(\tilde{\Omega}_{f_{max}})} = 2^{(\prod_{i=1}^{n}(1+M_i)-1)} \quad (29)$$

با کم کردن مجموعهٔ تهی از رابطه 29، داریم:

$$N_{TOP_{max}} = 2^{(\prod_{i=1}^{n}(1+M_i)-1)} - 1$$

نتیجه 2. اگر سیستمی متشکل از n جزء باشد که اجزاء آن تنها دو حالت دارند (موفقیت یا شکست)، در این‌صورت

$$N_{\wp(\tilde{\Omega}_{f_{max}})} = 2^{(2^n-1)} \quad (30)$$

برای اثبات این حالت، هر جزئی فقط یک مد خرابی دارد، یعنی

$$M_l = 1 \quad \text{for all } l \quad (31)$$

با جاگذاری این رابطه، در رابطه 22 و 30 خواهیم داشت:

$$N_{\text{TOP}_{\max}} = 2^{(2^n-1)} - 1$$

نتیجه 3. اگر حالت‌های خرابی یک سیستم رویدادهای دوبه‌دو ناسازگار باشند، مجموع تعداد رویدادهای اصلی که ممکن است انتخاب شود عبارت است از:

$$N_{\text{TOP}} = N_{\tilde{\Omega}_f} \quad (32)$$

برای اثبات این موضوع، با توجه به این حقیقت که رویداد پایه‌ای از یک فضای حالت یک المان بسیار پایه‌ای می‌باشد، و تمام رویدادهای پایه‌ای دوبه دو ناسازگار هستند، صحت این نتیجه واضح و روشن است. از قضایا و نتایج فرعی پیداست که تعریف حالت خرابی یک سیستم ممکن است بسیار انعطاف‌پذیر باشد. به زبان تئوری، روش فوق‌الذکر ممکن است برای آنالیز هر سیستم چند حالتی فارغ از اینکه چه ساختار پیچیده‌ای داشته باشد و چه تعداد حالت‌های خرابی ممکن است اتفاق بیافتد مورد استفاده قرار گیرد.

4- درخت خطای منسجم برای سیستم چندحالتی

درخت خطای همسان (CFT[1]) به‌همراه گیت‌های منطقی که در درخت‌های خطای منسجم بکار گرفته می‌شود، مشخص می‌گردند. این درخت ممکن است شامل سیستم *k*-out-of-*n* باشد[16]. علاوه براین، سیستم‌های غیرهمسان اغلب برای آنالیز دقیق رویدادهای گسسته [17]، رویدادهای وابسته [18]، و درخت‌های رویداد مورد استفاده قرار می‌گیرند[19]. تابع ساختار سیستم غیرمنسجم با افزایش تعداد اجزاء عملیاتی، دارای روند افزایشی یکنواختی نمی‌باشد. سیستم‌های غیرمنسجم بطور رایج در سیستم‌هایی با منابع محدود، چند مأموریتی و سیستم‌هایی با کاربردهای در حوزهٔ ایمنی مورد استفاده قرار می‌گیرند[20]. برای مثال، در سیستم تشخیص شرایط اضطراری به‌منظور دریافت سیگنال از هر یک از زیرسیستم‌های اساسی، می‌توان از سیستم *k*-to-*l*-out-of-*n* برای تشخیص ایراد در هر یک از سه بخش فرستنده سیگنال (نیروی پیشران اصلی، وارد شدن نرخ‌های زاویه‌ای بسیار زیاد به وسیله، و سیگنال ایراد الکتریکی) استفاده کرد. که *n*: تعداد کل سنسورها (در این مورد فرض می‌شود که *n*=3) برای شناسایی ایراد در هر یک از بخش‌ها، و *l*=*k*=2 حداقل تعداد سنسور لازم برای شناسایی ایراد باشند. ساختار این سیستم در شکل 6 آورده شده است.

اگر کمتر از حد معین *k* سنسور مورد استفاده قرار گیرد، سیستم در بهترین حالت نبوده و سیگنال فرستاده نخواهد شد؛ از سوی دیگر، اگر تعداد سنسورها بیشتر از *l* باشد، مشکلی در فرآیند شناسایی ایراد نداشته و نشانگر بروز حتمی ایراد در بخش مربوطه می‌باشد. در تحلیل درخت خطای این سیستم، عدم فرستادن سیگنال می‌تواند ناشی از دو حالت: یا اینکه هیچ سیگنالی که نشانگر ایراد باشد وجود ندارد، و یا اینکه حداقل دو سنسور

