استاندارد ملی ایران

۱۲۸۳۳

چاپ اول

جمهوری اسلامی ایران

Islamic Republic of Iran

سازمان استاندارد و تحقیقات صنعتی ایران

Institute of Standards and Industrial Research of Iran

ISIRI

12833

1st.edition

تحلیل درخت خرابی

Fault Tree Analysis

ICS: 03.120.01;03.120.99

به‌نام خدا

آشنایی با مؤسسهٔ استاندارد و تحقیقات صنعتی ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان مؤسسه* صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی(رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذیصلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که مؤسسه استاندارد تشکیل می‌دهد به تصویب رسیده باشد.

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور، از آخرین پیشرفتهای علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشو ر و / یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. مؤسسه می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سا زمانها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش ، مؤسسهٔ استاندارد این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آنها نظارت می کند .ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این مؤسسه است.

---

* موسسهٔ استاندارد و تحقیقات صنعتی ایران

1- International organization for Standardization
2 - International Electro technical Commission
3- International Organization for Legal Metrology (Organization International de Metrology Legal)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« تحلیل درخت خرابی»

رئیس:	سمت و/ یا نمایندگی
ذره، مهدی	کارشناس استاندارد
(فوق لیسانس مهندسی برق)	
دبیر:	
روشن، رنگین	کارشناس اداره کل استاندارد و تحقیقات صنعتی استان
(لیسانس مهندسی برق- الکترونیک)	کردستان
حسین زاده، بختیار	
(فوق لیسانس مهندسی برق- کنترل)	عضو هیات علمی دانشگاه کردستان
اعضاء: (اسامی به ترتیب حروف الفبا)	
بستان‌دوست راد، احسان	مدیرعامل شرکت مهندسی اعتماد توازن
(لیسانس مهندسی صنایع)	
حسینی، محمد	کارشناس شرکت توزیع برق استان کردستان
(لیسانس مهندسی صنایع، گرایش تولید صنعتی)	
عطااله خانی	کارشناس سازمان صنایع و معادن استان کردستان
(لیسانس مهندسی صنایع)	
روشن، اکبر	کارشناس شرکت مهندسی بازرسی تکین کو
(لیسانس مهندسی برق- الکترونیک)	
روشن، فاتح	معاون فنی و برنامه ریزی پروژه شرکت پرهون طرح(نیروگاه
(لیسانس مهندسی کامپیوتر)	سیکل ترکیبی)
طاهر نسب، محمد باقر	مشاور شرکت قدس نیرو
(لیسانس مهندسی برق- قدرت)	

منتظری، فرشاد دانشگاه علم و صنعت
(فوق لیسانس مهندسی برق-قدرت)

منتظری، فرهاد دانشگاه علم و صنعت
(فوق لیسانی مهندسی برق- قدرت)

فهرست مندرجات

عنوان **صفحه**

پیش گفتار

استاندارد "تحلیل درخت خرابی" که پیش نویس آن درکمیسیون های مربوط توسط مؤسسهٔ استاندارد و تحقیقات صنعتی ایران تهیه و تدوین شده و در یکصدو یکمین اجلاس کمیتهٔ ملی استاندارد مدیریت کیفیت مورخ ۸۹/۴/۲۸ مورد تصویب قرار گرفته است ، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ ، به عنوان استاندارد ملی ایران منتشر می‌شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و مآخذی که برای تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

IEC 61025:2006 – Fault Tree Analysis

مقدمه

تحلیل درخت خرابی FTA[1] به شناسایی و تحلیل وضعیت‌ها و عواملی می‌پردازد که موجب بالاترین رخداد تعریف شده می‌شوند یا بالقوه می‌توانند موجب بالاترین رخداد شده یا در وقوع آن نقش داشته باشند . در FTA این رخداد معمولاً توقف یا تنزل عملکرد ، ایمنی یا صفات عملیاتی مهم دیگر است ولی در مورد STA(تحلیل درخت موفقیت) این رخداد صفت تشریح‌کننده‌ی موفقیت است.

از FTA اغلب برای تحلیل ایمنی سیستم‌ها استفاده می‌شود(مانند سیستم‌های حمل و نقل ، نیروگاه برق ، یا هر سیستم دیگری که ارزیابی ایمنی بهره‌برداری آن لازم باشد). تحلیل درخت خرابی را می‌توان همچنین برای تحلیل آمادگی و قابلیت نگهداری هم بکار برد. برای سادگی از این به بعد در این استاندارد برای نشان دادن این جنبه‌های عملکرد سیستم از اصطلاح قابلیت اطمینان استفاده می‌شود.

در این استاندارد دو رویکرد به FTA وجود دارد . یک رویکرد، کیفی است یعنی به احتمال رخدادها و عوامل کمک‌کننده به آنها – رخدادهای ورودی – یا فراوانی وقوع آنها نمی‌پردازد. این رویکرد تحلیل مفصلی از رخداد/ وقوع خرابی‌ها است که به عنوان FTA کیفی یا سنتی معروف است. درخت خرابی کیفی به‌صورت گسترده در صنایع هسته‌ای و موارد دیگری که علل وقوع خرابی‌های بالقوه بدون توجه به احتمال وقوع آنها مورد نظر باشد، کاربرد دارد . گاهی اوقات بعضی از رخدادها FTA سنتی به‌طور کمی بررسی و تحقیق می‌شوند ولی این محاسبات هیچ ارتباطی با محاسبات قابلیت اطمینان کل ندارند یعنی اقدامی برای محاسبه قابلیت اطمینان کل با استفاده از FTA نشده است. رویکرد دومی را که خیلی از صنایع پذیرفته‌اند، عمدتاً کمی است یعنی FTA مفصل، کل محصول، فرآیند یا سیستم را مدل می‌کند. اکثریت قاطع رخدادهای اصلی اعم از خرابی‌ها و رخدادها دارای احتمال وقوعی می‌باشند که با تحلیل یا آزمون تعیین می‌شوند. دراین صورت، نتیجه نهائی، احتمال وقوع بالاترین رخدادی است که معرف قابلیت اطمینان یا احتمال خرابی یا وقوع خرابی است .

[1]-Fault Tree Analysis

تحلیل درخت خرابی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، توصیف « تحلیل درخت خرابی» و ارائه رهنمود هایی در رابطه با کاربرد آن به ترتیب زیر است:

- تعریف اصول پایه :

-توصیف و توضیح مدل سازی ریاضیاتی مربوطه

-توضیح روابط FTA با سایر روش های مدل سازی قابلیت اطمینان

-توصیف گامهای دخیل در اجرای FTA

-شناسایی مفروضات مناسب ، رخداد ها و مُد های وقوع خرابی ;

-شناسایی و توصیف نمادهای رایج مورد استفاده.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

۲-۱ استاندارد ملی ایران شماره ۱۰۴۲۵-۱۹۱، سال ۱۳۸۸ ، واژگان الکتروتکنیک – فصل ۱۹۱ قابلیت اعتماد و کیفیت خدمت

۲-۲ استاندارد ملی ایران شماره ۱۱۷۴۸ سال ۱۳۸۷، کاربرد فنون مارکوف

۳ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف تعیین شده در استاندارد ملی ایران شماره ۱۰۴۲۵-۱۹۱ سال ۱۳۸۷ به کار می‌رود.

در روش‌شناسی درخت خرابی و کاربردهای آن، اصطلاحات بسیاری به منظور توضیح بهتر در مورد مقصود تحلیل یا فرآیند تفکر پشتیبان آن، به کار می‌روند. همچنین اصطلاحات مترادفی که از نظر تحلیلی صحیح در نظر گرفته می‌شوند توسط نویسندگان مختلف به کار می‌روند. از اصطلاحات تکمیلی زیر در این استاندارد استفاده می شود:

۱-۳

(برآمد) [1]

نتیجه یک اقدام یا ورودی دیگر ، عقبه‌ی یک علت

یادآوری ۱- برآمد می‌تواند یک رخداد یا یک حالت باشد. در یک درخت خرابی، برآمد ناشی از ترکیب رخدادهای ورودی مربوطه که با یک دروازه نشان داده می‌شود می‌تواند یک رخداد میانی یا بالاترین رخداد باشد.

یادآوری ۲- در یک درخت خرابی، برآمد می‌تواند یک ورودی برای یک رخداد میانی باشد یا خود بالاترین رخداد باشد.

۲-۳

بالاترین رخداد[2]

حاصل ترکیبات کلیه رخدادهای ورودی

یادآوری ۱- بالاترین رخداد، رخدادی است که تحت آن درخت خرابی ایجاد می شود. بالاترین رخداد اغلب تحت عنوان **رخداد نهایی** یا **برآمد نهایی** هم خوانده می‌شود.

یادآوری ۲- بالاترین رخداد، از قبل تعریف شده و نقطه آغاز یک درخت خرابی است و بالاترین جایگاه را در سلسله مراتب رخدادها دارد.

۳-۳

رخداد نهایی[3]

نتیجه نهایی از ترکیبات کلیه ورودیها، رخدادهای میانی و اصلی است.

یادآوری- این رخداد، نتیجه رخدادها یا حالت های ورودی است (به ۳-۲ مراجعه کنید).

۴-۳

برآمد نهایی[4] **(برآمد نهایی)**

برآمدی که با ایجاد درخت خرابی تحقیق و بررسی می‌شود.

یادآوری-نتیجه نهایی از ترکیبات کلیه رخدادهای ورودی، رخدادهای میانی و اصلی، که نتیجه رخدادهای یا حالتهای ورودی می‌باشد (به ۳-۲ مراجعه کنید).

۵-۳

دروازه[5]

نمادی که برای برقرار کردن پیوند نمادین بین رخداد خروجی و ورودیها مربوطه مورد استفاده قرار می‌گیرد.

---

1 -Outcome
2 -Top event
3 -Final event
4 -Top outcome
5 -Gate

یادآوری- نماد دروازه منعکس کننده نوع رابطه لازم بین رخدادهای ورودی برای وقوع رخداد خروجی است.

۶-۳

مجموعه قطعی کننده[1]

گروهی از رخدادها که در صورت وقوع، موجب وقوع بالاترین رخداد خواهند شد.

۷-۳

مجموعه قطعی کننده مینیمال[2]

حداقل یا کوچکترین مجموعه رخداد لازم برای ایجاد علت بالاترین رخداد

یادآوری- عدم وقوع هر یک از رخدادها در این مجموعه مانع از وقوع بالاترین رخداد خواهد شد.

۸-۳

رخداد[3]

وقوع یک وضعیت یا یک اقدام

۹-۳

رخداد اصلی[4]

رخداد یا حالتی که دیگر قابل توسعه نباشد.

۱۰-۳

رخداد اولیه[5]

رخدادی که در پایین درخت خرابی وجود دارد.

یادآوری- در این استاندارد رخداد اولیه می‌تواند به معنی رخداد اصلی باشد که دیگر نیازی به توسعه بیشتر ندارد یا ممکن است رخدادی باشد که گرچه حاصل گروهی از رخدادها و دروازه‌هاست، اما ممکن است در جایی دیگر توسعه یابد یا اصلاً قابل توسعه نباشد(رخداد توسعه نیافته).

۱۱-۳

رخداد میانی[6]

رخدادی که نه بالاترین رخداد است و نه رخداد اولیه

یادآوری-این نوع رخداد، معمولاً نتیجه یک یا چند رخداد اولیه و/ یا میانی دیگر است.

---

1 -Cut set
2 -Minimal cut set
3 -Event
4 -Basic event
5 -Primary event
6 -Intermediate event

۱۲-۳

رخداد توسعه نیافته[1]

رخدادی که فاقد رخدادهای ورودی است.

یادآوری- عدم توسعه رخداد در تحلیل دلایل مختلفی دارد از قبیل نبود اطلاعات مشروح ، یا توسعه در تحلیل دیگر و حاشیه‌نویسی در تحلیل فعلی به عنوان توسعه نیافته. نمونه ای از دروازه‌های توسعه‌نیافته می‌تواند اقلام بازاری باشد(COTS[2]).

۱۳-۳

وقوع خرابی کانونی (رخداد)[3]

رخداد وقوع خرابی که در صورت وقوع ، موجب وقوع خرابی کل سیستم شده یا بدون توجه به سایر رخدادها یا ترکیبات، خود، رخداد نا مطلوب نهایی را موجب می شود.

۱۴-۳

رخداد هایی با علت مشترک[4]

رخدادهای مختلف در یک سیستم یا درخت خرابی که دارای علت مشابه برای وقوع می باشند.

یادآوری- نمونه‌ای از این رخداد می‌تواند اتصالی خازن سرامیکی ناشی از خمش تخته مدار باشد. بنابراین گرچه اینها می توانند خازن‌های مختلف با وظایف مختلف در طراحی شان باشند اما اتصالی علت مشترک یعنی رخداد ورودی مشابه می باشد.

۱۵-۳

علت مشترک

علت وقوع چندین رخداد

یادآوری- در نمونه فوق این خمش تخته است که خود می‌تواند یک رخداد میانی ناشی از چندین رخداد باشد از قبیل شوک محیطی، لرزش یا قطعی دستی صفحه مدار چاپی طی ساخت محصول

۱۶-۳

رخداد مشابه یا تکراری[5]

رخدادی که ورودی بیش از یک رخداد سطح بالاتر است.

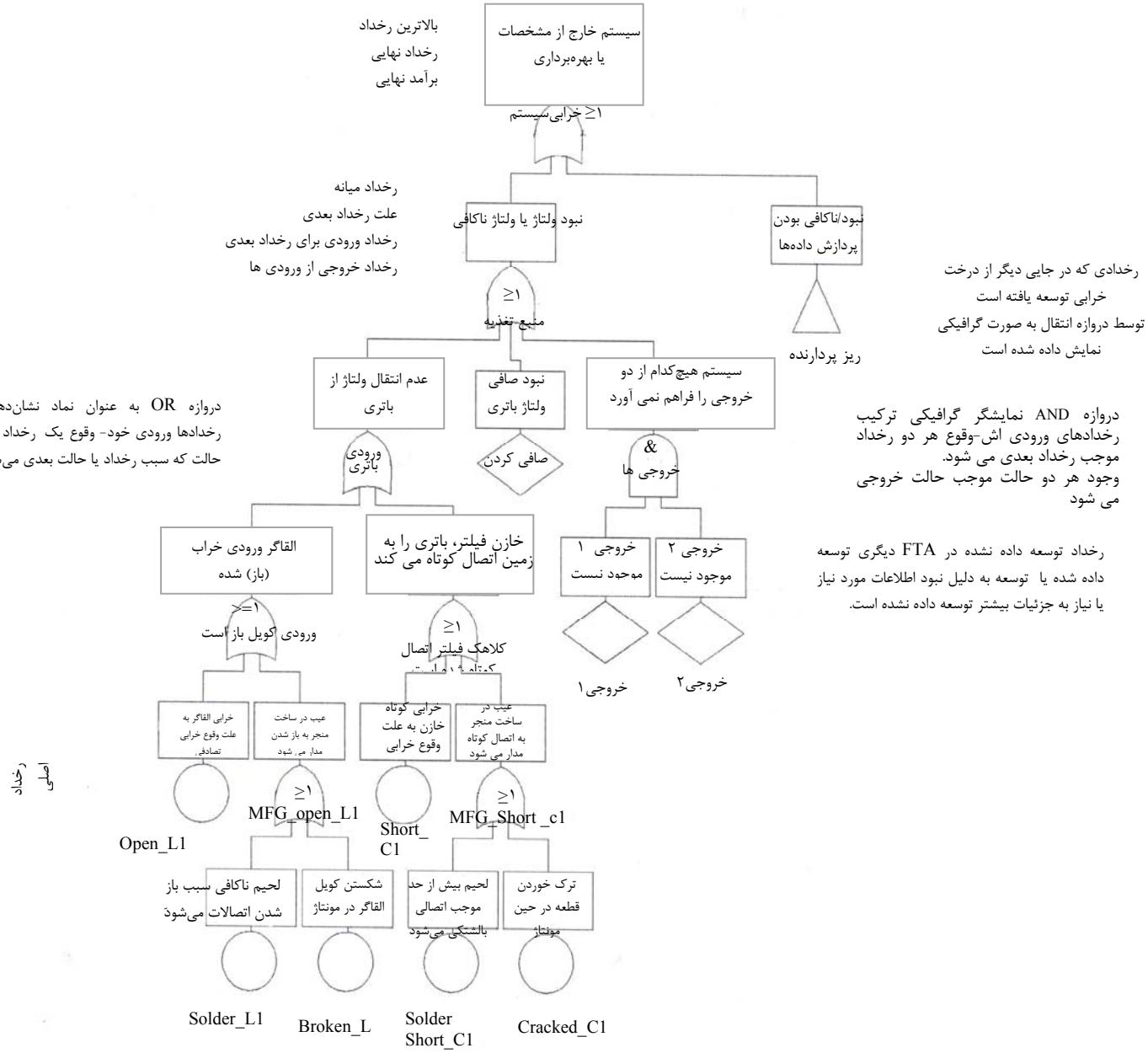
یادآوری-این رخداد می‌تواند رخدادی با علت مشترک یا مُد وقوع خرابی یک جز باشد که در بیش از یک بخش از طراحی مشترک است.

شکل ۱ بعضی از تعاریف فوق را نشان می دهد این شکل شامل یاداشت‌ها و توصیف رخدادها برای توضیح بهتر کاربرد عملی درخت خرابی است. در شکل ۱ توضیح گرافیکی مجموعه‌های قطعی کننده یا مجموعه های قطعی کننده مینیمال برای ساده کردن نمایش گرافیکی یا سایر اصطلاحات مربوطه حذف شده است.