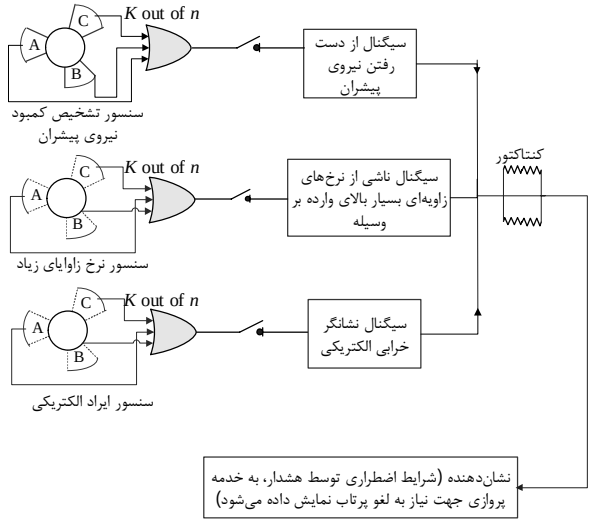
1- Coherent Fault Trees

سیگنال را دریافت نکرده باشند وجود دارد (2-out-of-3). برای تعیین احتمال رخداد رویداد اصلی، آنالیز کمّی مورد استفاده قرار خواهد گرفت. بطور گسترده، سه رویکرد کمّی برای آنالیز درخت خطای سیستم‌های پیچیده وجود دارد: روش‌های برمبنای فضای حالت [22،21]، روش‌های ترکیبی [23]، و روش‌های مدولار [25،24] (ترکیبی از دو روش فوق) که بیشتر برای درخت خطاهای دینامیکی کاربرد دارند [26،16]. برای آنالیز کمّی سیستم فوق که یک درخت خطای استاتیکی است از روش حداقل مجموعه-برش یا دیاگرام تصمیم باینری می‌توان استفاده کرد. درخت خطای منسجم مربوط به این سیستم چندحالتی در شکل 7 نمایش داده شده است. برای تحلیل درخت خطای چندحالته استاتیکی از یک روش ترکیبی به‌کمک روش مجموعه-برش و BDD استفاده خواهد شد.

رویدادهای x_1، x_2 و x_3 سیستم‌های تشخیص سیگنال در هر یک از زیرسیستم‌ها بوده و از نوع k-out-of-n می‌باشند. این سه بخش یکسان بوده و برای تحلیل آنها روش BDD مورد استفاده قرار گرفته است. روش‌های برمبنای BDD نیازمند حافظه و زمان محاسباتی کمتری می‌باشند و برای تحلیل درخت خطاهای بزرگ راه‌حل کارآمدی را فراهم می‌آورند. برای انجام آنالیز کمّی از درخت خطای استاتیکی فوق به‌کمک BDD، ابتدا درخت خطا را به BDD تبدیل کرده و سپس، BDD بدست آمده برای محاسبه عدم‌قابلیت اطمینان مورد ارزیابی قرار می‌گیرد.

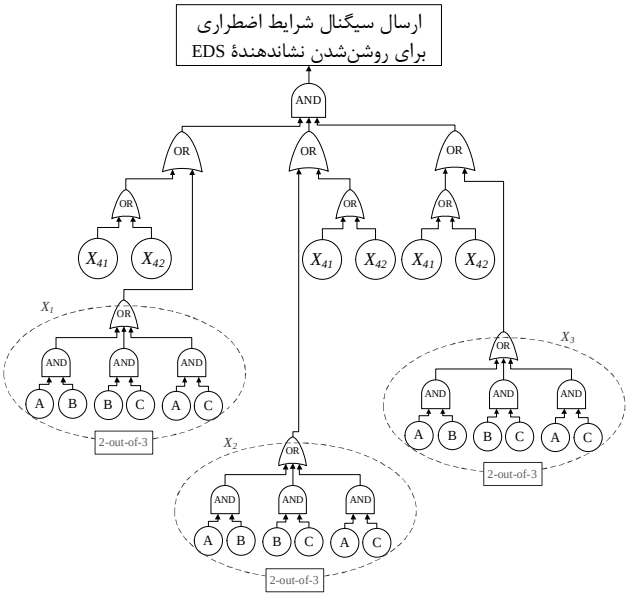
4-1 تبدیل درخت خطا به BDD

برای تبدیل درخت خطا از روش BDD مرتب‌شده (OBDD[1]) با این قید که متغیرها براساس شاخص احتمال رخداد مرتب شده‌اند استفاده می‌شود. ابتدا باید ترتیب متغیرها/اجزاء انتخاب گردد. استراتژی ترتیب برای تولید OBDD بسیار مهم می‌باشد زیرا اندازهٔ OBDD وابستگی بسیارشدیدی به ترتیب متغیرهای ورودی دارد. مرتب‌سازی ضعیف تأثیر قابل توجهی در اندازه BDD داشته و زمان حل آنالیز قابلیت اطمینان را برای سیستم‌های بزرگ بیشتر می‌کند[16]. برای بخش 2-out-of-3، که دارای سه المان A، B، و C هم‌نوع می‌باشد فرض می‌شود که قید شاخص احتمال رخداد، A<B<C (برای مثال، اگر A و B توسط یک گیت AND با هم ارتباط داشته باشند، المان A ریشه



شکل 6 دیاگرام ساده‌سازی شدهٔ منسجم برای سیستم چندحالتی تشخیص شرایط اضطراری یک فضاپیما

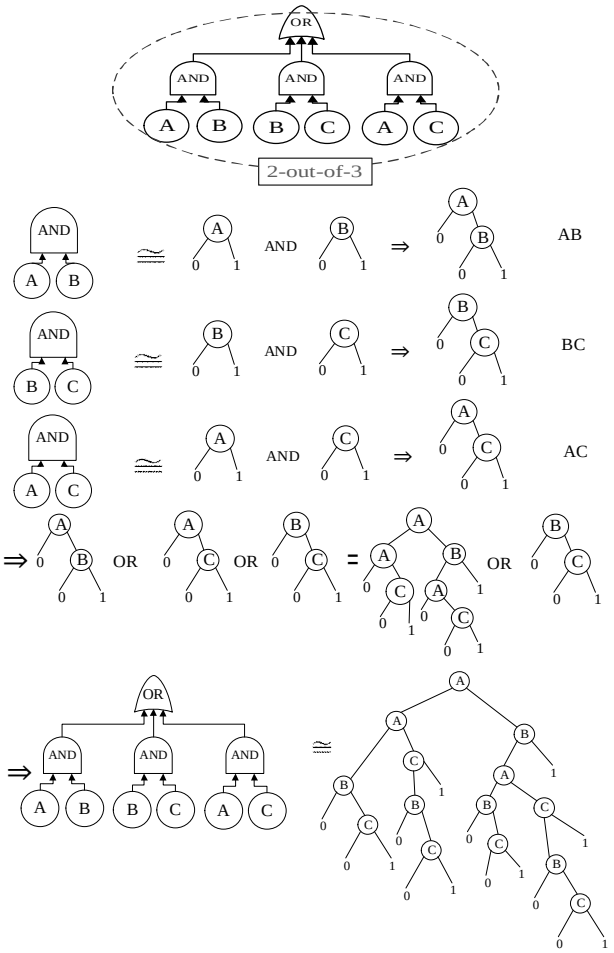
1. Ordered Binary Decision Diagram



شکل 7 درخت خطای سیستم چندحالتی منسجم تشخیص شرایط اضطراری یک فضاپیما

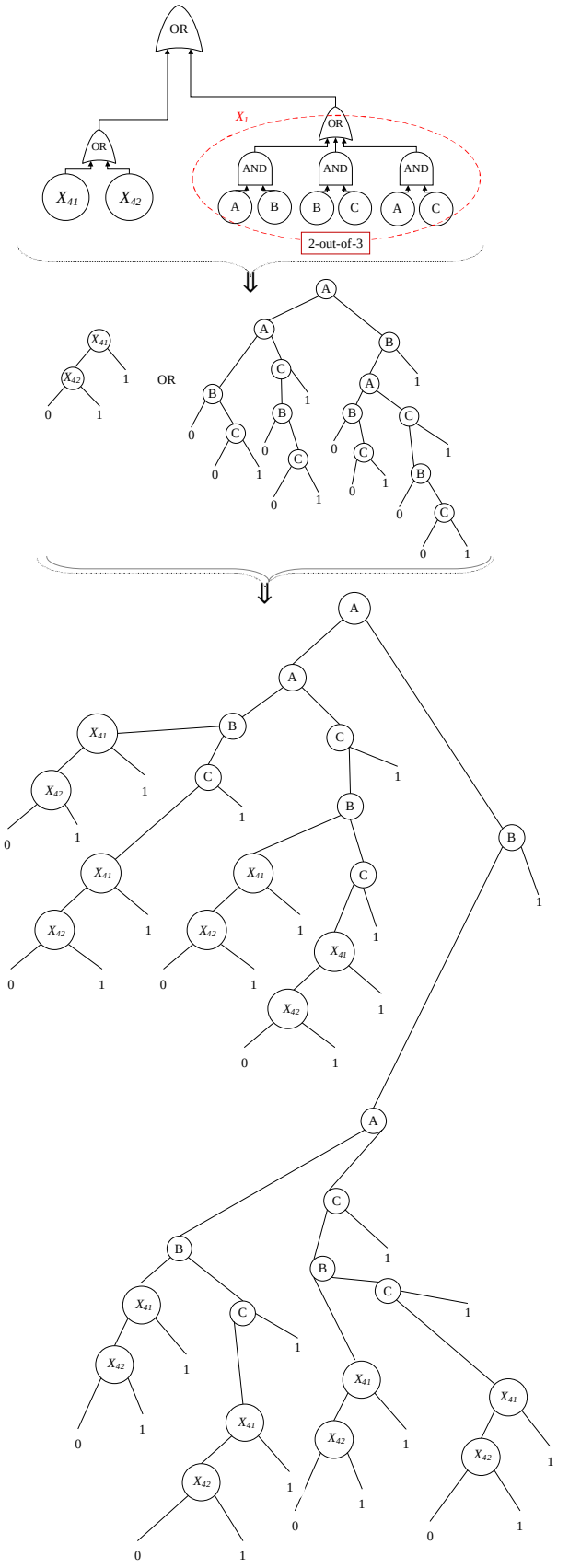
شده و B به قسمت باینری 1 المان A متصل می‌گردد) برای این المان‌ها وجود دارد. درنتیجه، برای درخت خطای بخش 2-out-of-3 (شکل 8) داریم.

به‌همین ترتیب و با استفاده از دیاگرام تصمیم باینری برای هر یک از زیربخش‌های ورودی گیت AND برای رخداد رویداد اصلی، ساختار شکل-8 را می‌توان براساس OBDD بدست آورد.



شکل 8 ساختار OBDD برای درخت خطای بخش 2-out-of-3

شکل 9 نشانگر ساختار BDD فقط برای یکی از شاخه‌های درخت خطای مربوط به سیستم چندحالته در شکل 7 می‌باشد.