---

1 -Undeveloped event
2 -Commercial Off The Shelf
3 -Single point failure (event)
4 -Common cause
5 -Replicated or repeated event

نمادها در شکل ۱ و همه‌ی شکل‌های بعدی نمایش داده می‌شود. تعدادی از آنها در جدول‌های الف-۱ تا الف-۴ وجود دارند چون کادر های اضافه شده در بالای دروازه برای توصیف رخدادهای جداگانه است.



شکل ۱ – مثال هایی برای اصطلاحات مورد استفاده در تحلیل های درخت خرابی

یادآوری- نمادهای شکل ۱ و سایر شکل ها ممکن است تا حدودی از نمادهای ارائه شده در پیوست الف متفاوت باشد. زیرا کادر های توضیحی اضافه شده تا بهتر بتوان رابطه رخدادهای مختلف را توصیف کرد.

۴ نمادها

نمایش گرافیکی درخت خرابی ایجاب می‌کند که نمادها شناسه‌ها و برچسب‌ها به شیوه یکسان مورد استفاده قرار گیرند. نمادهایی که رخدادهای درخت خرابی را توصیف می‌کنند بنابر سلیقه کاربر و بسته نرم افزاری متفاوت خواهد بود. راهنمای کلی در بند ۸ و پیوست الف ارائه شده است.

سایر نمادهای مورد استفاده در این استاندارد نمادهای استاندارد قابلیت اعتماد از قبیل F(t) یا احتمال وقوع رخداد F می‌باشد. به همین علت فهرست جداگانه ای از نمادها ارئه نشده است.

۵ کلیات

۵-۱ توصیف و ساختار درخت خرابی

چندین روش تحلیلی برای تحلیل قابلیت اعتماد وجود دارد که یکی از آنها تحلیل درخت خرابی است. مقصود هر روش و کاربرد جداگانه و ترکیبی آنها، در ارزیابی روند رخدادها یا حالت هایی که علت حاصل شدن یا قابلیت اطمینان و آمادگی سیستم یا جزء داده شده است بایستی توسط تحلیل گر قبل از شروع FTA امتحان شود. توصیه می‌گردد قبل از شروع FTA، تحلیل‌گر، مزایا، معایب هر روش، نتایج مربوطه، داده‌های لازم برای اجرای تحلیل، پیچیدگی تحلیل و سایر عوامل شناسایی شده در این استاندارد را مورد توجه قرار دهد.

درخت خرابی، نمایش گرافیکی سازمان یافته شرایط یا سایر عوامل ایجاد کننده یا موثر در وقوع برآمد مشخص تحت عنوان «بالاترین رخداد» است. هنگامی که برآمد، موفقیت است، درخت خرابی به درخت موفقیت تبدیل می‌گردد که در آن رخدادهای ورودی آنهایی هستند که به موفقیت بالاترین رخداد کمک می‌کنند. نمایش یک درخت خرابی به شکلی است که به راحتی قابل فهم و تحلیل بوده و در صورت نیاز جهت تسهیل در شناسایی موارد ذیل تجدید آرایش[1] شود.

- عوامل موثر در بالاترین رخداد مورد بررسی که در اکثر تحلیل‌های مرسوم درخت خرابی انجام می‌گیرد؛
- عوامل موثر در قابلیت اطمینان و ویژگیهای عملکردی سیستم، هنگام استفاده از روش FTA، به منظور تحلیل قابلیت اطمینان برای مثال نقص‌های طراحی، تنش های محیطی و بهره برداری ، مُد وقوع خرابی جزء، اشتباهات کاربر، خرابی‌های نرم‌افزاری؛
- رخدادهای موثر بر بیش از یک جز وظیفه‌ای که بتواند ردوندانسی خاص را از بین برده یا بر دو یا چند بخش از محصول که ممکن است از نظر بهره برداری بی ارتباط یا مستقل به نظر آیند، تاثیر گذارد (رخدادهای علت مشترک).

تحلیل درخت خرابی، روش قیاسی (از بالا به پایین) است. تحلیل با هدف بررسی دقیق علت ها یا مجموعه علت هایی است که منجر به بالاترین رخداد می‌شود. این تحلیل بسته به هدف و دامنه کاربرد آن می‌تواند کمی یا کیفی باشد.

1 -Rearrange

درخت خرابی را می‌توان مانند مکمل آن یعنی تحلیل درخت موفقیت[1](STA) ایجاد کرد، که در آن بالاترین رخداد یک موفقیت است و ورودی‌های آن عوامل موثر بر رخداد موفقیت (مطلوب) است.
در مواردی که احتمال وقوع رخدادهای اولیه قابل برآورد نباشد، FTA کیفی را می‌توان برای بررسی علل برآمدهای نامطلوب بالقوه با رخدادهای اولیه جداگانه، با احتمال توصیفی رخداد، نشان داد مثلاً با احتمال بسیار زیاد، احتمال زیاد، احتمال متوسط، احتمال کم و غیره، هدف اصلی FTA کیفی شناسایی مجموعه قطعی مینیمال، برای تعیین راه‌هایی است که رخدادهای اولیه یا اصلی بر بالاترین رخداد تاثیر می‌گذارند.
FTA کمّی را می‌توان هنگامی به کار برد که احتمال رخدادهای اولیه مشخص باشند. احتمال‌های وقوع همه رخدادهای میانی و بالاترین رخداد (برآمد) را آنگاه می‌توان مطابق با مدل محاسبه کرد .همچنین FTA کمّی در تحلیل قابلیت اطمینان یک محصول یا سیستم و توسعه آن، بسیار مفید است.
FTA را می‌توان برای تحلیل سیستم‌هایی با تعاملات پیچیده بین زیر سیستم‌های شامل تعاملات نرم‌افزاری/سخت‌افزاری به کار برد.

۲-۵ اهداف

FTA را می‌توان به طور مستقل یا همراه با سایر تحلیلهای قابلیت اطمینان به کار برد.
اهداف عبارتند از:
- شناسایی علل یا مجموعه ای از علل که منجر به بالاترین رخداد می‌شود؛
- تعیین این‌که آیا مقیاس قابلیت اطمینان یک سیستم خاص، شرایط مربوطه را برآورده می‌کند یا خیر؛
- تعیین این‌که کدام مُد وقوع خرابی یا عوامل بیشترین تأثیر را در احتمال وقوع خرابی سیستم (عدم قابلیت اطمینان) یا ناآمادگی دارد، اگر سیستم قابل تعمیر باشد، شناسایی امکان بهبودهای قابلیت اطمینان سیستم؛
- تحلیل و مقایسه انواع طراحی‌های مختلف دیگر جهت افزایش قابلیت اطمینان سیستم؛
- اثبات اعتبار مفروضات ارائه شده در سایر تحلیل‌ها (مانند مارکوف و FMEA)؛
- شناسایی مُدهای وقوع خرابی بالقوه که ممکن است منجر به مساله ایمنی شود، ارزیابی احتمال وقوع مربوط و امکان کاهش آن؛
- شناسایی رخدادهای مشترک(مانند شاخه های میانی یک مدار پل، به شکل ۱۰ رجوع شود)؛
- جستجو برای یک رخداد یا مجموعه‌ای از رخدادها که دارای احتمال بیشتری برای وقوع بالاترین رخداد هستند؛
- ارزیابی تأثیر وقوع رخداد اولیه بر احتمال وقوع بالاترین رخداد؛
- محاسبه احتمال‌های رخداد؛
- اگر شرایط پایدار را بتوان بدیهی فرض[2] کرد و تعمیرات پایانی[3] مستقل از یکدیگر باشند، محاسبه آمادگی‌ها و نرخ‌های وقوع خرابی سیستم یا اجزا آن که توسط درخت خرابی نشان داده می‌شود، (همان محدویت‌ها دیاگرام مسیر موفقیت و بلوک دیاگرام قابلیت اطمینان).

1 - Success tree analysis
2 -Postulated
3 -Eventual repair

۵-۳ کاربردها

FTA به ویژه برای تحلیل سیستم‌هایی که از چندین زیر سیستم که از جنبه‌ی وظیفه‌ای مرتبط یا وابسته باشند، مناسب است. فواید FTA هنگامی آشکار می‌گردد که طراحی سیستم حاصل چندین گروه طراح فنی ویژه مستقل بوده و درخت های جداگانه خرابی با همدیگر مرتبط شوند.

تحلیل درخت خرابی معمولاً هنگام طراحی ایستگاه‌های تولید برق هسته‌ای، سیستم‌های حمل و نقل، سیستم‌های ارتباطاتی، فرآیندهای شیمیایی یا دیگر صنایع، سیستم راه آهن، سیستم‌های تفریحی منازل، سیستم‌های پزشکی و رایانه ای و غیره به کار می‌رود. همچنین تحلیل درخت خرابی هنگام استفاده در سیستم های متشکل از انواع مختلفی اجزا و تعامل آنها (اجزای مکانیکی ، الکتریکی و نرم افزاری) که به‌راحتی با سایر روش‌ها مدل سازی نشود ارزش ویژه‌ای می‌یابد. نمونه ای از این مورد ترکیبی از رخدادها است که ترتیب پیدایش آنها اساسی است مانند وجود خستگی لرزشی که منجر به ترک‌ها و وقوع خرابی‌های ساختاری اجزا شود.

کاربردهای FTA به عنوان یک ابزار (تعداد اندکی از این کاربردها فهرست شده اند):

- تعیین ترکیب منطقی رخدادها که منجر به بالاترین رخداد و به‌صورت بالقوه اولویت آنها می‌گردد.؛
- بررسی سیستم تحت توسعه و پیش بینی و پیش‌گیری یا کاهش علل بالقوه بالاترین رخداد نامطلوب؛
- تحلیل یک سیستم، تعیین قابلیت اطمینان آن ، شناسایی عوامل اصلی موثر در عدم قابلیت اطمینان آن و ارزیابی تغییرات طراحی؛
- کمک به تلاش برای ارزیابی احتمال ریسک[1].

FTA را می‌توان برای کلیه محصولات جدید یا اصلاح شده در کلیه فاز های طراحی به عنوان ابزار تحلیلی جهت شناسایی مسایل بالقوه طراحی، از جمله فازهای اول که در آن اطلاعات در خصوص جزییات طراحی کامل نمی‌باشد، به کاربرد. آن‌گاه اقدامات اولیه را با بیشتر شدن اطلاعات مربوط به طراحی سیستم و اجزا آن می‌توان توسعه داد. FTA همچنین مسایل بالقوه ناشی از طراحی فیزیکی محصول، تنش‌های محیطی یا بهره‌برداری، اشکال[2] در فرایندهای تولید محصول و روندهای بهره‌برداری و نگهداری را شناسایی می‌کند.

۵-۴ ترکیب با سایر فنون تحلیل قابلیت اعتماد

۵-۴-۱ ترکیب FTA و تحلیل انواع وقوع خرابی ها و آثار آن‌ها (FMEA)

این ترکیب تحلیل اغلب توسط استانداردهای خاص این بخش به‌ویژه استانداردهای خاص ایمنی و استانداردهای حمل و نقل توصیه می‌شوند. فواید ترکیب تحلیلها به شرح ذیل است:

-FTA روش تحلیل از بالا به پایین و FMEA روش تحلیل از پایین به بالا است یعنی استفاده از استدلال استقرایی و استدلال استنتاجی دلیل خوبی برای فراهم آوردن تضمین کامل بودن تحلیل است.

1 -Probablistic risk assessment
2 -Flaw

- استانداردهای ایمنی غالباً مستلزم تحلیل وقوع خرابی واحد و در بعضی موارد تحلیل‌های وقوع خرابی چندگانه می‌باشند که اولین نیازمندی آن با FMEA انجام شود و تحلیل وقوع خرابی واحد و تحلیل وقوع خرابی چند گانه هر دو در FTA انجام شود؛

- FMEA همچنین روش مفیدی برای شناسایی جامع رخدادهای اصلی یا خطرهای اصلی می باشد در حالیکه FTA روش عملی برای تحلیل علی[1] رخدادهای نا مطلوب است؛

به‌علاوه کنترل ساده سازگاری بین FMEA و FTA وجود دارد:

- هر وقوع خرابی واحد شناسایی شده‌ایی در FMEA که منجر به بالاترین رخداد در درخت خرابی شود باید به عنوان وقوع خرابی کانونی پدیدار شود (در مجموعه‌ی قطعی مینیمال)؛

یادآوری- وقوع خرابی کانونی وقوع خرابی است که اگر رخ دهد باعث خرابی کل سیستم می شود.

-هر گونه وقوع خرابی کانونی، که در FTA شناسایی شود نیز باید در FMEA نمایان گردد.

اگر این تحلیل ها جداگانه و مستقل انجام شوند ارزش این کنترل سازگاری افزایش می‌یابد. این مساله به‌ویژه در تحلیل‌های ایمنی حائز اهمیت است.

استاندارد ملی به شماره ۱-۶۰۳۰۰ این روش را توضیح می‌دهد.

۵-۴-۲ ترکیب FTA و تحلیل درخت رخداد(ETA)[2]

هر رخداد را می‌توان توسط FTA تحلیل کرد. با این وجود، در بعضی موارد این مساله ممکن است به چند دلیل زیر مناسب نباشد

- گاهی راحت تر است که توالی رخداد را به جای روابط علی ایجاد کرد؛
- درخت حاصل ممکن است بیش از حد بزرگ شود؛
- غالباً تیم های جداگانه‌ای برای پرداختن به بخش‌های مختلف تحلیل وجود دارند.

برای یافتن روش اجرایی عملی، غالباً این رخداد نا مطلوب نیست که ابتدا تعریف می‌شود بلکه رخدادهای نا مطلوب احتمالی در حد فاصل[3] بین دامنه وظیفه ای و تکنیکی تعریف می شود.

برای توضیح بیشتر، بالاترین رخداد را از دست دادن خدمه یا وسیله نقلیه برای ماموریت فضایی در نظر بگیرید. به جای ایجاد یک درخت خرابی بزرگ در مورد از دست دادن خدمه یا وسیله نقلیه، رخداد نامطلوب میانی مانند خرابی احتراق یا خرابی رانش ممکن است تحت عنوان بالاترین رخداد تعریف شده و به عنوان درخت های خرابی جداگانه تحلیل شوند. از این بالاترین رخداد تنزل یافته به نوبه خود به عنوان ورودی ها برای یک درخت رخداد به منظور تحلیل پی آمدهای بهره‌برداری استفاده خواهد شد.

این ترکیب ETA و FTA گاهی تحت عنوان تحلیل علت–عواقب معرفی می‌شود[4](CCA).

1 -Casual
2- Event Tree Analysis
3 -Interface
4- cause –consequence analysis

۵-۴-۳ ترکیب FTA و تحلیل مارکوف

FTA که فقط دارای ترکیبی از رخدادهای استاتیک (زمان بندی – توالی ترکیب رخدادهایی لحاظ یا مدل سازی نمی شوند- دروازه‌های استاتیک) است، معمولاً سیستم‌ها را مستقل از توالی رخدادهای ارزیابی می کند. با این وجود می‌توان FTA را با تعریف دروازه‌های اضافه شده‌ایی که معرف مدلهای مارکوف است توسعه داد. این دروازه‌ها تحت عنوان دروازه‌های دینامیک خوانده شده و شامل دروازه‌های (AND اولویت‌دار) و SEQUENTIAL (متوالی) و SPARE (یدکی) می‌باشند. برای این‌گونه دروازه های AND اولویت‌دار لازم است احتمال وقوع خرابی را در زمان t با استفاده از مدل مناسب مارکوف یا شبیه‌سازی، ارزیابی کرد. بعد از ارزیابی، دروازه دینامیک و ورودی‌های آن را می‌توان با رخداد اولیه ساده، با احتمال وقوع محاسبه شده توسط تحلیل مارکوف جایگزین کرد. بعضی از نرم‌افزارهای تجاری مدل‌سازی دروازه‌های دینامیک و توانمندی محاسبه‌ی احتمال پیشامد رخدادی که معرف آن هستند را امکان‌پذیر می‌سازند. نمونه‌ای از دروازه AND (اولویت دار) دینامیک در پیوست الف نشان داده شده است.

دروازه‌های استاتیک و دروازه‌های دینامیک با یک درخت خرابی بر اساس این مفروض به کار می‌روند که رخدادهای منحصر به‌فرد مستقل می‌باشند (مگر این‌که تحت عنوان رخداد مشترک تعریف شوند). با این وجود، باید به خواص استقلال بین رخدادها مندرج در مدل مارکوف و رخدادهای مندرج در درخت خرابی توجه خاصی مبذول شود.

۵-۴-۴ ترکیب تکنیک های FTA دیاگرام تصمیم باینری (BDD)

محاسبه احتمال وقوع برای بالاترین رخداد یک درخت خرابی با تعداد زیادی از مجموعه‌ی قطعی ، مستلزم محاسبه احتمال برای کلیه ترکیبات مجموعه‌های قطعی می‌باشد. به علت پیچیدگی زیاد آن، این محاسبه اغلب باید کوتاه[1] شود. می‌توان BDD را به طور بازگشتی از یک درخت خرابی ساخت و این یک روش محاسباتی کامل و موثر بوجود می‌آورد. این روش به خوبی در "NASA Fault Tree Handbook with Aerospace Applications version 1.1[1]"[۲] ارائه شده است.

رویکرد BDD هنگامی مفید است که کوتاه کردن محاسبات احتمال مجموعه‌های قطعی منتج به از دست رفتن درستی به‌طور غیر قابل‌قبول شده یا راه‌حل FTA بیش از حد طولانی شود، به‌ویژه هنگامی که بسیاری از رخدادهای با احتمال بالا در مدل ظاهر شوند. از آنجا که مسیرهای حداقل که در رویکرد BDD[3] بوجود آمده انفصال شده‌اند[4] (به بند ۴-۵-۵-۷ رجوع شود) محاسبه اهمیت و حساسیت را نیز می‌توان بطور مؤثر و دقیق انجام داد.

---

1 -Truncated

[۲]- اعداد داخل قلاب به کتاب نامه اشاره دارند.

3- Binary decision diagram

4 -Disjointed

۵-۴-۵ ترکیب با نمودار بلوکی قابلیت اطمینان

نمودار بلوکی قابلیت اطمینان متشکل از بلوک‌ها یا ماجول[1] هایی است که معرف گروهی از اجـزا یـا مُـدهای وقوع خرابی می‌باشند. این گروه‌ها معمولاً بعد از نمودار وظیفه‌ای محصول، سیسـتم یـا فرآینـد تشـکیل داده می‌شوند. این ماجول‌ها یا دارای نرخ معین وقوع خرابی یا قابلیت اطمینان محاسـبه شـده یـا احتمـال وقـوع خرابی برای استفاده مورد نظر یا پروفایل بهره‌برداری می‌باشند. به‌طور مرسوم، بلوک‌ها دارای نرخ وقوع خرابی می‌باشند که برابر مجموع نرخ‌های وقوع خرابی اجزای جداگانه است. به این طریق، تعامل وظیفه ای اجـزا در یک ماجول مد نظر قرار نمی‌گیرد.

برای افزایش صحت مدل‌سازی وظیفه ای در بلوک (نرم افزار/ سخت افزار، تعامل قطعـات مکـانیکی) قابلیـت اطمینان بعضی بلوک‌ها را می‌توان با درخت خرابی مدل کرد و سپس اطلاعات حاصل در مورد احتمال وقـوع این بلوک‌ها را می توان به آن بلوک ویژه اختصاص داد که خود بخشی از نمودار بلوک قابلیت اطمینان اسـت. به این شیوه از نمودارهای بلوک قابلیت اطمینان که معمولاً اسـتقلال وقـوع خرابـی اجـزا را در بلـوک فـرض می‌کنند، پیش‌بینی واقع بینانه‌تری به دست می‌آید.

۶ توسعه و ارزیابی

۶-۱ ملاحظات کلی

۶-۱-۱ مرور

درخت خرابی نمایش گرافیکی سازمان یافته‌ی وضعیت هایی است که علت وقوع یا علت موثر در وقوع برآمـد نامطلوب معین مرتبط با بالاترین رخداد را نشان می‌دهد. نمایش به شکلی انجام می‌گیرد که به‌راحتـی قابـل فهم و تحلیل بوده و در صورت لزوم جهت تسهیل شناسایی موارد زیر تجدید آرایش شود.

- عوامل موثر بر قابلیت اطمینان و سایر ویژگی‌های عملکردی سیستم. این عوامل برای مثال شامل نقص‌های طراحی ، تنش‌های محیطی یا بهره‌برداری، مُد خرابی اجزا، اشتباه‌های کاربر و خرابی نرم افزاری است.
- رخدادهای مشترک که می‌تواند بر بیش از یک برآمد از رخدادهای میانه در یک درخت خرابی تاثیر بگذارد. برای مثال، رخدادهای موثر بر بیش از یک جز وظیفه‌ای که می‌تواند فواید ردوندانسی خاص را از بین برده یـا بر دو یا چند بخش از محصول تاثیر گذارد که ممکن است از نظر بهره‌برداریی نامرتبط به نظر آید.

تحلیل درخت خرابی یک روش استقرایی (از بالا به پایین) برای تحلیل با هـدف بررسـی دقیـق علـت‌هـا، یـا ترکیبی از علت‌ها می‌باشد که می‌تواند منجر به بالاترین رخداد تعریف شده شود. این تحلیل بسته بـه دامنـه تحلیل می‌تواند کیفی، روش A، یا کمی، روش B، باشد..

در مواردی که احتمال وقوع رخداد اصلی را نتوان پیش‌بینـی کـرد، FTA کیفـی، روشA را مـی‌تـوان بـرای بررسی علل برآمدهای نامطلوب بالقوه به کار برد همراه با با رخدادهای اصلی مجزا با احتمال وقوع توصیفی از قبیل احتمال بسیار زیاد، احتمال زیاد، احتمال متوسط و احتمال کم.

---

1 -Module

FTA کمی، روشB، را وقتی می‌توان به کار برد که احتمال رخدادهای اصلی یا اولیه مشخص باشد. احتمال‌های وقوع رخداد میانه و بالاترین رخداد (حاصل) را می‌توان با استفاده از عبارات ریاضی مناسب محاسبه کرد.

۶-۱-۲ مفاهیم و ترکیبات رخدادها و حالت‌ها

برآمد نهایی درخت خرابی (بالاترین رخداد) می‌تواند فی النفسه، خرابی یا رخداد باشد. در اینجا درخت خرابی، خرابی یا رخدادی را که ناشی از رخدادهای موثر یا سایر خرابی‌هاست، توصیف می‌کند. در تحلیل درخت خرابی ، ترکیب معین رخدادها می‌تواند حالت‌ها یا رخدادها باشد در حالیکه سایرین باید با برآمد مطابقت داشته باشد. برای مثال، ورودی‌های دروازه OR که در آن برآمد یک حالت یا یک رخداد هستند می‌تواند حالت‌ها یا رخدادها باشند. کلیه ورودی‌های یک دروازه AND که به عنوان برآمد یک رخداد است باید رخدادها باشند در حالیکه اگر به عنوان برآمد، نمایشگر یک حالت باشد کلیه ورودی‌ها باید حالت باشند. حالت را می‌توان با احتمال وجود در زمان t معرفی کرد در حالیکه رخداد یا با نرخ وقوع خرابی یا تکرار وقوع خرابی با احتمال وقوع در زمان t مشخص می‌شود.

۶-۱-۳ درخت خرابی برای بررسی خرابی‌های منجر به سایر خرابی‌ها یا رخدادها

به‌طور مرسوم، درخت خرابی برای بررسی خرابی‌ها یا رخدادهای منجر به یک برآمد ساخته می‌شود. این مفاهیم مدتها در بسیاری از صنایع به کار رفته و در صنعت هسته‌ای از کارآیی و کاربرد خاصی برخوردار است. به این ترتیب، یک ابزار قدرتمند و ارزرشمند برای بررسی مسایل بالقوه، رخدادها، بهبودها و سایر معیارهای پیش‌گیرانه که یک برآمد نامطلوب را محدود کرده یا کاهش می‌دهد. یا آن را تخفیف می‌دهد به شمار می‌آید. یک برآمد، موفقیت یا خرابی، مورد بررسی قرار می‌گیرد و حالت‌ها یا رخدادهای منجر به خروجی مورد بررسی قرار می‌گیرد و احتمال وجود یا وقوع آن‌ها مشخص می‌شود و مدل درخت خرابی به طور مناسب ساخته می‌شود که همه‌ی این‌ها منجر به وجود یا وقوع آن برآمد مفروض می‌گردد.

در این کاربرد، درخت خرابی طبق توصیف بند ۷ ساخته و ارزیابی می‌شود، با این ذهنیت که برآمد بر اساس احتمال وجود خرابی یا وقوع رخداد معرفی می‌شود و ارتباطی به قابلیت اطمینان قلم یا سیستم مورد تحلیل ندارد. این امکان وجود دارد که به رخداد اصلی یا سایرین در این نوع تحلیل هیچ مقدار احتمال واقعی داده نشود و صرفا در بررسی رخدادی که احتمال وقوع آن وجود دارد مورد استفاده قرار گیرد (روش A)، دراین‌گونه موارد، ممکن است آن‌ها را احتمال توصیفی بسیار زیاد، متوسط یا کم، مشخص کرد و به عنوان عوامل موثر احتمالی در رخداد یا خرابی بالا ارزیابی نمود. این نوع درخت خرابی غالباً برای شناسایی خرابی اولیه یا رخداد اولیه به کار می‌رود که تنها عامل یا عامل عمده خرابی بالا یا بالاترین رخداد بوده و درانواع وسیعی از صنایع به کار می‌رود مانند :کارخانه‌های خودروسازی، هسته‌ای، تولیدی و غیره.

۶-۱-۴ استفاده از FTA در ارزیابی قابلیت اطمینان و بهبود طی تکوین محصول[1]

در این کاربرد که بر اساس روش نوع B، FTA است، درخت خرابی می‌تواند کل محصول، یا بخش‌هایی از محصول را که ممکن است برای قابلیت اطمینان یا ایمنی بهره‌برداریی آن ریسک ساز باشد مدل سازی کند. در این مورد، روش B، تحلیل احتمال وقوع می‌تواند با روش مرسوم مانند تحلیل خرابی وابسته به ایمنی یا رخداد محصول یا تحلیل مشروح وقوع خرابی بالقوه در دوره زمانی معین، که ممکن است منجر به بیان عدم قابلیت اطمینان یا احتمال وقوع خرابی در آن دوره گردد، تعین شود. در این کاربرد روش درخت خرابی، اصول مُدهای وقوع خرابی از بالا به پایین و تحلیل آثار تبعیت می‌کند که در آن هر مُد وقوع خرابی بالقوه می‌تواند منجر به رخداد یا خرابی که منجر به وقوع خرابی محصول گردد.

FTA اختصاصاً مفید خواهد بود چون مدل سازی می‌تواند منعکس کننده دینامیک رخدادها در محصول، تعامل نرم افزاری/ سخت‌افزاری و نیز تعاملات بین خرابی یا رخداد شاخص مُدهای وقوع خرابی بالقوه باشد. نمایش این تعامل در FMEA متعارف امکان‌پذیر نبوده و مدل سازی با استفاده از نمودارهای بلوکی قابلیت اطمینان مرسوم بسیار مشکل است. همچنین، برآورد قابلیت اطمینان محصول واقعی‌تر خواهد بود اگر فقط مُدهای وقوع خرابی موثر بر وقوع خرابی محصول، مطابق تعریف، مورد بررسی قرار گیرند.

توسعه درخت خرابی بایستی در مرحله طراحی سیستم آغاز شده و در کلیه مراحل تکوین محصول ادامه داشته باشد. تکامل درخت خرابی بایستی به‌گونه‌ای باشد که پیشرفت طراحی را منعکس کند. بنابراین، افزایش آگاهی از مُدهای وقوع خرابی همزمان با پیشرفت طراحی به‌دست می‌آید. «تحلیل همزمان با طراحی»[2] تغییر طراحی زود هنگام سیستم‌ها را امکان‌پذیر می‌سازد. بسیاری از درخت‌های خرابی بزرگ خواهند بود، که در این موارد ممکن است به نرم‌افزار تحلیل درخت خرابی برای انجام آن‌ها نیاز باشد. نرم‌افزار جهت تسهیل تحلیل و امکان برآورد سریع و ساده احتمال بالاترین رخداد است. برنامه‌های نرم‌افزاری بسیاری وجود دارد و شاید بسیاری دیگر نیز ساخته شود که همه آنها کاربردهای متفاوتی با توجه به نیاز کاربر دارند.

توجه به این نکته مهم است که رخدادهای درخت خرابی تنها محدود به وقوع خرابی های نرم‌افزاری و سخت‌افزاری نیستند بلکه شامل تعامل آنها و سایر فاکتورها مثلا عوامل و اقدام‌های انسانی و فرآیندهای مرتبط با بالاترین رخداد می‌باشند.

هنگام تحلیل کمی اگر نتوان احتمال وقوع برخی رخدادها را مشخص کرد، حتی اگر این خرابی‌ها یا رخدادها (وقوع خرابی) سیستماتیک باشند، بایستی این رخدادها و ترکیب وظیفه‌ای (منطقی) آنها در تحلیل لحاظ شود. در این صورت، این حالات وقوع خرابی برای پیش‌بینی قابلیت اطمینان (یا احتمال وقوع خرابی) لحاظ نخواهد شد، اما وجود آنها حتی به روش کیفی مدنظر قرار می‌گیرد.

به منظور استفاده اثربخش از فن درخت خرابی به عنوان روش تحلیل سیستم، روش اجرایی بایستی حداقل شامل موارد زیر باشد:

- تعریف دامنه تحلیل؛

---

1 -Product development

2 -Analysis concurrent with design

- آشنایی با طراحی، وظیفه‌ها و بهره برداری سیستم؛
- تعریف بالاترین رخداد؛
- ساختمان درخت خرابی؛
- تحلیل منطق درخت خرابی؛
- گزارش مربوط به نتایج تحلیل‌ها؛
- ارزیابی بهبودهای قابلیت اطمینان و سبک و سنگین کردن ها

اگر تحلیل عددی طرح ریزی شود، تعریف فن ارزیابی عددی احتمالات رخداد اولیه یا سایر صفات[1] مانند شدت وقوع خرابی، میانگین زمان بین وقوع خرابی‌ها (MTBF)[2] یا میانگین زمان تا وقوع خرابی (MTTF)[3] و غیره ضروری است. انتخاب داده‌های مورد استفاده و ارزیابی عددی قابلیت اطمینان یا مقیاس‌های عدم قابلیت اطمینان خارج از دامنه این استاندارد می‌باشد.

اهداف چندگانه ای در درخت خرابی طراحی سیستم وجود دارد. یکی از این اهداف مدل‌سازی ساختار و وظیفه‌مندی محصول از بالا به پایین و جستجو برای مُد های وقوع خرابی بالقوه و علل آنها است که ممکن است به برآمدی تحت عنوان رخداد نهایی منجر شود. بر اساس این اطلاعات، عوامل موثر در احتمال وقوع بالاترین رخداد یا عدم قابلیت اطمینان سیستم (به صورت کیفی و کمی برای شناسایی علل موثر) بررسی رو به پایین را به منظور شناسایی علت‌های مرتبط آنها ادامه می‌دهند. این مساله سبک و سنگین کردن و مطالعات راه‌حل‌های احتمالی را برای کاهش مُدهای وقوع خرابی بالقوه غیر قابل قبول و سرانجام ارزیابی بهبود قابلیت اطمینان به دست آمده را امکان‌پذیر می‌سازد.

با وجود مدلی از ساختار و وظیفه‌مندی محصول، FTA بایستی توسط افرادی که شناخت لازم در مورد سیستم، خصوصیات طراحی و بهره برداری آن و افراد آموزش دیده در زمینه FTA و سایر روش‌های مدل سازی قابلیت اطمینان مربوطه‌اند اجرا شود. تحلیل‌گر باید قادر باشد که عوامل موثر در مُد وقوع خرابی بالقوه را ارزیابی کرده و به‌صورت منطقی علل احتمالی عملکرد ناهنجار محصول را شناسایی کند. کمبود دانش مهندسی در مورد طراحی محصول و مدهای وقوع خرابی بالقوه، منجر به ایجاد درخت خرابی‌ای خواهد شد که ممکن است نمایانگر صحیح وظیفه‌مندی محصول نبوده و در نتیجه نتایج تحلیلی بی‌معنی شود. بعد از آماده شدن FTA، بایستی توسط تیم مهندسی شرکت کننده در طراحی محصول از نظر صحت و کامل بودن مورد بازنگری قرار گیرد. اقدامات اصلاحی مورد توافق باید ثبت و پی‌گیری شود.

۲-۶ اطلاعات مورد نیاز سیستم

سیستم مورد تحلیل بایستی با توصیف وظیفه‌مندی سیستم و با شناسایی سطوح مشترک (اینترفیس های) سیستم مشخص شود این تعاریف بایستی شامل موارد زیر باشد:

- خلاصه منظور طراحی؛
- تعریف این‌که چه چیزهایی، وقوع خرابی سیستم را تشکیل می دهد،

---

1 -Attributes
2-Mean time between failures
3 - Mean time to failure

- ساختار وظیفه ای سیستم که معمولاً با نمودار بلوکی وظیفه‌ای نمایش داده می‌شود؛
- مرزهای سیستم از قبیل سطوح مشترک الکتریکی، مکانیکی و سطوح اشتراک بهره برداری که در فرمان تعامل و سطوح مشترک با سایر سیستم‌هاست. این مرزها بهتر است که با تعریف وظیفه‌ه‌ای ویژه‌ای مانند اتصالات الکتریکی(داخلی یا خارجی)، فیوز که سطوح مشترک را تشکیل می‌دهند توصیف شود؛
- ساختار فیزیکی سیستم در مقایسه با ساختار وظیفه‌ای؛
- شناسایی مدهای بهره برداری سیستم همراه با توصیف بهره برداری سیستم و عملکرد مورد انتظار و قابل قبول سیستم، در هر مد بهره برداری؛
- پروفایل بهره برداریی سیستم؛
- شرایط محیطی سیستم و جنبه‌های انسانی مربوطه (به‌طور مثال میزان آموزش برای کاربران و پرسنل نگهداری)؛
- فهرست اسناد مورد استفاده مانند نقشه‌ها، مشخصات، راهنمای بهره برداری که جزئیات بهره برداری و طراحی تجهیزات را ارائه می‌دهد. مدت کار، بازه‌ی زمانی بین آزمون‌ها و زمان موجود برای اقدامات اصلاحی نگهداری و همچنین جزئیات تجهیزات و نیروی پشتیبانی دخیل نیز بایستی معلوم باشد. اطلاعات ویژه در خصوص وظایف تعیین شده طی هر فاز بهره برداری نیز مورد نیاز است.

۳-۶ توصیف و ساختار گرافیکی درخت خرابی

اجزای درخت خرابی به شرح ذیل است:

دروازه‌ها

- نمادهایی که رابطه منطقی بین رخداد ورودی و رخداد خروجی را نشان دهند؛
- دروازه‌های استاتیکی- برآمد به ترتیب وقوع ورودیها وابسته نیست؛
- دروازه‌های دینامیکی- برآمد به ترتیب وقوع ورودیها وابسته است.

در پیوست الف جدول الف-۱ توصیف دروازه‌های دینامیکی و توضیحات مربوط به کاربرد آنها نشان داده شده است. جدول الف ۳ نمونه‌ای از دروازه PAND در شکل الف -۱ را نشان می دهد.