شکل 9 ساختار OBDD برای هر یک از زیربخش‌ها

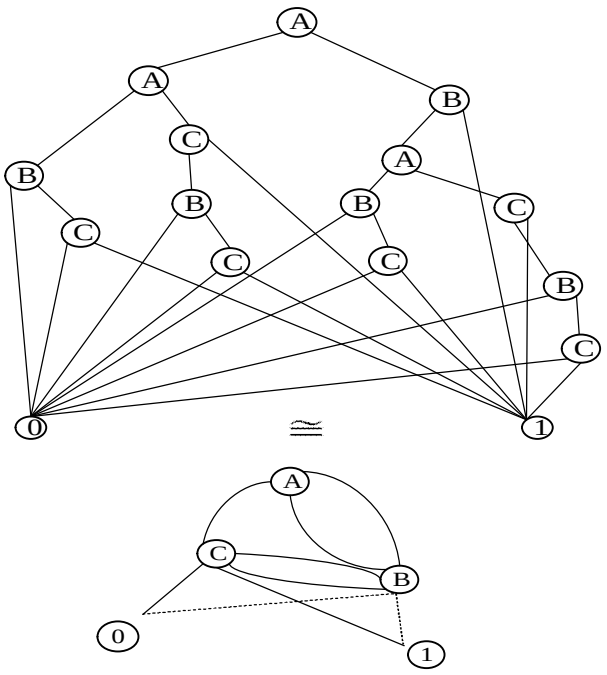
اگر ساختار BDD برای کل سیستم ترسیم گردد، در این‌صورت، سیستمی با پیچیدگی بالا و ترم‌های اشتراکی بسیاری به‌وجود خواهد آمد که تحلیل چنین سیستمی چه به روش حداقل مجموعه-برش و چه با استفاده از روش BDD بسیار زمان‌بر و دارای تحلیل بسیار مشکلی به لحاظ ترم‌های اشتراکی بوده و همچنین نتایج بدست آمده از دقت کمتری برخوردار خواهند بود. برای غلبه بر این مشکل، یک روش ترکیبی برای تحلیل درخت خطای استاتیکی فوق مورد استفاده قرار خواهد گرفت. در این روش، حداقل مجموعه-برش با روش BDD ادغام شده و احتمال رخداد رویداد اصلی مورد محاسبه قرار می‌گیرد.

2-4 تشکیل درخت خطای OBDD کاهش‌یافته

با ساخت OBDD برای سیستم مربوطه، قانون کاهش را به‌منظور حداقل ساختن برای ترتیب می‌توان بکار گرفت. به‌دلیل بیان جبر بولی، درخت‌های متناظر در شکل 8، باهم ادغام شده و زیر-OBDDها و ترم‌های زائد حذف می‌شوند. در این‌صورت درخت خطای مرتب‌شدهٔ کاهش یافته (ROBDD[1]) برای زیرسیستم بخش 2-out-of-3 همانند شکل 10 می‌باشد.

برای ساختار درخت خطای بخش 2-out-of-3 فوق و با فرض اینکه احتمال خرابی برای هر یک از اجزاء $P(A) = P(B) = P(C) = 0.02$ باشد، جدول 2 ترکیبی (جدول درستی) زیر را می‌توان براساس دیاگرام BDD فوق تشکیل داد و حالت‌های شکست یا موفقیت را تعیین کرد. نکته اینکه S حالت موفقیت، و F حالت خرابی می‌باشند. براساس جدول 2، ترکیب‌های 4، 6، 7، و 8 منجر به رخداد رویداد خرابی از این بخش می‌شود (رویداد اصلی این بخش می‌باشد).

بنابراین، برای تحلیل درخت خطای کل سیستم، درخت خطای بخش 2-out-of-3 را با استفاده از روش تحلیل BDD انجام داده و حالت‌های خرابی این بخش که نشانگر رخداد رویداد اصلی مربوط به این بخش است، به‌عنوان یک ورودی به درخت خطای کل سیستم وارد می‌شود.



شکل 10 ساختار ROBDD برای درخت خطای بخش 2-out-of-3

1- Reduced Ordered Binary Decision Diagram

جدول 2 ترکیب، حالات و احتمال رخداد برای درخت خطای بخش 2-out-of-3

تعداد ترکیب	حالت‌های سیستم	احتمال C_i	عملکرد سیستم
1	$A_S B_S C_S$	0/681472	*S*
2	$A_S B_S C_F$	0/015488	*S*
3	$A_S B_F C_S$	0/015488	*S*
4	$A_S B_F C_F$	0/000352	*F*
5	$A_F B_S C_S$	0/015488	*S*
6	$A_F B_S C_F$	0/000352	*F*
7	$A_F B_F C_S$	0/000352	*F*
8	$A_F B_F C_F$	0/000008	*F*