رخدادها

پایین‌ترین سطح ورودی‌ها در یک درخت خرابی، نمادها و تعاریف مورد استفاده رایج در پیوست الف جدول الف-۱ نشان داده شده است.

اجزا گرافیکی درخت خرابی به شرح زیر است:

الف) نماد منطقی درخت خرابی (دروازه‌ها)؛

ب) خطوط ارتباط ورودی دروازه؛

پ) توصیف‌های رخدادهای میانی؛

ت) نمادهای انتقال به داخل یا خارج؛

ث) نمادهای رخداد اولیه.

درخت خرابی بایستی شامل همه رخدادهای مربوطه باشد. این رخدادها بایستی شامل آثار محیطی یا سایر شرایط تنش باشند که قلم در معرض آن قرار می گیرد و شامل نرم افزار و کنترل‌ها و سایر پایش وضعیت‌هایی است باشد در طول بهره برداری امکان‌پذیر هستند حتی اگر خارج از مشخصات طراحی باشند.
رخدادهایی که تحلیل‌گر به‌عنوان تحلیل‌های غیر قابل کاربرد بررسی کرده است بایستی در گزارش قید شوند ولی در درخت خرابی نهایی در نظر گرفته نشوند.
چنانچه درخت خرابی موکد بر دو یا چند مشکل عملکردی سیستم ناشی از یک خرابی موجود باشد آن‌گاه توصیه می‌شود که رخداد توصیف کننده آن خرابی در چندین نقطه در درخت خرابی گنجانده شود. همچنین توصیه می‌شود که این رخداد تحت عنوان یک رخداد مشترک ذکر گردد. در تحلیل کمی، رخداد مشترک فقط یک‌بار در محاسبات لحاظ می‌گردد. توصیه می‌شود که تمامی معیارهای ناپیوسته نشان داده شده در بند ۷-۵-۵-۴ اعمال گردد. جهت اجتناب از مشمولیت تصادفی رخدادهای مشترک در محاسبات چندگانه، بهتر است که طبقه‌بندی مرسوم اینگونه رخدادها انجام و مورد استفاده قرار گیرد. این نوع طبقه‌بندی سازگاری دارد. اگر نرم‌افزار کامپیوتر برای پایش ارزیابی درخت خرابی مورد استفاده قرار می‌گیرد لازم است از قواعد و ترتیبات مناسب استفاده شود. وقتی درخت خرابی ساخته می‌شود، می‌تواند به شکل عمودی، از بالا به پایین یا به شکل افقی از چپ به راست نمایش داده شود. وقتی به شکل افقی ارائه می‌شود کلیه نمادهای ارائه شده در جدول الف ۱ تا جدول الف ۴، ۹۰ درجه خلاف جهت عقربه ساعت چرخانده می‌شوند.
درخت‌های خرابی را نیز می‌توان در جهت‌های متضاد خواند یا مورد بررسی قرار داد مثلا هنگام برخورد با رخداد ها، وقوع خرابی‌ها یا غیره.

۷ ارزیابی و ایجاد درخت خرابی

۷-۱ کلیات

ایجاد درخت خرابی با تعریف بالاترین رخداد آغاز می‌شود. ایجاد درخت خرابی در کاربردهای مرسوم یا برای قابلیت اطمینان یک سیستم و تحلیل مُد وقوع خرابی، یک روش قیاسی است که در آن، تحلیل از رخداد نامطلوب بالا آغاز می‌گردد، رخداد نامطلوبی که در دامنه تحلیل مشخص شده است. هنگامی که درخت خرابی به اندازه مورد نظر توسعه یافت به نمایش گرافیکی کلیه رخدادهایی تبدیل می‌شود که با همدیگر یا به تنهایی به وقوع بالاترین رخداد کمک می‌کنند.

۷-۲ دامنه تحلیل

در تعریف دامنه تحلیل بایستی تعریف سیستم مورد تحلیل، مقصود و گستره‌ی تحلیل و مفروضات اصلی گنجانده شود. این مفروضات بایستی شامل مفروضات مرتبط با شرایط بهره برداری و نگهداری مورد نظر و نیز عملکرد سیستم تحت کلیه شرایط کاربردی ممکن، باشند.
FTA می تواند اطلاعاتی را در موارد زیر فراهم سازد
- تحلیل قابلیت اطمینان سیستم در مواردی که احتمال وقوع رخداد اولیه مشخص است؛

- علت (علت‌های) ریشه ای برآمد نامطلوب که واقع شده و ممکن است نیازمند اقدام اصلاحی مناسب باشد؛
- هنگامی که بالاترین رخداد باید تعیین شود، دامنه‌ی FTA به یک سیستم پیچیده تبدیل می شود. در اینجا، بر خلاف مدل سازی قابلیت اطمینان و روش‌های تحلیلی پیش‌بینی، دامنه تحلیل تنها شامل آن‌دسته مُدهای وقوع خرابی یا رخدادهای بالقوه‌ای می‌شود که بر بهره‌برداری سیستم تاثیر می‌گذارد یعنی تنها آن دسته از مُدهای وقوع خرابی که مربوط به وقوع بالاترین رخداد است. این مساله به یک ارزیابی سیستم متمرکز می انجامد، که بهتر می‌تواند با عملکرد میدانی مقایسه شود.

۳-۷ آشنایی با سیستم

برای انجام موفق تحلیل درخت خرابی به دانش مشروح سیستم نیاز است. با این وجود، بعضی سیستم‌ها ممکن است به حدی پیچیده باشد که خارج از فهم کامل یک فرد باشند. در این صورت، فرآیند آشناسازی[1] ایجاب می‌کند که دانش تخصصی لازم از طریق فعالیت تیمی حاصل گردد.

۴-۷ ایجاد درخت خرابی

ایجاد درخت خرابی با تعریف بالاترین رخداد یا برآمد نامطلوب آغاز می‌گردد که بهتر است بدون ابهام تعریف گردد. بالاترین رخداد کانون کل تحلیل است. این رخداد ممکن است شروع یا وجود وضعیت خطرناک (تحلیل ایمنی) یا ناتوانی سیستم جهت عملکرد مطلوب باشد.

اگر در تحلیل عملکرد یا قابلیت اطمینان سیستم، یک رخداد خروجی از یک دروازه، ناتوانی در اجرای وظیفه را تعریف کند، رخدادهای ورودی متناظر می‌تواند نمایشگر علل مناسب باشند: مانند: وقوع خرابی به علت خرابی سخت‌افزاری، خرابی نرم‌افزاری، محدودیت‌های عملکرد، فرمان نادرست (خرابی کنترل) و خطای انسانی باشد.

توسعه یک شاخه خاص از درخت خرابی بعد از رسیدن به یک یا چند مورد از موارد زیر پایان می‌یابد:
- رخدادهای اولیه یعنی رخدادهای مستقلی که برای آنها ویژگی‌های مربوطه را بتوان بوسیله ابزاری غیر از درخت خرابی تعریف کرد.؛
- رخدادهایی که طبق تعریف تحلیل‌گر ، نیازی به توسعه بیشتر ندارند؛
- رخدادهایی که در یک درخت خرابی دیگر توسعه‌یافته یا خواهد یافت- انتقالات، اگر این رخداد بیشتر توسعه یابد، چنین رخدادهایی مشخصات یکسانی مانند رخدادهای متناظر در دیگر درخت خرابی را در بر داشته باشد به‌طوری‌که درخت بعدی عملاً تداوم درخت قبلی باشد.

۵-۷ ساختمان درخت خرابی

۱-۵-۷ قالب درخت خرابی

درخت‌های خرابی را می‌توان به شکل عمودی یا افقی ترسیم کرد. در صورت استفاده از آرایش عمودی، بالاترین رخداد در راس صفحه و رخداد اصلی در قسمت پایین آن قرار می‌گیرد. اگر از آرایش افقی استفاده شود بالاترین رخداد باید یا در قسمت چپ یا راست صفحه قرار گیرد.

---

1 -Familirization

مثالهای استاندارد (شکل ۱ و سایر شکل‌ها) ایجاد و نمایش یک درخت خرابی را نشان می‌دهند، علاوه بر نمادهای تعریف شده برای منطق درخت خرابی، مثالها شامل کادر توصیف رخداد و نیز وظیفه یا حالت نمایش رخداد هستند.

۷-۵-۲ استفاده از FTA کمی (روشB) در توسعه سیستم یا محصول برای بهبود قابلیت اطمینان

۷-۵-۲-۱ کلیات

FTA روشی سیستماتیک برای شناسایی رخدادهایی است که در وقوع بالاترین رخداد و با استفاده از روشهای قیاسی قبلی، در رخدادهای میانی و سرانجام در رخداد اولیه موثرند. این تحلیل سیستماتیک مُدهای وقوع خرابی اجزا سیستم و عوامل موثر در احتمال وقوع خود آن‌ها را شناسایی می‌کنند مانند: تنش‌های بهره برداریی یا محیطی شامل دستورات نرم‌افزاری، عوامل انسانی و غیره است.

تفاوت اصلی بین FTA و سایر روش‌های مدل‌سازی و تحلیل قابلیت اطمینان این است که FTA تنها شامل رخدادهایی می شود که در وقوع بالاترین رخداد موثر بوده و ترکیب وظیفه‌ای آنها و تعامل دینامیک ممکن و وابستگی درونی آنها را مدل‌سازی می‌کند، در حالیکه روشهای دیگر با نرخ وقوع خرابی اجزا (نه احتمال مد وقوع خرابی اجزا) یا فرضیه رایج وقوع خرابی مستقل سروکار دارند. برای مثال، در یک خازن صافی، ولتاژ می‌تواند وقوع خرابی باز (حدود ٪ ۳۵ وقوع خرابی‌های آن)، اتصال کوتاه (حدود ۵۵٪ از وقوع خرابی‌های آن) یا تغییر ظرفیت (۱۰٪ باقی‌مانده وقوع خرابی‌های آن را) شامل گردد اما تنها مُد وقوع خرابی اتصال کوتاه، عامل وقوع خرابی محصول می‌باشد، از این رو تنها حدود ٪ ۵۵ از احتمال وقوع خرابی آن به حساب می‌آید. این مساله شناسایی واقعی آن دسته ازمُدهای وقوع خرابی یا عللی را امکان‌پذیر می‌سازد که نیازمند به توجه طراح می‌باشد.

توانمندی FTA برای مدل کردن صحیح توالی رخدادهای اولیه یا میانی (به کمک تحلیل مارکوف)، به عنوان ورودی به رخداد میانی دیگر، آن را به ابزاری سودمندی برای شناسایی آن دسته از رخدادها / وظایف اولیه یا رخدادهای میانی تبدیل می‌کند که این رخدادها جزو عوامل اصلی موثر در عدم قابلیت اطمینان محصول به‌شمار می‌روند. این امر موجب بهبود طراحی یعنی کاهش ضعف[1] طراحی شده و بازنگری FTA را برای تصدیق بهبود یا انجام مطالعه سبک و سنگین کردن بین دو یا چند گزینه بهبود را امکان‌پذیر می‌سازد.

درکلیه مدلهای دروازه سری، لازم است به خاطر داشته باشیم که مقادیر احتمال، فقط مقادیر آن مُدهای وقوع خرابی و عوامل موثر بر آنها یا احتمالات ترکیبات استاتیک یا دینامیک مُدهای وقوع خرابی هستند که منجر به کاهش وقوع خرابی یا وظیفه سیستم می‌شوند. مقادیر مُدهای وقوع خرابی و عوامل موثر در آنها می‌باشند یا احتمال ترکیبات استاتیک و دینامیک مُدهای وقوع خرابی است که منجر به فقدان وظیفه و وقوع خرابی سیستم می‌شوند.

1 -Mitigate design flaws

۷-۵-۲-۲ پیکربندی ساختار سیستم سری

در مدل سازی قابلیت اطمینان، مجموعه‌ها (بلوک‌ها یا اجزا در نمودار بلوکی قابلیت اطمینان) در سیستم دارای پیکره بندی سری هستند.

مدل متناظر در درخت خرابی، اینطور است که تمام آن بلوک‌ها (دروازه‌ها یا رخدادها) به یک دروازه OR وصل می‌شوند.

ریاضیات قابلیت اطمینان سیستم بالا متشکل از n تعداد بلوک‌های مستقل، به صورت زیر است:

$$R_S(t) = R_1(t) \cdot R_2(t) \cdot R_3(t) ... R_I(t) ... R_n(t) \qquad (۱)$$

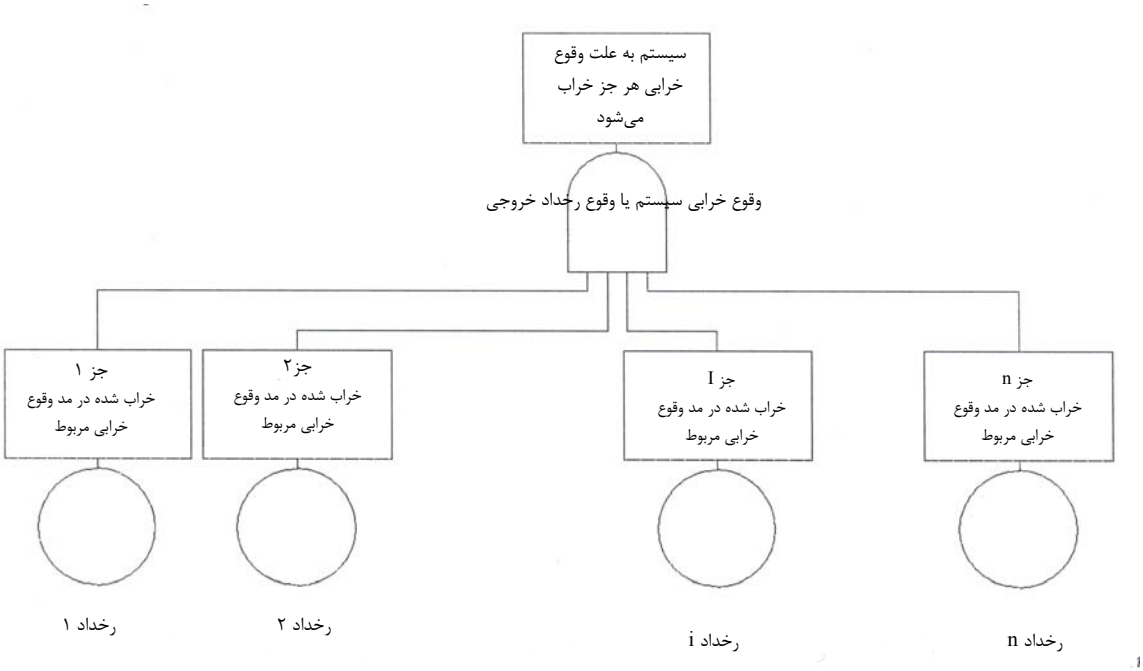
عبارت فوق درباره‌ی قابلیت اطمینان این‌گونه بیان می‌شود که بلوک ۱ وبلوک ۲ و بقیه بلوک‌ها باید قابل بهره برداری باشند تا سیستم قابل بهره برداری باشد. در FTA عکس این مساله به‌کار می‌رود. حاصل وقوع خرابی یا بر اثر وقوع خرابی جزء ۱ یا جزء ۲ و غیره حاصل می‌شود. به همین علت است که دروازه OR پیکربندی یک سیستم سری یا مجموعه را نشان می‌دهد. ریاضیات مربوط به دروازه OR مشابه فرمول نشان‌داده شده برای سیستم سری است با این تفاوت که بر حسب احتمال وقوع خرابی F(t) بیان می‌شود که یک مکمل احتمالی برای قابلیت اطمینان است.

$$F(t) = 1 - R(t) \qquad (۲)$$

احتمال یک برآمد نامطلوب برای یک دروازه OR (سیستم) متشکل از N ورودی مستقل دروازه چنین خواهد بود:

$$F_S(t) = 1 - (1 - F1(t)).(1 - F_2(t)) \cdot ..... \cdot (1 - F_I(t) \cdot ..... \cdot (1 - F(_n(t)) \qquad (۳)$$

این سیستم وقتی خراب می‌شود که هر یک از اجزاء آن (بلوک‌ها) خراب شوند. نمونه‌ای از دروازه OR در شکل ۲ نشان داده شده است. در شکل ۲ و همه شکل‌های بعدی در این بند، مُد وقوع خرابی مربوط به یک جزء، مُدی از وقوع خرابی است که به عنوان یک رخداد ورودی موجب وقوع رخداد خروجی خواهد شد.



شکل ۲- نمایش ساختار سری درخت خرابی

۳-۲-۵-۷ پیکربندی سیستم موازی، سیستم‌های ردوندانسی

۱-۳-۲-۵-۷ ردوندانسی فعال

این بند فرعی فرض می‌کند که ویژگیهای وقوع خرابی (مُدها) برای هر ورودی در ردوندانسی فعال، یکسان بوده و مستقل از تعداد ورودی‌های در حال کار است و نیز فرض را بر این می‌گذارد که هر ورودی نسبت به بلوک ردوندانسی فعال، مستقل است، هنگامی‌که مستقل نباشد می‌توانید به مطلب مربوط به درپیوست ب برای راهنمایی‌های بیشتر رجوع کنید.

اگر قرار باشد رخداد خروجی فقط در صورتی رخ دهد که همه رخدادهای مستقل مؤثر رخ دهند، آنگاه باید با یک دروازهAND مرتبط شوند. این‌گونه پیکربندی که می‌تواند ردوندانت باشد برای تحلیل قابلیت اطمینان به این پیکره بندی، پیکره بندی موازی اطلاق می شود. گرچه پیکربندی فیزیکی ممکن است متفاوت باشد.

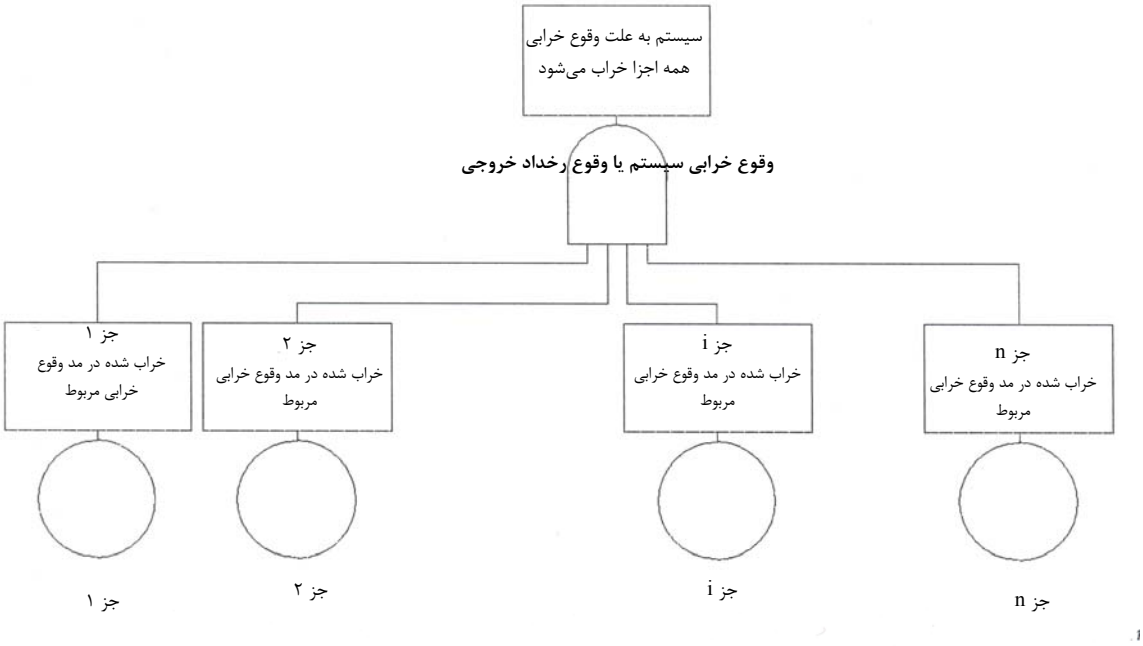
شرایط استقلال وقتی برآورده می‌شود که احتمال رخدادهای ورودی بدون توجه به حالت ورودی‌های، دیگر تغییر نکند. عبارت ریاضیاتی مربوطه در قابلیت اطمینان این است که سیستم در صورتی قابل بهره برداری است که جزء ۱ یا جزء ۲ یا حداقل یکی از آنها کار کند این به این معنی است که اگر همه اجزاء خراب باشند، سیستم خراب می شود.

$$R_S(t) = 1 - \prod_{i=1}^{n} \left(1 - R_i(t)\right) \qquad (۴)$$

در FTA، این مساله با یک دروازه AND دارای n ورودی دروازه یا رخداد نمایش داده می‌شود به این معنی که سیستم خراب می‌شود اگر جزء ۱ و جزء۲ و بقیه اجزاء خراب شوند و با ریاضیات مشابه احتمال وقوع خرابی چنین خواهد بود:

$$F_S(t) = \prod_{i=1}^{n} \left(F_i(t)\right) \qquad (۵)$$

یک نمایش از ردوندانسی که در آن بقای یک جزء برای بهره برداری موفق سیستم کفایت می کند یا این که سیستم در صورتی خراب می شود که همه اجزا خراب شده باشند، در شکل ۳ نشان داده شده است.



شکل ۳- نمایش درخت خرابی به صورت موازی، ردوندانسی فعال

اجزای ردوندانت ممکن است در مد بار مشارکتی[1] کارکند (مانند ژنراتورهای یک شبکه) و احتمال رخداد خرابی، اجزای باقی[2] ممکن است با خرابی هر یک افزایش یابد. این‌گونه تغییرات در احتمال رخداد الزام استقلال برای استفاده‌ی یک دروازه ساده AND را نقض می‌کند.

اگر قرار باشد یک خروجی تنها در شرایطی رخ دهد که همه رخدادهای مؤثر رخ دهند اما رخدادهای ورودی به همدیگر وابسته باشند، در این صورت نمی‌توان از دروازه AND استفاده کرد و از دروازه دینامیک استفاده می‌شود.

وقتی ردوندانسی چنان باشد که وضعیت موفق سیستم باقی ماندن k از n تعداد بلوک یکسان در حال بهره برداری باشد ریاضی عدم اطمینان مورد استفاده در FTA مطابق فرمول معمول زیر است:

$$R_S(t) = 1 - \sum_{i=0}^{k-1} \frac{n!}{i!(n-i)!} \left[R_O(t)\right]^i \cdot \left[1 - R_O(t)\right]^{n-i}$$

یا (۶)

1 -Load sharing
2 -Surviving

$$F_S(t) = \sum_{i=0}^{k-1} \frac{n!}{i!\cdot(n-i)!} \cdot [1 - F_O(t)]^i \cdot [F_O(t)]^{n-i}$$

در FTA این ترکیب رخدادها بوسیله یک دروازه رای اکثریت نشان داده می‌شود، که در آن تعداد رای m=n-k+1 و نماد m در دروازه مربوطه مشخص می‌کند که چه تعداد رخداد باید واقع شوند تا رخداد در درخت مربوطه منتشر شود. به عنوان مثال، اگر روندانسی مورد نیاز ۳ از ۶ باشد، رای اکثریت ۴ است، در صورت وقوع چهار رخداد (نامطلوب) ورودی تنها دو جزء عملیاتی (موفق) باقی می‌ماند، که به این معنی است که سیستم خراب شده است زیرا شرایط لازم این بود که سه جزء از شش جزء در حال بهره برداری باقی بماند. دروازه رای اکثریت همراه با سایر دروازه‌های مورد استفاده، در مدل‌سازی قابلیت اطمینان در شکل ۴ نشان داده شده است.

۷-۵-۲-۳- ۲ ردوندانسی غیر فعال(حاضر به خدمت)

ردوندانسی حاضر به خدمت، برای زمانی است که تنها شمار معینی از اجزاء برای بهره برداری فعال، لازم باشند و در صورت خرابی یک یا چند جزء، یک یا چند جزء یدکی جایگزین، فعال می‌شوند تا عملکرد اجزاء خراب را بر عهده گیرند. خرابی سیستم زمانی تحت عنوان رخداد تعریف می‌شود که تعداد کل اجزاء وظیفه‌ای، کمتر از تعداد لازم برای بهره برداری سیستم باشد. اجزاء ردوندانت (یدکی) ممکن است در تحلیل، موضوع خرابی نباشند (یدکی سرد)، یا در معرض احتمال وقوع خرابی میانی قرار داشته باشند(یدکی گرم) یا این‌که در بهره برداری فعال در معرض خرابی قرار گیرند. مانند موقع بهره‌برداری(یدکی داغ).

نمایش ردوندانسی حاضر به خدمت با دروازه‌های استاتیک امکان‌پذیر نیست. گرچه، نماد دروازه SPARE را می‌توان به کار برد. تحلیل مارکوف را باید برای تحلیل این دروازه به کار برد.

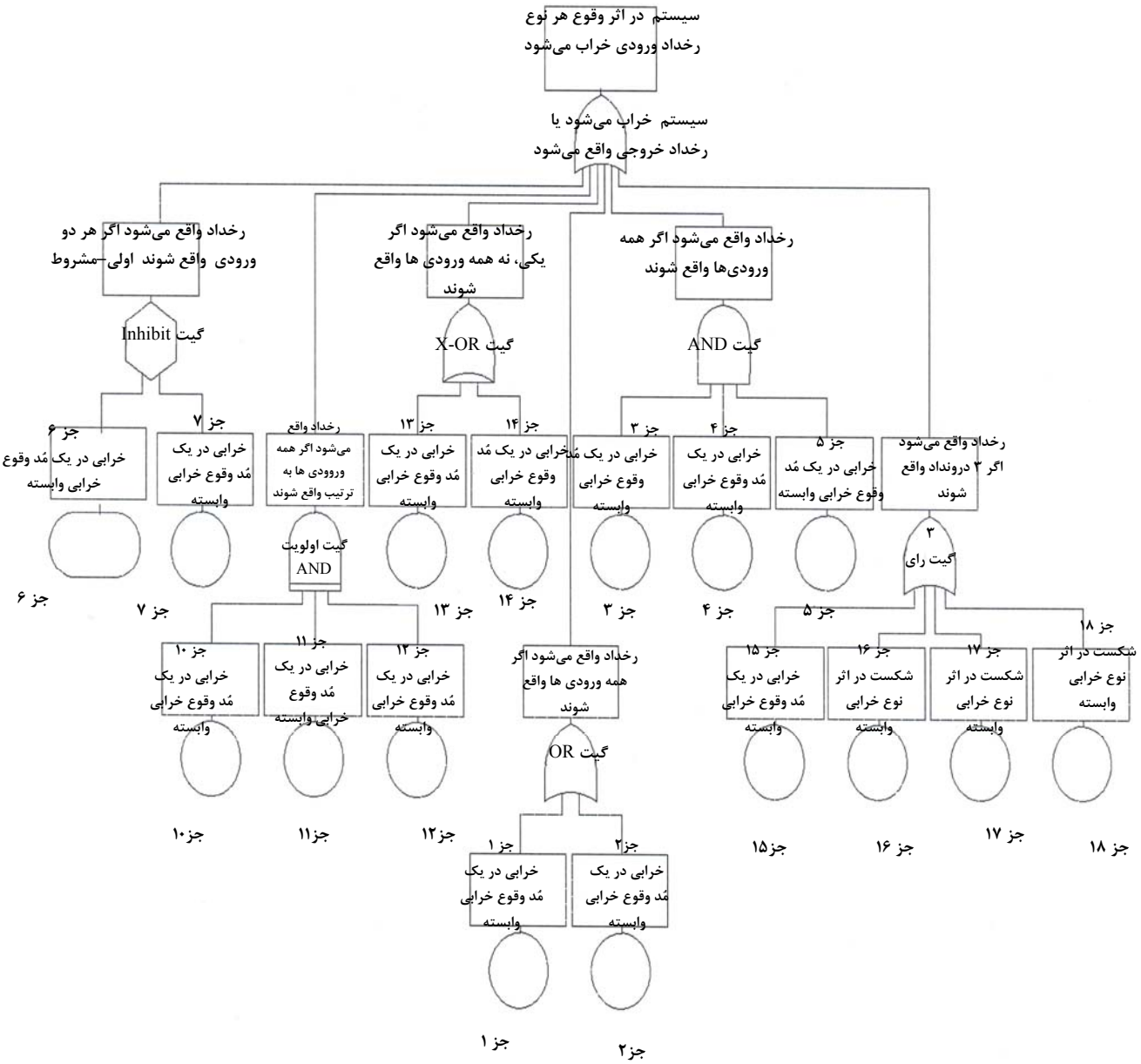
ردوندانسی حاضر به خدمت در دروازه‌های دینامیک عملکرد موفقی دارد. با این وجود دروازه SPARE برای سیستم‌های ردوندانسی که در آن احتمال رخداد تغییر می‌کند به کار می‌رود.

۷-۵-۲-۴ نمایش رخدادهای احتمال شرطی تکرار شده(علت مشترک) و انتقال به خارج رخدادها

احتمال شرطی زمانی است که احتمال وقوع یک رخداد به وقوع رخداد دیگری وابسته باشد. رخداد دوم فقط وقتی رخ می‌دهد که رخداد اول رخ داده باشد.

احتمال شرطی نیز تحت عنوان دروازه‌های دینامیکی که از تحلیل مارکوف استفاده می‌کنند بیان می‌شوند مانند دروازه‌های AND اولویت‌دار که درجدول الف -۴ ، پیوست الف تعریف شده است.

نمونه‌ای از احتمال شرطی به عنوان بخشی از شکل ۴ نشان داده شده است.



شکل۴- مثالی برای درخت خرابی که انواع مختلف دروازه ها را نشان می دهد

نمایش گرافیکی درخت خرابی که در شکل ۱ و شکل های دیگر این استاندارد نشان داده شده اند بایستی فقط به عنوان نمونه در نظر گرفته شوند.

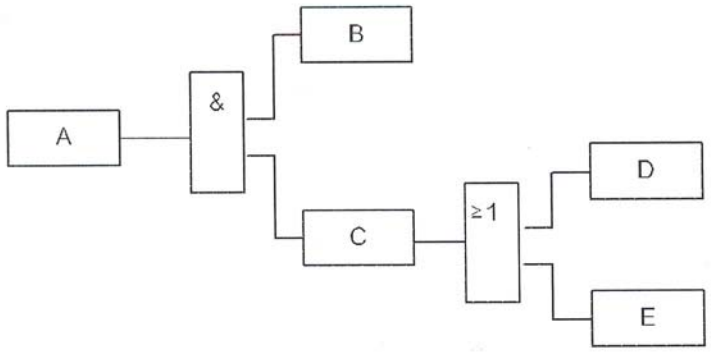
۷-۵-۲-۵ نمایش بصری درخت خرابی

درخت‌های خرابی می‌تواند انواعی از گرافیک‌ها را داشته باشد که به سلیقه و نمایش رایج در کشورهای مختلف و کاربردهای متفاوت بستگی دارد. بعضی از آنها از اشکال مستطیلی با نمادهایی مانند & برای دروازه AND و $\geq$ برای دروازه OR استفاده می‌کنند. در این مورد دروازه NULL همچنین در دسته دروازه OR قرار می‌گیرد. به استثنای این که چنین دروازه ORی فقط یک رخداد ورودی دارد، مشابه با دروازه های NULL، نمایانگر یک رخداد برآمد است که فقط یک رخداد ورودی دارند.

هنگام نمایش دروازه‌ها و رخدادها به صورت مستطیل، لازم است در تعریف مناسب و علامت گذاری واضح این نمادها دقت لازم به عمل آید.

نمایش دروازه‌ها و رخدادها به‌صورت مستطیل در شکل ۵ نشان داده شده است.

در شکل ۵، رخداد A تنها در صورتی رخ می‌دهد که رخدادهای B و C رخ دهند. رخداد C در صورتی رخ خواهد داد که رخداد D یا E رخ دهد.



شکل ۵- دروازه‌های چند ضلعی و نمایش رخدادها

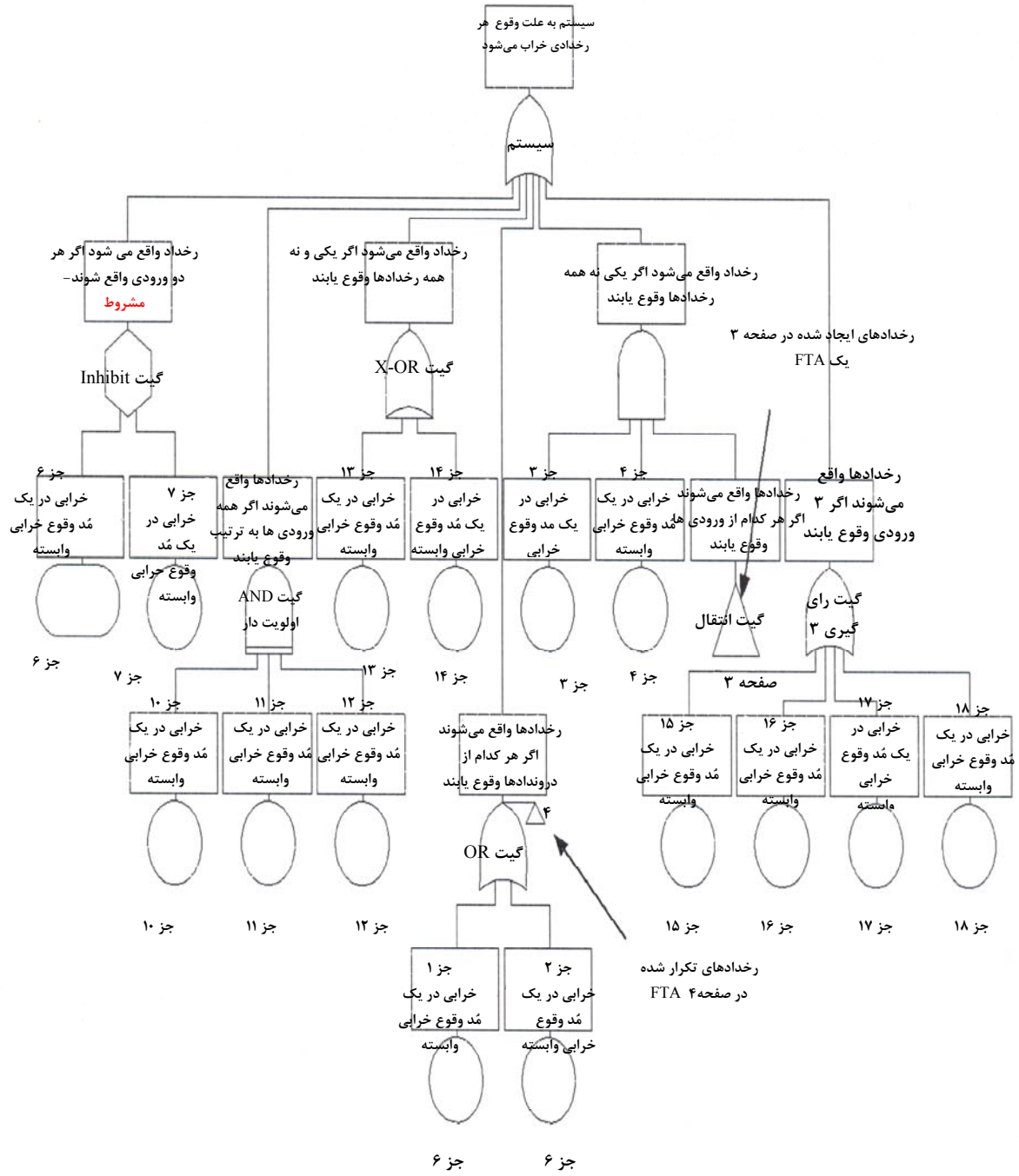
یادآوری- برای هررخداد A، B و غیره ترجیح داده می‌شود که نام یا توصیف رخداد ابتدا قید شود و سپس کد رخداد و احتمال وقوع آن ذکر گردد.