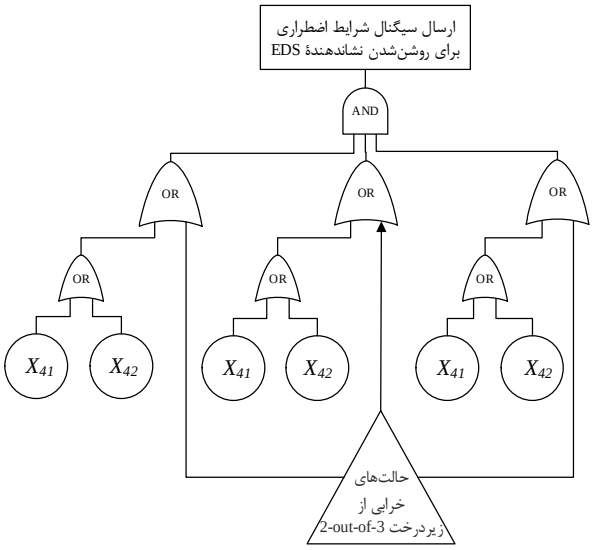
برای نمایش این تحلیل ترکیبی، روش حداقل مجموعه-برش برمبنای دیاگرام تصمیم باینری (CSBDD[1]) برای این سیستم پیچیده با ترم‌های اشتراکی زیاد، درخت خطای شکل 7 را می‌توان همانند شکل 11 ساده‌سازی کرد.

براساس شکل 11 حداقل مجموعه‌های-برش (رابطه 6) عبارتند از:

$$C(1): Y_1 = (F_1, F_2, F_3)$$
$$C(2): Y_2 = (F_1, F_2, X_{41})$$
$$C(3): Y_3 = (F_1, F_2, X_{42})$$
$$C(4): Y_4 = (F_1, X_{41}, F_3)$$
$$C(5): Y_5 = (F_1, X_{42}, F_3)$$
$$C(6): Y_6 = (X_{41}, F_2, F_3)$$
$$C(7): Y_7 = (F_2, F_3, X_{42})$$
$$C(8): Y_8 = (X_{41}, X_{42})$$

که در رابطه فوق، F_1, F_2, F_3 حالت‌های خرابی برای هر کدام از بخش‌های 2-out-of-3 می‌باشند. بیشترین مقداری که برای حالت خرابی این زیرسیستم براساس جدول 2 وجود دارد، مقدار 0/000352 می‌باشد.

بنابراین، فرض می‌شود که احتمال خرابی هر یک از این بخش‌ها برابر 0/000352 باشد. یعنی، $P(F_1) = P(F_2) = P(F_3) = 0.000352$، که بیانگر حد بالای خرابی برای این زیرسیستم‌ها است. و احتمال خرابی کنتاکتور در



شکل 11 ساختار ترکیبی درخت خطای سیستم چندحالتی غیرمنسجم تشخیص شرایط اضطراری یک فضاپیما

هر دو حالت یکسان و برابر $F(x_{41}) = F(x_{42}) = 0.01$ باشد (همانند سیستم قبلی). با توجه به اینکه رویدادها دوبه‌دو مشترک می‌باشند، از رابطه مربوط به رویدادهای مشترک برای رخداد رویداد اصلی استفاده می‌شود، طبق رابطه 4 مقدار زیر برای P_{TOP} بدست می‌آید.

$$P_{\mathrm{TOP}} = \sum_{i=1}^{k} P(Y_i) - \underbrace{\sum_{i=2}^{k}\sum_{j=1}^{i-1} P(Y_i Y_j)}_{\text{ترمهای اشتراکی}} + \sum_{i=3}^{k}\sum_{j=2}^{i-1}\sum_{n=1}^{j-1} P(Y_i Y_j Y_n)$$

$$\Rightarrow P_{\mathrm{TOP}} = [(0.02) - (0.006) + (0.0007)] \times 10^{-6} = 0.0147 \times 10^{-6}$$

اگر رویدادهای اصلی رویدادهای دوبه‌دو ناسازگار باشند، داریم:

$$F = \sum_{i=1}^{k} P(\mathrm{TOP}_i) \qquad (33)$$

F: احتمال خرابی سیستم، k: تعداد کل حالت‌های خرابی سیستم.

و اگر رویدادهای اصلی مشترک باشند، در این‌صورت، از رابطه 34 برای محاسبهٔ احتمال خرابی سیستم استفاده می‌گردد.

$$F = \sum_{i=1}^{k} P(\mathrm{TOP}_i) - \sum_{i=2}^{k}\sum_{j=1}^{i-1} P(\mathrm{TOP}_i \mathrm{TOP}_j) + \ldots + (-1)^{n-1} P(\mathrm{TOP}_1 \ldots \mathrm{TOP}_k) \qquad (34)$$

همان‌طور که مشخص است، ترم‌های آخر رابطه فوق، به‌استثنای ترم اول، سهم بسیار کمی در مقدار محاسبه فوق دارند. از این‌رو، ممکن است فقط ترم اول رابطه 34 مورد استفاده قرار گیرد. یعنی، رابطه 33 برای محاسبهٔ مقدار تقریبی احتمال خرابی سیستم مورد استفاده قرار می‌گیرد.

برای بیان کامل این روش، از مثال سیستم تشخیص شرایط اضطراری (EDS) یک فضاپیما استفاده می‌گردد. با این تفاوت که در اینجا، آنالیز سیستم از یک دیدگاه کلی‌تر صورت می‌گیرد. به این معنی که فرض می‌شود کل سیستم شامل دو زیرسیستم می‌باشد: زیرسیستم مربوط به فرستنده‌های سیگنال و زیرسیستم نشاندهندهٔ داخل کابین. بنابراین، دو حالت خرابی، حالت اول: خرابی سیستم به‌علت ایراد در فرستادن سیگنال توسط هر یک از زیرسیستم‌ها، و حالت دوم: خرابی سیستم به‌علت ایراد در نشاندهنده را برای کل سیستم می‌توان تعریف کرد.

در این‌صورت، دو درخت خطای متفاوت برای هر یک از حالت‌ها باید ساخته شود. حالت اول مانند درخت خطای نشان داده شده در شکل 2 می‌باشد. و همان‌طور که مشاهده شد، احتمال خرابی آن در بخش 2- محاسبه گردید. درخت خطای مربوط به حالت دوم، باید براساس ساختار منطقی داخلی نشان‌دهنده، که در بخش 4- بطور کامل نشان داده شده است، و همان‌طور که عدم اشتراک بخش فرستندهٔ سیگنال و نشان‌دهنده مشهود است، ساخته شود.

بنابراین، امکان دارد که پروسه‌های آنالیز جزئی حذف گردند و از نمادگذاری سادهٔ X_5 برای نمایش رویداد اصلی دوم استفاده شود. حال فرض می‌شود که احتمال رخداد X_5 محاسبه گردیده و برابر $X_5 = 2.6 \times 10^{-5}$ می‌باشد.

از آنجائی‌که دو حالت خرابی سیستم دوبه‌دو ناسازگار نمی‌باشند، بنابراین از رابطه 33 برای محاسبهٔ مقدار تقریبی احتمال خرابی کل سیستم

1- Cut-Set based on Binary Decision Diagram

استفاده شده و مقدار زیر بدست می‌آید.

$$F = \sum_{i=1}^{k} P(\text{TOP}_i) = \sum_{i=1}^{2} P(\text{TOP}_i) = (1.0673 \times 10^{-5}) + (2.6 \times 10^{-5}) = (3.6673 \times 10^{-5})$$

با استفاده از رابطه 34 برای حالتی که خرابی‌های سیستم دوبه‌دو ناسازگار نمی‌باشند، مقدار دقیق احتمال خرابی کل سیستم را می‌توان بدست آورد. مقدار زیر برای احتمال خرابی کل سیستم قابل محاسبه است.

$$F = \sum_{i=1}^{k} P(\text{TOP}_i) - \sum_{i=2}^{k}\sum_{j=1}^{i-1} P(\text{TOP}_i\text{TOP}_j) = P(TOP_1) + P(TOP_2) - P(TOP_1 \times TOP_2) = [(1.0673 + 2.6) - (1.0673 \times 2.6)] \times 10^{-5} = 8.9232 \times 10^{-6}$$

در پایان، برای محاسبه مقدار قابلیت اطمینان سیستم یا احتمال موفقیت و کارکرد صحیح سیستم لغو پرتاب، می‌توان از رابطه 35 برای حالتی که رویدادها دوبه‌دو ناسازگار باشند استفاده کرد.

$$R + F = 1 \Rightarrow R + \sum_{i=1}^{k} P(\text{TOP}_i) = R + \sum_{i=1}^{2} P(\text{TOP}_i) = 1 \Rightarrow R + (1.0673 + 2.6) \times 10^{-5} = 1 \Rightarrow R = 1 - (3.6673 \times 10^{-5}) = 0.999963 \quad (35)$$

و به طریقی مشابه، مقدار قابلیت اطمینان یا احتمال موفقیت سیستم را برای حالتی که رویدادها دوبه‌دو مشترک می‌باشند، با استفاده از رابطه 36 قابل محاسبه می‌باشد.

$$R + F = 1 \Rightarrow R + \sum_{i=1}^{k} P(TOP_i) - \sum_{i=2}^{k}\sum_{j=1}^{i-1} P(\text{TOP}_i\text{TOP}_j) + \cdots + (-1)^{n-1} P(\text{TOP}_1 \ldots \text{TOP}_k) = 1 \quad (36)$$

$$\Rightarrow R + P(\text{TOP}_1) + P(\text{TOP}_2) - P(\text{TOP}_1 \times \text{TOP}_2) = 1$$
$$\Rightarrow R = 1 - [(1.0673 + 2.6) - (1.0673 \times 2.6)] \times 10^{-5} = 1 - 0.89232 \times 10^{-5}$$
$$\Rightarrow R = 0.9999910768$$

R، مقدار قابلیت اطمینان کل سیستم می‌باشد.