چنانچه رخدادی شاخص یک رخداد تکراری یا یک رخداد علت مشترک باشد، در درخت خرابی مکرراً نشان داده می‌شود اما با یک علامت[1] که به عنوان یک رخداد ورودی برای سایر رخدادها در درخت خرابی نمایش داده می‌شود. کلیه رخدادها با علت مشترک یا تکراری در این مجموعه باید دارای کد مشابه و نماد انتقال بداخل یا نمادی که معمولاً در یک درخت خرابی خاص به این منظور به‌کار می‌رود باشند. این قاعده برای کلیه رخدادهای تکراری یا علت مشترک به‌کار می‌رود به جز رخدادی که در پایین‌ترین سطح در مجموعه رخ می‌دهد و با نماد انتقال به بیرون مشخص می‌گردد. در بعضی از نمودارهای ترسیمی، نمادها برای رخدادهای تکراری اولیه یا سطوح بالاتر مشابه می‌باشد.

شکل ۶ نمونه‌ای از نمایش گرافیکی را نشان می‌دهد که در آن رخداد تکراری، نمایش داده شده با یک دروازه OR و شماره صفحه، در مکان دیگری از درخت خرابی پیدا می شود که آن رخداد ورودی مربوط به یک رخداد سطح بالای متمایز است. این رخداد می‌تواند در بیش از دو نقطه در درخت خرابی ظاهر شود. نمونه‌ای از این رخداد می‌تواند افزایش دما یا رطوبت باشد که عامل وقوع دو رخداد مختلف در یک سیستم می‌باشد. قطع اتصال در مورد چنین رخدادی به کار می‌رود در شکل ۶، همچنین یک دروازه انتقال وجود دارد تا نشان دهد که این رخداد در جایی دیگر یا صفحه‌ای دیگر از درخت خرابی ایجادشده است. این مورد معمولاً وقتی رخ می‌دهد که رخداد پیچیده‌تر به عنوان رخداد ورودی به یک رخداد سطح بالاتر وجود داشته باشد، در نتیجه لازم است که در یک صفحه جداگانه بیشتر توسعه یابد. یک دروازه AND اولویت دار که

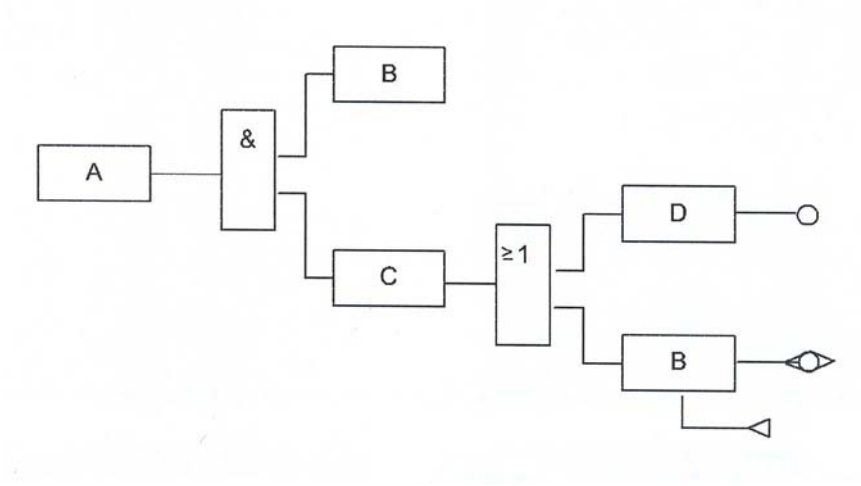
1 -Rule

درشکل ۶ نشان داده شده وقتی مورد استفاده قرار می‌گیرد که رخداد خروجی به ترتیب رخدادهای ورودی وابسته باشد.



شکل ۶ – مثال درخت خرابی شامل رخداد تکرار شده و انتقالی

شکل ۷ مثالی برای نمایش چند ضلعی درخت خرابی که رخداد تکرار شده انتقال به بیرون یا رخدادهای علت مشترک را نمایش می‌دهد. رخداد B که بیشتر از سایر رخدادهای درخت تحلیل می‌شود و رخداد D که یک رخداد اصلی است.



شکل ۷- مثالی برای نمایش علت مشترک در نمایش‌های دروازه مستطیلی

۷-۵-۳ روش اجرایی ساخت

مراحل اولیه ساخت یک درخت خرابی، تعریف روشن بالاترین رخداد، دامنه و هدف درخت خرابی، مرزهای سیستم یا هدف تحلیل و نتیجه تحلیل[1] می‌باشد. این هدف بایستی تحت عنوان بالاترین رخداد تعریف شود.

بالاترین رخداد باید مساله‌ای باشد را که باید تحلیل شود، توصیف کند تا علل موثر تعیین شود. در کاربرد FTA برای بهبود قابلیت اطمینان سیستم در حال تکوین، بالاترین رخداد، وقوع خرابی در سیستم است و هدف تحلیل تعیین عوامل موثر بر این رخداد و شناسایی ضعف یا اجزاء غیر قابل اطمینان طراحی می‌باشد. در تحلیل کمی، احتمال وقوع بالاترین رخداد و همه یا اکثر ورودی‌ها تعیین خواهد شد. در تحلیل کیفی، روشA، ورودی‌ها برای بالاتری رخداد مورد بررسی قرار می‌گیرد تا علل وقوع آن شناسایی شود. در تحلیل کمی، روش B، برای بهبود طراحی، ورودی‌های بالاترین رخداد تحلیل می‌شوند تا عوامل موثر اصلی بر بالاترین رخداد مشخص شده و طراحی با حذف سیستماتیک آن ضعف‌ها یا کاهش مُدهای خرابی مؤثر، بهبود یابد.

دامنه‌ی تحلیل رخدادها یا مُدهای وقوع خرابی‌ای را که در درخت خرابی گنجانده خواهد شد، تعریف می‌کند. این دامنه همچنین جزئیات مشکل تحت تحلیل، سطح بازنگری طراحی[2] سیستم تحت تحلیل و پروفایل استفاده شده از سیستم و سایر شرایط بهره برداری و محیطی را در بر می‌گیرد. در حالیکه مرزها موارد گنجانده شده و موارد حذف شده از سیستم را مشخص می‌کنند(مانند اتصالات داخلی، محفظه های مکانیکی و غیره).

درخت خرابی بایستی به گونه‌ای ساخته شود که روند رخدادهایی را که موجب وقوع بالاترین رخداد می‌شوند به وضوح نشان دهد.

بعد از این‌که بالاترین رخداد به وضوح تعریف شد و نیز مرزهای سیستم یا وسعت تحلیل مشخص گردید، آن‌گاه روند ساخت درخت خرابی از بالا به پایین جریان می یابد. بالاترین رخداد ورودی‌هایی دارد و ترکیب

1 -Resolution of analysis
2 -Design revision

آنها مدل‌سازی شده و با دروازه مناسب نشان داده می‌شود. ورودی‌های بالاترین رخداد بطور سیستماتیک ایجاد می‌شوند که باید حاصل رخدادهای ورودی خود باشند. هر یک از ورودی های رو به پایین در درخت خرابی به طور جداگانه ایجاد می شود و این توسعه هنگامی به انجام می رسد که به رخدادهای اولیه رسیده باشیم.

نتیجه مشخص می‌کند که تا چه حدی سیستم باید تحلیل شود. برای مثال یک سیستم الکترونیکی را می‌توان به سمت پایین تا اجزاء و مُدهای وقوع خرابی و علل آنها یا به سطح بالاتر از مجموعه‌های آن(مانند پردازنده سیگنال،تقویت کننده توان، تنظیم کننده ولتاژ ویژه و غیره) تجزیه کرد. گاهاً نتیجه می‌تواند ترکیبی از جزئیات و تحلیل‌های سطح مجموعه باشد که بستگی به آمادگی و احتمال وجود اطلاعات وارد.

تبعیت صریح از مفهوم« علت بی واسطه» لازم است تا اطمینان حاصل گردد که مُدهای وقوع خرابی در اثر فرض لحاظ آنها در مدهای قبلی حذف نشده اند.

مفهوم واحدهای اصلی[1] را می‌توان به کار برد تا تحلیل‌گر دیگر نیازی به ایجاد نمودارهای درخت خرابی که اطلاعات جدید و مفیدی به دست نمی‌دهند نداشته باشد. یک واحد اصلی بیشتر از این توسعه نمی‌یابد و با آن به گونه‌ای رفتار خواهد شد که یک واحد منفرد یا جزء جداگانه یا مقداری جداگانه است.

برای این‌که واحدی یا رخدادی، اولیه در نظرگرفته شود لازم و کافی است که سه شرط زیر رعایت شود:

- هم محدودیتهای وظیفه ای و هم مرزهای فیزیکی به وضوح تعریف شوند؛
- بهره برداری واحد مربوطه به وظیفه پشتیبانی وابسته نباشد یا همه رخدادهای وابسته به این واحد توسط یک دروازه OR واحد بیان شود که یک ورودی آن نمایانگر خرابی واحد ، و مابقی ورودیها نمایانگر ناتوانی در انجام وظایف پشتیبانی مربوطه باشد؛
- نتوان علت بی واسطه را برای وقوع رخداد تعیین کرد؛

توصیه می شود که واژه[2]های مورد استفاده در یک درخت خرابی استاندارد باشد تا ابهام به حداقل رسیده و نام‌گذاری و توضیح رخدادها به شیوه ای سازمان یافته، به وضوح انجام شود.

ساختار واقعی درخت خرابی از تحلیل منطقی روند رخدادها پیروی می کند.

- مفهوم علت بلاواسطه مستلزم این است که تحلیل‌گر علل آنی لازم و کافی برای وقوع بالاترین رخداد را تعیین کند. لازم به ذکر است که این ها علل اصلی برآمد نهایی یا بالاترین رخداد نیستند بلکه علل آنی یا مکانیسم‌های بلاواسطه برای وقوع بالاترین رخداد به شمار می‌آیند. این‌ها ممکن است رخدادهای سطح پایین(میانی) باشند.
- علل بلاواسطه لازم و کافی برای بالاترین رخداد اکنون به عنوان رخداد میانه در نظر گرفته شده و تحلیل تا تعیین علل آنی و کافی آنها (رخدادهای ورودی) ادامه می یابد و در نتیجه علل لازم و کافی آنها تعیین می‌شود.
- ساختار به پایین درخت پیش می رود و توجه از مکانیسم به مدها، منتقل می شود و به طور مستمر به سطح پایین تر از مکانیسم و مد می رسیم تا نهایتاً یک سطح مناسب و مشخص انفصال پذیری حاصل شود

1 -Basic units
2 -Nomenclature

.رخدادهای اصلی منحصر بفرد یا رخداد اولیه (تحتانی) آنهایی هستند که شاخص علل منحصر بفرد خرابی‌های بالقوه یا خرابی هستند.

۷-۵-۴ پایش درخت خرابی

۷-۵-۴-۱ بررسی و تحلیل

تحقیق و بررسی شامل مروری بازنگری ساختار درخت خرابی در مقایسه با اطلاعات موجود از قبیل شماها[1]، نقشه‌ها، نمودارهای وظیفه‌ای، دستورات نرم‌افزاری، شناسایی رخدادهای مشترک و جستجو برای شاخه‌های مستقل است. در بررسی، بایستی رخدادهای علل مشترک شناسایی شوند، اما نبایستی فرض کنیم که وجود حضور آنها خوش خیم[2] است. این نتیجه‌گیری‌ها را می‌توان تنها بعد از تحلیل کامل با استفاده از کاهش بولی یا تعیین مجموعه قطعی مینیمال در صورت وجود دروازه‌های استاتیک بدست آورد زیرا مجموعه قطعی مینیمال در دروازه‌های دینامیک وجود ندارند مگر این‌که از برآورد نادیده گرفتن توالی استفاده شود. همچنان که دشواری تحلیل نسبت به اندازه درخت خرابی به سرعت افزایش می‌یابد، به تحلیل‌گر اجازه می‌دهد ضمن بازرسی درخت خرابی، شاخه‌های مستقل درخت را شناسایی کرده و بدین ترتیب در صورت نیاز، به صورت مستقل مورد تحلیل قرار دهد.

تحلیل درخت خرابی به دنبال روند رخدادها انجام گرفته و علل این دسته از رخدادها را در جهت پایین شناسایی می‌کند. ارزیابی درخت خرابی ممکن است منطقی(کیفی) یا عددی (کمی) یا هر دو باشد. تحلیل کمی درخت خرابی که برای بهبود قابلیت اطمینان در تکوین محصول به‌کار می رود، عوامل با سطح بالای مؤثر بر احتمال وقوع بالاترین رخداد و علت‌های با احتمال وقوع زیاد را شناسایی می‌کند. به عنوان مثال، اگر احتمال وقوع خرابی یک مجموعه از یک سیستم، عامل اصلی احتمال وقوع خرابی سیستم باشد علت آن بررسی شده و بعد از شناسایی، این مُد وقوع خرابی را می‌توان کاهش داد. برای توضیح بیشتر این مساله یک عامل مهم برای احتمال وقوع خرابی منبع تغذیه یک سیستم را می‌توان یک خازن تحت اضافه تنش (بار) شناسایی کرد تعویض این خازن با یک خازن دیگر با مقادیر اسمی ولتاژ بالاتر تا حد زیادی احتمال وقوع خرابی مجموعه و در نتیجه سیستم را کاهش می‌دهد.

توصیه می‌شود که تحلیل‌ها به‌گونه‌ای مستند شوند که نتایج را بتوان مورد بررسی قرار داده و هر گونه تغییر لازم را انجام داد تا بتوان این تغییرات را، در طراحی، روش اجرایی بهره برداری یا افزایش آگاهی از فیزیک وقوع خرابی بازخور داد. برای انجام این کار، به رویکرد سیستماتیکی برای ساختار نیاز می‌باشد. برای اجرای این رویکرد سیستماتیک لازم است دو مفهوم درک شده و بطور سازگار مورد استفاده قرار گیرد. این فرضیه‌ها عبارتند از :«علت بلاواسطه» (رخدادهای ورودی) و «واحد اصلی».

اهداف اصلی تحلیل‌های منطقی(کیفی) و عددی(کمی) یک سیستم را می‌توان به صورت زیر خلاصه کرد:

- شناسایی رخدادها یا خرابی‌هایی که به طور مستقیم می‌توانند وقوع خرابی یک سیستم را موجب شوند و به احتمال این‌گونه رخدادها کمک می‌کنند و به این ترتیب قابلیت اعتماد سیستم را بهبود بخشید؛

---

1 -Schematics
2 -Benign

- کاهش خرابی های موثر در برآمد نهایی که می‌توانند به‌صورت بالقوه خطرات ایمنی داشته باشند؛
- ارزیابی تحمل خرابی سیستم (قابلیت انجام وظیفه حتی بعد از تعداد مشخصی از خرابی‌های سطح پایین یا رخدادهای مؤثر بر خرابی‌های سیستم که وقوع یافته باشند)؛
- ارزیابی اطلاعات برای مکان‌یابی محل اجزا بحرانی و مکانیسم‌های وقوع خرابی؛
- شناسایی تشخیص های وقوع خرابی ابزار، ورودی‌های استراتژی‌های تعمیر و نگهداری و غیره؛
- ارزیابی تحمل خرابی سیستم شامل تعیین میزان ردوندانسی در سیستم و تایید این مساله که ردوندانسی از طریق رخداد مشترک مختل شده است. گرچه بخش اصلی ارزیابی تحمل خرابی نیازی به استفاده از داده‌های عددی ندارد اما این داده‌ها برای ارزیابی این‌که کدام ترکیب رخدادها عامل وقوع خرابی سیستم، بیشتر احتمال وقوع دارند، لازم و ضروری است.

۷-۵-۴-۲ تحلیل منطقی

۷-۵-۴-۲-۱ کلیات

از سه فن اصلی برای تحلیل منطقی استفاده می‌شود: تحقیق، کاهش بولی و تعیین مجموعه قطعی مینیمال. اساس تحلیل منطقی مدل‌سازی است که نمایش درخت خرابی ساختار را فراهم می کند خواه این نمایش، وظیفه‌ای، ساختاری یا مخلوطی از هر دو، باشد مدل‌سازی صحیح به مفهوم نمایش وظیفه‌ها یا اجزای یک سیستم به شیوه‌ای است که تعاملات، وابستگی‌ها، علل بلاواسطه برآمدهای نامطلوب و غیره را مشخص کند.

۷-۵-۴-۲-۲ کاهش بولی

کاهش بولی را می‌توان برای ارزیابی تاثیرات رخدادهای مشترک در درخت خرابی به‌کار برد (وقوع رخدادهای یکسان در شاخه‌های مختلف) که در آن وقوع بالاترین رخداد بستگی به زمان‌بندی یا توالی رخدادها ندارد. کاهش بولی را می‌توان با حل معادلات بولی برای درخت خرابی انجام داد. کاهش بولی را نیز می‌توان جهت شناسایی مجموعه های برشی مینیمال به‌کار برد.