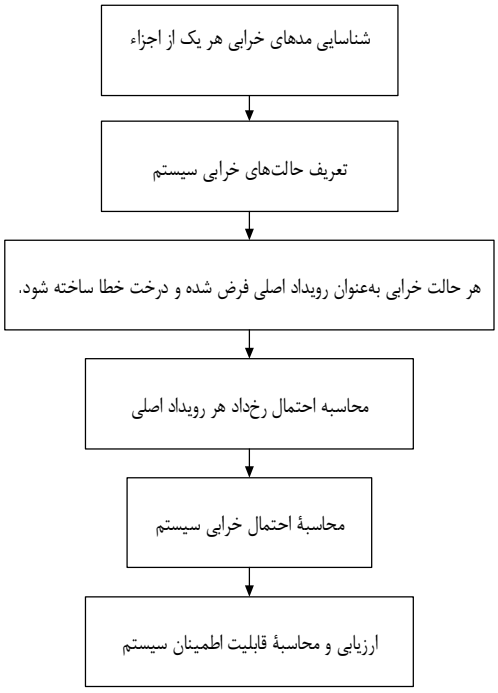
5- الگوریتم پیشنهادی

خلاصه‌ای از گام‌های آنالیز برای سیستم‌های چند حالتی متشکل از اجزاء چند حالتی که به‌کمک آنالیز درخت خطا انجام می‌گیرد در فلوچارت شکل 12 آورده شده است. که عبارتند از:

مراحل ذکر شده در فلوچارت فوق، که در آنالیز سیستم موردنظر به‌کار گرفته شده‌اند عبارتند از:

1- مدهای خرابی هر یک از اجزاء را تعریف کرده، داده‌های خرابی اجزاء و مدهای خرابی را گردآوری کنید. به‌خاطر داشته باشید که مدهای خرابی یک جزء، دوبه‌دو ناسازگار می‌باشند.

2- حالت‌های خرابی سیستم را تعریف کنید. آنها ممکن است دارای رویدادهای دوبه‌دو مشترک یا رویدادهای دوبه‌دو ناسازگار باشند، اما اگر سعی برای آنالیز یک سیستم شامل اجزاء دو-حالتی می‌باشد، و سعی برای ساده‌سازی کار با استفاده از درخت خطای منسجم باشد،



شکل 12 فلوچارت مربوط به آنالیز سیستم چندحالتی برمبنای درخت خطا

حالت‌های خرابی مختلف سیستم معمولاً دارای رویدادهای دوبه‌دو مشترک می‌باشند.

3- هر حالت خرابی سیستم را به‌عنوان رویدادهای اصلی انتخاب کرده، درخت خطای مربوطه را ساخته و آنرا ساده کنید. زمانی‌که دلایل اصلی (یا حداقل مجموعه‌های برش، در صورت منسجم بودن سیستم) بدست آمدند، قضیه 2 باید برای چک صحت درخت‌های خطای رویدادهای دوبه‌دو ناسازگار مورد استفاده قرار گیرد.

4- احتمال رخداد هر رویداد اصلی را با استفاده از روش ارائه شده در بخش 2- محاسبه کنید.

برای محاسبهٔ احتمال خرابی سیستم، دو نوع متفاوت محاسبات براساس رویدادهای اصلی وجود دارد. محاسبات مربوط به رویدادهای دوبه‌دو ناسازگار و محاسبات مربوط به حالتی که رویدادها دارای ترم‌های مشترک باشند.

6- نتیجه‌گیری

در این مقاله، آنالیز قابلیت اطمینان و احتمال موفقیت سیستم چندحالتی تشخیص شرایط اضطراری (EDS) یک فضاپیما مورد بررسی قرار گرفت. این سیستم دارای پیچیدگی بالا و ترم‌های اشتراکی زیاد بوده که تحلیل چنین سیستمی با استفاده از روش‌های حداقل مجموعه-برش و روش BDD بسیار زمان‌بر و تحلیل ترم‌های اشتراکی مشکل بوده و نتایج حاصله از دقت کمتری برخوردار خواهند بود. در این مقاله، الگوریتمی برای آنالیز سیستم چندحالتی برمبنای درخت خطا ارائه شد. درخت خطای مورد بررسی به صورت استاتیکی است که در تحقیقات آتی نویسندگان، این درخت خطا به صورت دینامیکی در نظر گرفته خواهد شد.

برای غلبه بر این مشکل، یک روش ترکیبی برای تحلیل درخت خطای استاتیکی توسعه داده شد. در این روش، مجموعه (مسیر) حداقلی با روش BDD ادغام شده و احتمال رخدادن رویداد اصلی مورد محاسبه قرار می‌گیرد. در این تحقیق، آنالیز سیستم از یک دیدگاه کلی‌تر صورت گرفت، به این معنی که فرض شد کل سیستم شامل دو زیرسیستم: زیرسیستم مربوط به

فرستنده‌های سیگنال و زیرسیستم نشاندهنده‌های داخل کابین می‌باشد. دو درخت خطای متفاوت برای هر یک از حالت‌ها ساخته شده و در پایان، نتایج مربوط به احتمال خرابی برای سیستم چند حالتی متشکل از اجزاء چند حالتی به‌کمک آنالیز درخت خطا ارائه شده و مقدار قابلیت اطمینان سیستم محاسبه می‌شود.