۷-۵-۴-۲-۳ شناسایی مجموعه های قطعی کننده مینیمال

چندین روش برای تعیین مجموعه قطعی کننده مینیمال وجود دارد اما استفاده از درخت‌های بزرگتر ممکن است دشوار و ناقص باشد. به همین دلیل برنامه‌های کامپیوتری متفاوتی برای کمک به تحلیل‌گر وجود دارد.
یک مجموعه قطعی مینیمال ، کوچکترین گروهی از رخدادها است که وقتی با همدیگر واقع می‌شوند، علت وقوع بالاترین رخداد می‌شوند. اگر هر یک از رخدادها در یک مجموعه قطعی کننده مینیمال رخ ندهد آنگاه بالاترین رخداد رخ هم نخواهد داد. این تعریف را می‌توان بسته به توالی رخدادها به درخت‌های خرابی بسط داد. در این گونه موارد، مجموعه قطعی کننده مینیمال، گروه رخدادهای بالقوه را که علت وقوع بالاترین رخداد می‌شوند تعیین می‌کند. هنگامی که وقوع بالاترین رخداد بستگی به توالی رخدادهای ورودی داشته باشد، این رخداد با استفاده از فنون مارکوف که در استاندارد ملی شماره ۱۱۷۴۸ توصیف شده‌اند تحلیل می‌شود.

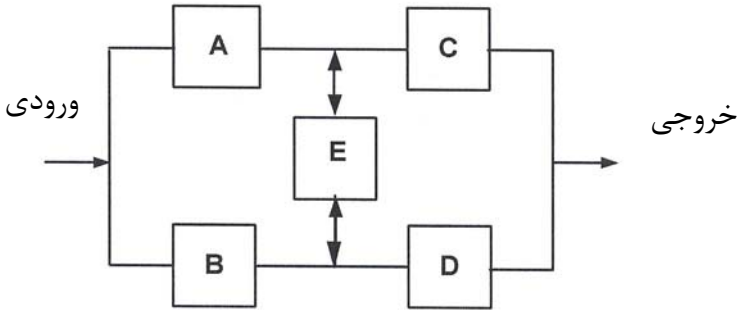
۳-۴-۵-۷ تحلیل عددی

هدف از تحلیل عددی، انجام پایش کمی احتمال وقوع بالاترین رخداد یا مجموعه انتخابی از رخدادهاست. این تحلیل عددی همچنین می‌تواند برای پشتیبانی و تکمیل تحلیل منطقی به‌کار رود. برای انجام ارزیابی عددی درخت خرابی، به داده‌ای احتمالی درسطح اجزاء نیاز است. روش‌های پیش‌بینی قابلیت اطمینان و آمادگی، آزمایش واقعی یا داده‌های میدانی را می‌توان برای تعیین مقادیر کمی مورد استفاده قرار داد.

۵-۵-۷ مثالهایی برای ارزیابی سخت‌افزار ساده مورد استفاده در جبر بولی و نمایش آن با درخت خرابی

۱-۵-۵-۷ مثال مدار پل

درخت خرابی با جبر بولی می‌تواند تحلیل قابلیت اطمینان را ساده کند. همانطور که در این مثال نشان داده شده است، عبارات ریاضی بسیار پیچیده باید نوشته شود. چنانچه تحلیل با استفاده از نمودار بلوک قابلیت اطمینان انجام گرفته باشد، جای خود را به جبر ساده‌تر بولی می‌دهد. بدیهی است که استفاده از FTA به‌ویژه برای مدارهای پیچیده‌تر که در آن وابستگی درونی نرم‌افزاری و سخت‌افزاری و تحلیل با استفاده از یکی از انواع بسته های نرم‌افزاری موجود انجام می‌شود ساده می‌باشد.
نمونه‌ای از کاربرد تحلیل درخت خرابی برای نمایش مدار پل در شکل ۸ نشان داده است.



یادآوری- به شکل‌های ۱۱ و ۱۲ برای مدل سازی درخت های خرابی معادل مراجعه کنید

شکل ۸- مثال مدار پل، تحلیل شده توسط درخت خرابی

در مدار پل فوق، سیگنال باید از ورودی به خروجی جریان یابد. سیگنال می‌تواند از بلوک E در هر دو مسیر جریان یابد. یک روش برای انجام تحلیل، مدل‌سازی سیستم تحت دو موقعیت احتمالی است. ابتدا فرض این‌که بلوک E مناسب باشد و دوم این‌که بلوک E نامناسب باشد. در مورد اول، سیگنال از طریق بلوک‌های A یا B و C یا D جریان می‌یابد مثل این‌که بلوکها موازی هستند. بر عکس وقتی که بلوک E نامناسب است(شرایط وقوع خرابی در بلوک E) بلوک‌های سری A و C با بلوک‌های سری B و D موازی هستند. این مساله با فرمول زیر نمایش داده می‌شود:

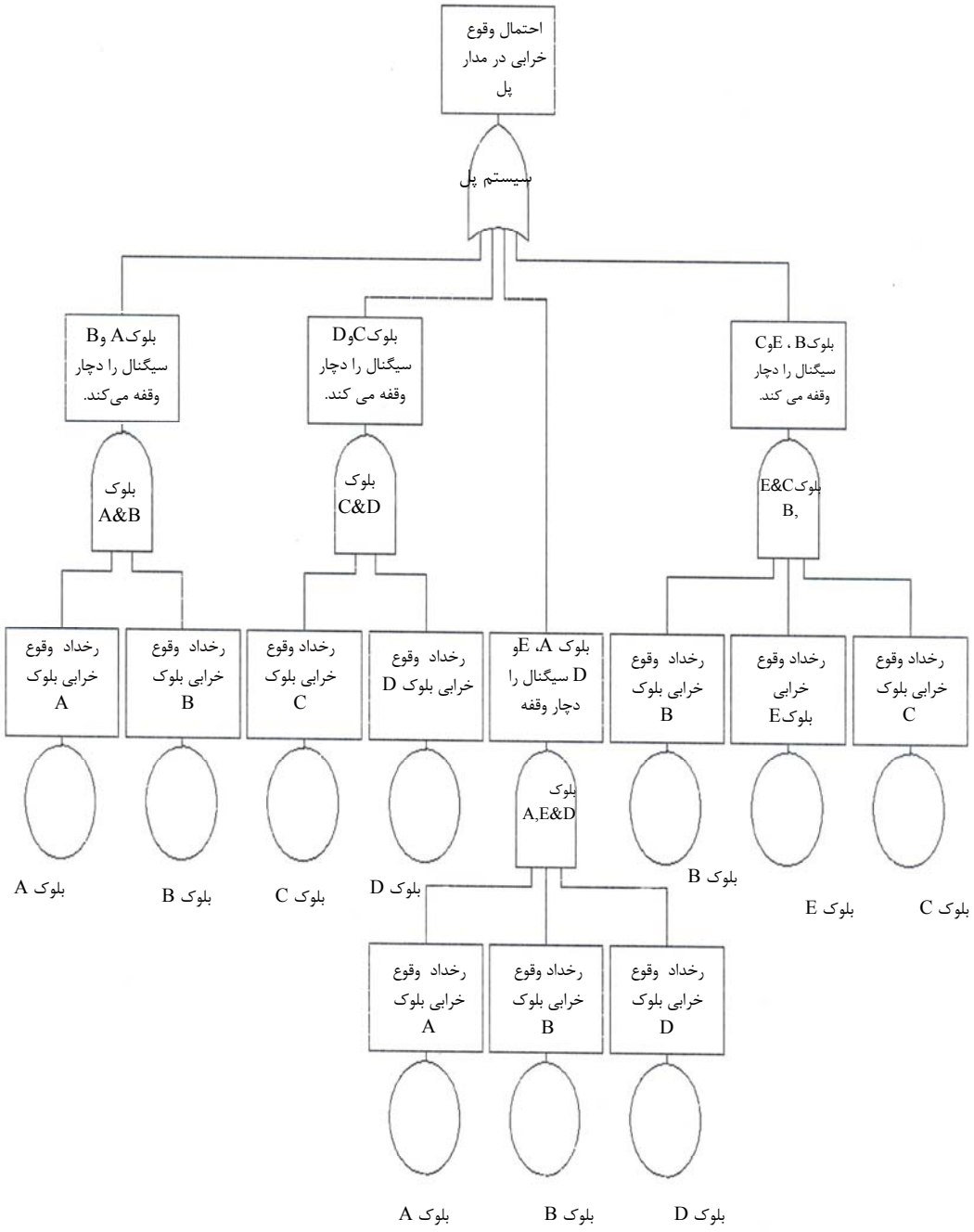
$$R_S = (R_A + R_B - R_A.R_B).(R_C + R_D - R_C.R_D).R_E + (R_A.R_C + R_B.R_D - R_A.R_B.R_C.R_D).(1 - R_E) \qquad (۷)$$

اگر $R_A=0.78; R_B=0.3; R_C=0.15; R_D=0.5; R_E=0.4$

بنابر این $RS=0.344$

و احتمال وقوع خرابی بدست می‌آید : $F_S=0.656$

نمایش درخت خرابی (سیستم) مدار پل در شکل ۹ نشان داده شده است.



شکل ۹- نمایش درخت خرابی در مدار پل

با استفاده از جبر بولی و مجموعه قطعی مینیمال سیستم موجود در شکل ۹ طبق زیر خواهد بود (مسیرهایی که برای بهره برداری سیستم آماده می‌کند)

مجموعه قطعی در این سیستم از ترکیبات رخدادهای مربوط به سیگنال بلوک‌های زیر ساخته می‌شوند:

بلوک‌های A و B($c1=FaFb=ab$)

بلوک‌های C و D ($c_2=cd$)

بلوک‌های A و E و D ($c_3=aed$)

بلوک‌های B و E و D ($c_4=bec$)

در صورت وقوع خرابی هر یک از ترکیبات فوق، جریان سیگنال از ورودی تا خروجی قطع خواهد شد.

با جبر بولی، احتمال وقوع خرابی سیستم چنین خواهد بود:

$$F_s=pr(c_1\cup c_2\cup c_3\cup c_4) \qquad (۸)$$

احتمالات مجموعه قطعی عبارتند از:

$$\begin{aligned} Pr\,(c_1) &= F_A.F_B= (1-R_A).\,(1-R_B)\\ Pr\,(c_2) &= F_C.F_D= (1-R_C).\,(1-R_D)\\ Pr(c_3) &= F_A.F_E.F_D=(1-R_A).(1-R_E).\,(1-R_D) \qquad (۹)\\ Pr\,(c_4) &= F_B.F_E.F_C= (1-R_B).\,(1-R_E).\,(1-R_C) \end{aligned}$$

مثال ساده فوق دارای احتمال معین تعداد زیادی خرابی عمدی است تا صحت بعضی روش‌های درخت خرابی یا روش های محاسبات جبری بولی را نشان داده و خرابی هایی که ممکن است در سایر روش های محاسباتی رخ دهد را مشخص کند. این خرابی ها ممکن است در درخت‌های خرابی بزرگی رخ دهد که برای سیستم‌ها آماده شده حتی اگر احتمالات وقوع رخداد اولیه یا اساسی بسیار ناچیز باشد. احتمال وقوع رخداها در این درخت‌های بزرگ خرابی به سطوح بالاتر رسیده به‌طوری‌که رخدادهای ورودی دربالاترین رخداد از احتمال زیادی برای خرابی برخوردار بوده، و منجر به نتایج نادرست در برآورد احتمال وقوع بالاترین رخداد می‌گردد

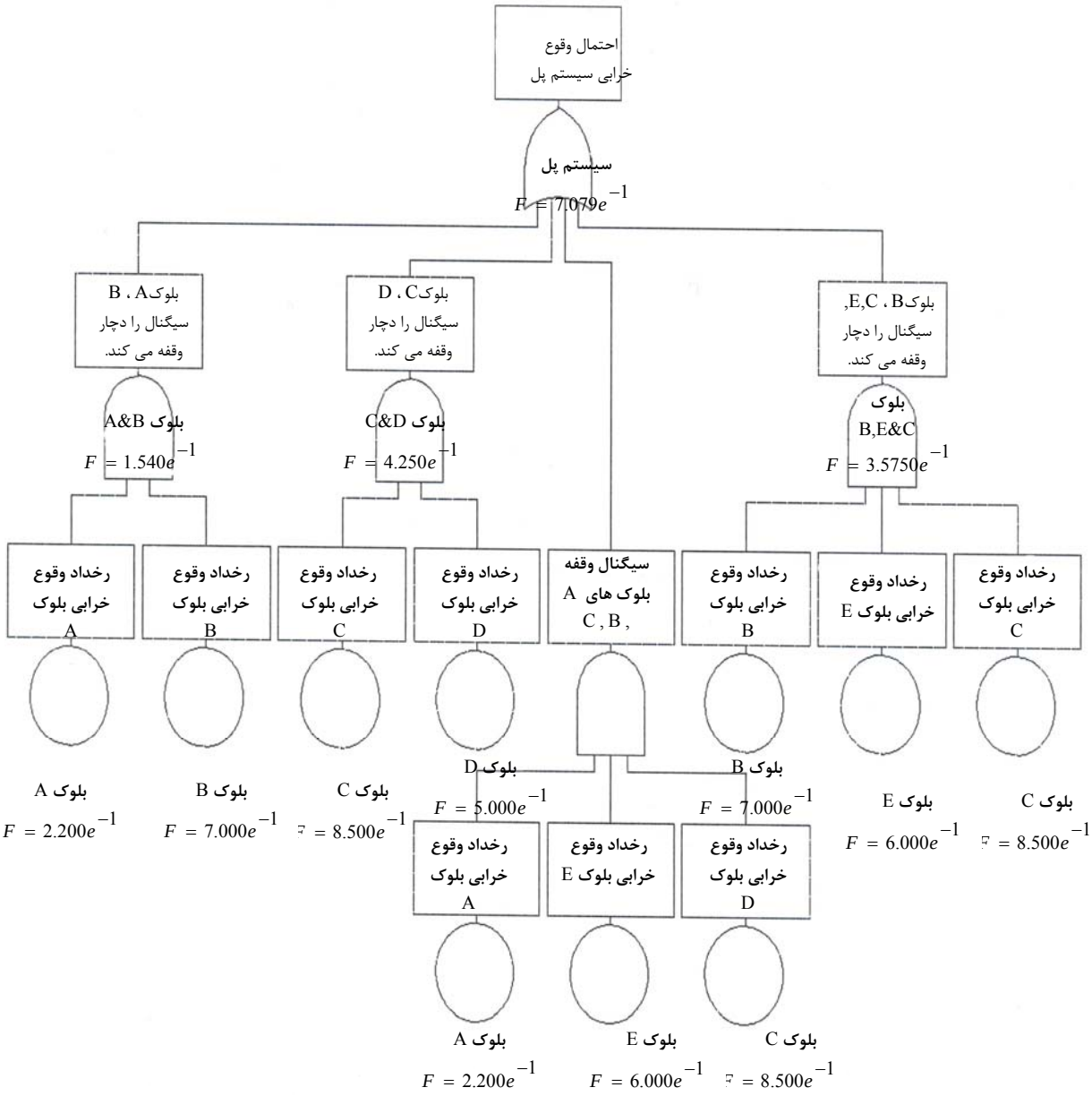
۷-۵-۵-۲ روش اساری – پروشان[1]

بدون در نظر گرفتن شاخه مشترک که توصیه نمی شود بیش از یکبار در محاسبات در نظر گرفته شود، احتمال وقوع خرابی (بدون انفصال) مطابق معادلات اساری- پروشان طبق زیر خواهد بود

$$\begin{aligned} F_{S\text{-}EP} &= Pr\,(c_1\cup c_2\cup c_3\cup c_4) =\\ &1-[1-pr(c_1)].[1-pr\,(c_2)].\,[1-pr\,(c_3)].\,[1-pr\,(c_4)] \qquad (۱۰)\\ F_{S\text{-}EP} &= 0.7079\\ R_{S\text{-}EP} &= 0.2921 \end{aligned}$$

محاسبات فوق توسط درخت خرابی در شکل ۱۰ نشان داده‌شده که درآن از گزینه انفصال استفاده نشده است.

1 -Esary-Proschan method



یادآوری – این محاسبات کاملاً صحیح نیستند

شکل ۱۰ – FTA سیستم پل روش اساری – پروشان، بدون انفصال

۳-۵-۵-۷ محاسبه رخداد نادر

تقریب رخداد نادر، همه احتمالات همزمانی وقوع مجموعه قطعی را نادیده می‌گیرد. با تقریب رخداد نادر، این محاسبات(مجدداً بدون انفصال) وقوع خرابی و قابلیت اطمینان سیستم مشابه با افزودن یک احتمال ساده خواهد بود:

$$FS\text{-}RA=pr\,(c1) + pr\,(c2) + pr\,(c3) + pr\,(c4)$$

$$F_{S\text{-}RA}= F_A.F_{B+}\, F_C.F_{D+}\, F_A.F_E.F_{D+}\, F_B.F_E.F_C$$

$$F_{S\text{-}RA}=1.002 \qquad (۱۱)$$

$$R_{S\text{-}RA}=-2.10^{-3}$$

در حالیکه انجام آن کار ساده‌ای است اما برآورد رخداد نادر ممکن است خرابی های بزرگی را در محاسبات بوجود آورد، هنگامی که دارای اعداد بزرگتری مانند آنچه در مثال بالا دیده می شود، هستند. (به احتمال وقوع خرابی بیشتر از واحد توجه کنید).

برآورد نادر که با FTA محاسبه و نمایش داده شده در شکل ۱۱ ارائه شده است.

همانطور که در شکل ۱۱ مشاهده می‌شود، وقتی احتمال وقوع خرابی رخدادهای ورودی اعداد نسبتا بزرگی باشد که اغلب در مورد رخدادهای ورودی به سمت بالاترین رخداد از یک سیستم بزرگ است، ممکن است منجر به یک خرابی جدی سیستم در محاسبه شود.(توجه کنید که احتمال وقوع بالاترین رخداد به غلط بیشتر از ۱ اعلام شده است).