7- فهرست علائم

F	احتمال شکست (خرابی)
M	مدهای خرابی
N	مجموع تعداد رویدادهای اصلی
P	احتمال رخداد
R	قابلیت اطمینان
x_{li}	حالت خرابی
Y	حداقل مجموعه-برش

علایم یونانی

α_{li}	ضریب حالت برای iامین حالت خرابی جزء lام
$\varphi(x)$	تابع ساختار
$\tilde{\Omega}$	فضای حالت سیستم

بالانویس‌ها

BDD	دیاگرام تصمیم باینری
CFT	درخت خطای منسجم
CSBDD	مجموعه-برش برمبنای دیاگرام تصمیم باینری
EDS	سیستم تشخیص شرایط اضطراری
EDSI	نشان‌دهندهٔ سیستم تشخیص شرایط اضطراری
FTA	آنالیز درخت خطا
OBDD	دیاگرام تصمیم باینری مرتب‌شده
ROBDD	دیاگرام تصمیم باینری مرتب‌شدهٔ کاهش یافته
TOP	رویداد اصلی

زیرنویس‌ها

f	حالت شکست
i,j	اندیس‌های شمارشی
k	تعداد کل حالت‌های خرابی
l	المان پایه‌ای
n	بردار n-بعدی
S	حالت موفقیت

8- مراجع

[1] B. Natvig, *Multistate systems reliability theory with applications*., John Wiley & Sons, 2010.
[2] L. Caldarola, *Fault tree analysis with multistate components,* in *Synthesis and analysis methods for safety and reliability studies*., Springer, pp. 199-248, 1980.
[3] Y.W. Liu and K.C. Kapur, *New Models and Measures for Reliability of Multi-state Systems,* in *Handbook of Performability Engineering*., Springer, pp. 431-445, 2008.
[4] I. Gertsbakh and Y. Shpungin, *Multidimensional spectra of multistate systems with binary components,* in *Recent Advances in System Reliability*.,Springer, pp. 49-61, 2012.
[5] X. Huang, *The generic method of the multistate fault tree analysis. Microelectronics Reliability,* vol. 24, no. 4, pp. 617-622, 1984.
[6] X. Janan, On multistate system analysis*., IEEE Transactions on Reliability,* vol. 34, no. 4, pp. 329-337, 1985.
[7] R.E. Barlow and A.S. Wu, Coherent systems with multi-state components. *Mathematics of Operations Research,* vol. 3, no. 4, pp. 275-281, 1978.
[8] L. Caldarola, Coherent systems with multistate components. *Nuclear Engineering and Design,* vol. 58, no. 1, pp. 127-139. 1980.
[9] A.T. Neil, *Apollo Experience Report-Launch Escape Propulsion Subsystem, Munned Spacecraft Center Houstotz,* Texas 77058, 1973.
[10] S.I. Jimenez, B.C. Grover, *Apollo Spacecraft & Systems Familiarization,* NAA Space Division Downey, California, August 1967.
[11] K.B. Misra, *Handbook of performability engineering*., Springer, 2008.
[12] A. Lisnianski, and I. Frenkel, *Recent advances in system reliability*., Springer, 2012.
[13] W.S. Lee, et al., *Fault Tree Analysis, Methods, and Applications □ A Review., IEEE Transactions on Reliability,* vol. 34, no. 3, pp. 194-203, 1985.
[14] Y. Kai, Multistate fault-tree analysis. *Reliability Engineering & System Safety,* vol. 28, no. 1,pp. 1-7, 1990.
[15] G. Yingkui, and L. Jing, Multi-state system reliability: A new and systematic review. *Procedia Engineering,* vol. 29, pp. 531-536, 2012.
[16] L. Xing, and S.V. Amari, *Fault tree analysis,* in *Handbook of performability engineering*., Springer. pp. 595-620, 2008.
[17] Twigg DW, et al., Modeling mutually exclusive events in fault trees. *Proceedings of the Annual Reliability and Maintainability Symposium;* pp. 8–13, Los Angles, CA, 2000.
[18] DW Twigg, AV Ramesh, and S. TC., Modeling event dependencies using disjoint sets in fault trees. *Proceedings of the 18th International System Safety Conference* 2000; pp. 275–279, 2000.
[19] JD Andrews and D.SJ., Event-tree analysis using binary decision diagrams. *IEEE Transactions on Reliability*; vol. 49, no. 2, pp. 230–238, 2000.
[20] M. Modarres, M. Kaminskiz, and V. Krivstov, *Realiability Engineering and Risk Analysis: A Practical Guide*. Vol. 55: CRC press., 1999.
[21] J.B. Dugan, S.J. Bavuso, and B. MA., Fault trees and Markov models for reliability analysis of fault tolerant systems. *Reliability Engineering and System Safety*; vol. 39, pp. 291–307, 1993.
[22] Sugier, J. Reliability analysis based on Markov models adjusted to various maintenance policies. in *Proceedings of the 11th International Conference on Reliability and Statistics in Transportation and Communication (RelStat'11)*., 2011.
[23] Xu, H. and J.B. Dugan. Combining dynamic fault trees and event trees for probabilistic risk assessment. in *Reliability and Maintainability, 2004 Annual Symposium-RAMS*., IEEE, 2004.
[24] Dugan, J.B., and S. A. Doyle, *New results in fault-tree analysis, Tutorial notes of the Annual Reliability & Maintainability Symposium*, Jan. 1997.
[25] M. Stamatelatos, and J. Caraballo, *Fault tree handbook with aerospace applications*., Office of safety and mission assurance NASA headquarters, 2002.
[26] R. Gulati, and J.B. Dugan. A modular approach for analyzing static and dynamic fault trees. in *Reliability and Maintainability Symposium.,Proceedings, Annual*., IEEE, 1997.