۴-۵-۵-۷ انفصال[1]

انفصال یک سری اعمال جبری جهت تضمین این مساله می‌باشد که شاخه مشترک (یا خرابی علت مشترک) در محاسبات بطور مکرر به حساب نیاید. چندین روش برای انفصال وجود دارد: جبری، مراحل چندگانه که در آن با وجود عبارات چند گانه در محاسبات، عبارات از عبارات قبلی جدا می‌شوند، مدل ضریب بتا، مدل ضریب آلفا، مدل حروف یونانی چندگانه، و غیره. همه موارد فوق جز مورد اول برای محاسبه خرابی‌های علت مشترک مورد استفاده قرار می‌گیرد.

در پیوست ب در خصوص انفصال به تفصیل بحث و بررسی شده است.

لازم به ذکر است که روندهای انفصال را می‌توان به عنوان یک برنامه کامپیوتری نوشت. با استفاده از چنین برنامه‌ای، عبارات بسیار دشوار بولی را می‌توان منفصل کرد. این کاربرد قابلیت اطمینان بدون تمرکز بر روی عبارات صحیح به دست آمده برای موفقیت سیستم (یا وقوع خرابی سیستم) در نظر نمی گیرد. یکنواختی تبدیل عبارات بولی به یک عبارت احتمال قابلیت اطمینان بر عهده کامپیوتر گذاشته می‌شود.

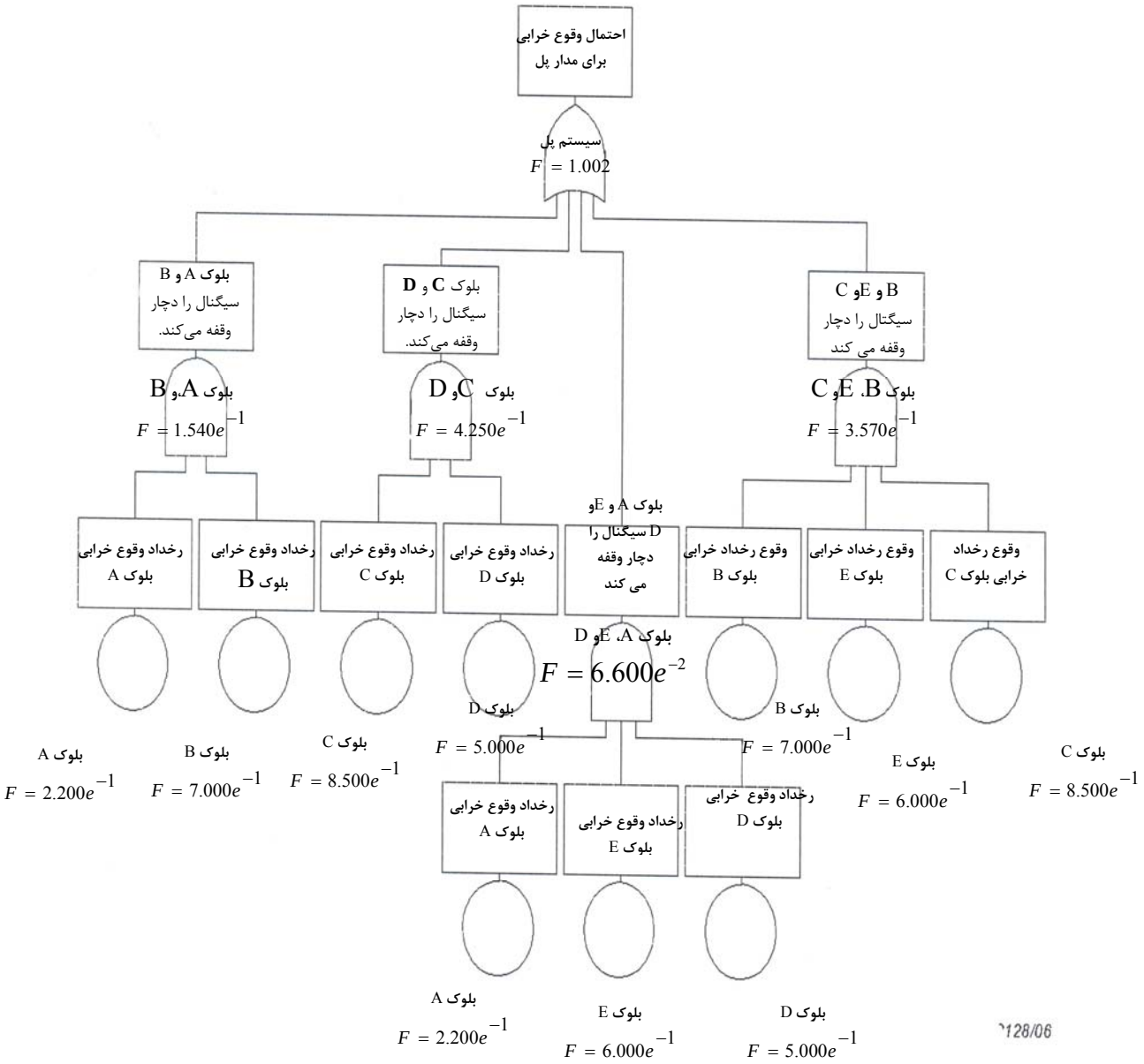
به عبارت دیگر، رویکردی که از برهان احتمال استفاده می‌کند کارآیی فوق العاده‌ای برای این نمونه دارد، اما در بسیاری موارد به‌ویژه وقتی که RBD نامتقارن است بسیار پیچیده و دشوار می‌گردد.

بسیاری از بسته‌های نرم افزاری تجاری موجود در FTA حاوی گزینه‌ای برای انفصال می‌باشند. شکل ۱۳ محاسبات را هنگام امکان انفصال نشان می‌دهد. این شکل بدون توجه به هر گونه نرم‌افزار ویژه‌ای ترسیم شده است زیرا این استاندارد از توصیه‌ها یا اولویت‌های نرم‌افزاری اجتناب می‌کند. این مسایل بر عهده کاربران با نیازهای خاص آنان گذاشته می‌شود.

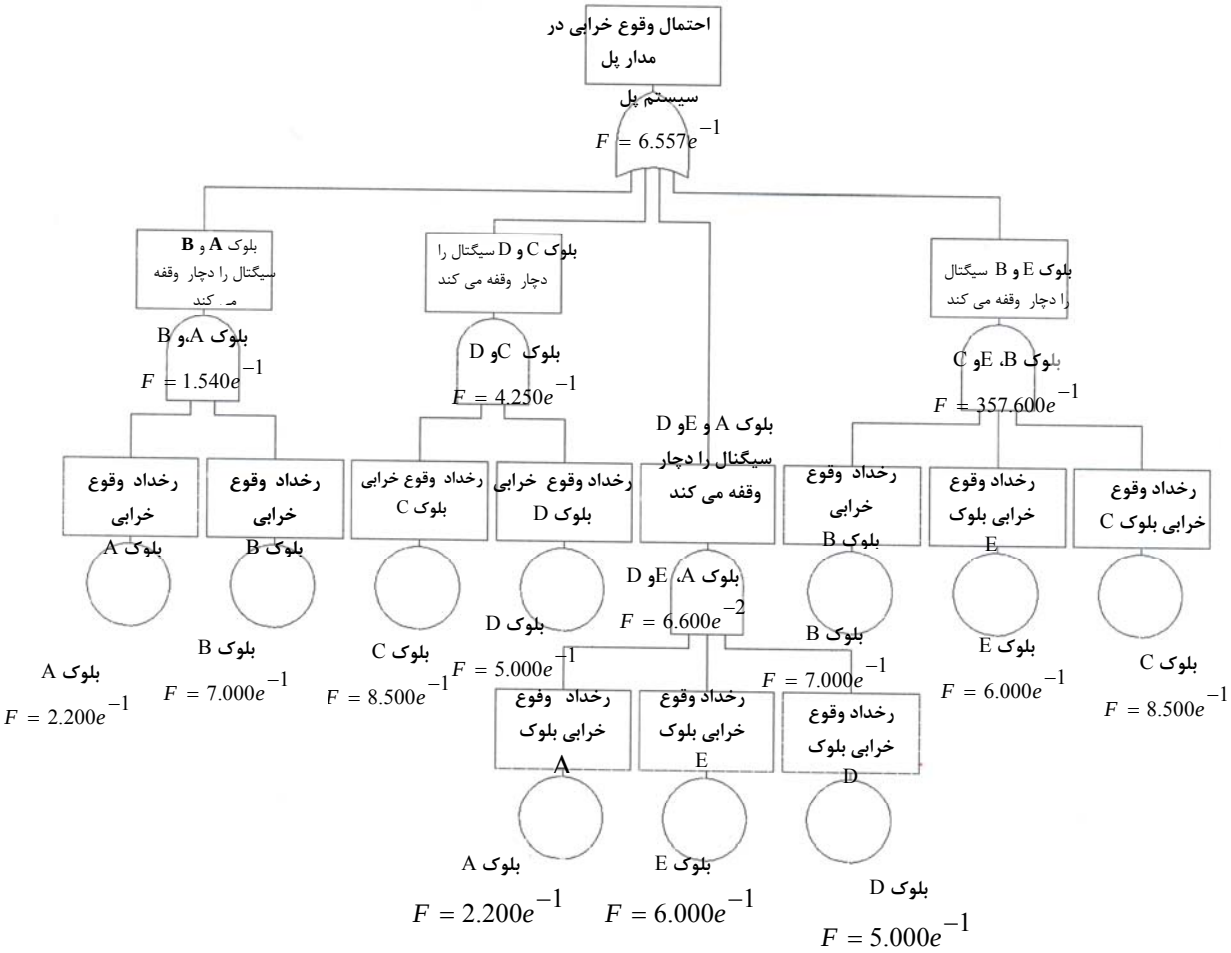
در شکل ۱۲ برای قابلیت اطمینان سیستم یا مکمل، احتمال وقوع بالاترین رخداد مانند مورد محاسبه شده، با استفاده از معادله اول مدل‌سازی قابلیت اطمینان می‌باشد. در اشکال ۱۰، ۱۱و ۱۲ نماد F برای احتمال وقوع خرابی یک سیستم غیر قابل تعمیر به‌کار می‌رود.

---

1 -Disjoining



شکل ۱۱- احتمال سیستم پل با محاسبه وقوع خرابی با استفاده برآورد رخداد نادر



یادآوری- محاسبات کاملاً صحیح هستند

شکل ۱۲- احتمال وقوع رخداد نهایی با انفصال

۶-۷ نرخ وقوع خرابی در تحلیل درخت خرابی

در بسیاری موارد، در تحلیل درخت خرابی می‌توان از نرخ وقوع خرابی به جای احتمال های وقوع خرابی رخدادها استفاده کرد. در این خصوص، فرض بر این است که توزیع پواسون برای تعیین وقوع رخدادها به کار رفته و این‌که نرخ وقوع خرابی مربوطه ثابت می‌باشد. جبر مورد استفاده در این مورد مربوط به مدل‌سازی معمول قابلیت اطمینان است و الگوریتم‌های مورد استفاده برای محاسبه نرخ وقوع خرابی رخدادهای خروجی با مدل‌سازی نمودار بلوک قابلیت اطمینان یکسان است. نتیجه بالاترین رخداد حاصل نیز با نرخ وقوع خرابی آن نمایش داده می‌شود.

همچنین می‌توان درخت خرابی را با ترکیبی از نرخ وقوع خرابی و احتمال‌های وقوع خرابی مختص به رخدادهای مختلف، ساخت. راحت‌ترین روش برای تحلیل این نوع درخت خرابی، تبدیل نرخ وقوع خرابی به احتمال مورد قبول و تهیه اصول استاندارد تحلیل خرابی می‌باشد. بعضی نرم‌افزارها اطلاعات ترکیبی رخدادها را پذیرفته و از الگوریتم‌های مناسب برای ارائه احتمال یا نرخ وقوع خرابی بالاترین رخداد استفاده می‌کند. در این رابطه، سایر اطلاعات مورد نیاز عبارت است از بازه زمانی برای احتمال وقوع خرابی‌های مورد ملاحظه قرار می گیرد.

استفاده گسترده ازFTA برای تحلیل سیستم‌های قابل تعمیر موضوعی جداگانه و خارج از این استاندارد می‌باشد.

۸ شناسایی و نامگذاری در درخت خرابی

هر رخداد در درخت خرابی باید بطور انحصاری تعریف گردد. توصیه می شود که رخدادها به گونه‌ای نامگذاری شوند که مراجعه متقابل از درخت خرابی به اسناد طراحی مربوطه به‌راحتی انجام گیرد.
بالاترین رخداد از درخت خرابی یک برآمد نامطلوب است که علت اولیه برای تحلیل های درخت خرابی می‌باشد. لازم به یادآوری است که فقط بالاترین رخداد واحد می‌تواند وابسته به درخت خرابی مفروض باشد.
اگر چندین رخداد در یک درخت خرابی همه به مُدهای وقوع خرابی در یک زمان اشاره داشته باشند آنگاه این گونه رخدادها باید به‌گونه‌ای نامگذاری کرد که تشخیص آنها امکان‌پذیر باشد. در عین حال بهتر است مشخص گردد که آنها یک گروه از رخدادهای مرتبط با یک قلم یکسان هستند. اکثر بسته‌های نرم‌افزاری برای FTA به تحلیل‌گر این امکان را نمی‌دهد که دو رخداد ورودی را با یک نام، نامگذاری کند، در نتیجه تحلیل‌گر را مجبور می‌کنند آگاهانه یک نام مشابه را برای رخدادهای تکراری، رخدادهای علت مشترک تعیین کند.
اگر یک رخداد خاص مانند ناتوانی یک دریچه خاص جهت بسته شدن در چندین نقطه در درخت رخ دهد یا اگر در چندین درخت اتفاق افتد، همه این اتفاقات باید نام مشترک داشته باشند. (در استفاده نرم افزاری، برای رخدادهای ورودی یکسان با نام های مخصوص برای مکانها مختلف در درخت خرابی اضافه خواهد شد).
با این وجود، رخدادهایی که مشابه هستند اما شامل چندین قلم مختلف می‌باشند نباید یک معرف مشابه داشته باشند. یک کد رخداد نوعی بهتر است حاوی اطلاعاتی در خصوص شناسایی زیر سیستم ، برای شناسایی یک جزء و مُد وقوع خرابی آن باشد. (دومین بند زیر).
نمونه‌هایی از تحلیل مدار الکترونیکی به قرار زیر است:
Short-C132 به این معنی است که وضعیت خرابی خازن C132 اتصال کوتاه می‌باشد.
Short-A – C135 که در آن حرف A برای همه اجزای زیر سیستم آنالوگ، در مواردی به‌کار می‌رود که تکرار اسامی مرجع در سایر زیر سیستم‌های وجود داشته باشد (مانندیک C135 که در زیر سیستم پردازش وجود دارد)
OPEN-R34 وضعیت خرابی مقاومت R34، مدار باز می‌باشد.
LOW OUT PUT –U2 یعنی این که وضعیت خرابی مدار یکپارچه، سطح پایین خروجی است.
یک مجموعه تکمیلی از عناوین یا اسامی خاص رخدادها را می‌توان در صورت لزوم بوجود آورد. با این وجود، تحلیل‌گر لازم است که این عناوین و اسامی مورد استفاده را تعریف و گزارش کند و استفاده هماهنگ و پایدار در سر تا سر یک تحلیل درخت خرابی را تضمین کند. این مساله به ویژه اگر از روش‌های کامپیوتری استفاده شود، صادق است.
سازگاری در نامگذاری حتی وقتی اهمیت بیشتری می‌یابد که نرم‌افزار تحلیل درخت خرابی، ورود مقادیر برای احتمال رخدادهای اولیه یا اصلی را امکان‌پذیر سازد که در یک صفحه گسترده مبتنی بر فهرست مواد،

اجزاء، مُد های وقوع خرابی اجزاء و پروفایل کاربرد آنها محاسبه شده باشند. این موضوع می‌تواند وقتی مطرح گردد که تحلیل بر روی یک سیستم پیچیده انجام می‌گیرد. در این مورد، عناوین و اسامی برای رخداد اصلی و اولیه در هر دو فایل ممکن است یکسان باشند(صفحه گسترده و تحلیل درخت خرابی)به طوری که تطابق اسمی و مقادیر احتمال وقوع را به رخدادهای مربوطه امکان‌پذیر سازد.

۹ گزارش

گزارش تحلیل درخت خرابی باید حاوی حداقل قلم‌های اصلی فهرست شده در زیر باشد. اطلاعات تکمیلی و اضافی را می‌توان جهت شفافیت بیشتر به‌ویژه در موارد مربوط به تحلیل‌های سیستم‌های پیچیده ارائه کرده این استاندارد هیچ قالب خامی را توصیه نمی‌کند.

قلم‌های اصلی در گزارش باید طبق زیر باشد:

- هدف و دامنه کاربرد؛
- توصیف سیستم: توصیف طراحی،بهره برداری سیستم، تعاریف جزئیات مرزهای سیستم؛
- مفروضات: مفروضات طراحی سیستم؛
- بهره برداری، نگهداری، مفروضات بازرسی و آزمون، مفروضات مدل‌سازی قابلیت اطمینان و آمادگی؛
- تحلیل تیم/ شخص با سابقه و تخصص مرتبط که در عنوان یا بخش جداگانه‌ای از گزارش اظهار شده است: تعاریف و معیارهای بالاترین رخداد ؛
- مرجع‌ها برای رخداد اصلی، رخدادهای توسعه نیافته و رخدادهایی که در جایی دیگر تحلیل شده اند مثلاً در پروژه‌های مختلف و توجیه استفاده از احتمالات آنها (مثلا تنش‌های یکسان و پروفیل‌کاربرد یکسان و غیره)؛
- تحلیل درخت خرابی: تحلیل داده‌ها، نمادهای مورد استفاه، وقوع خرابی‌های علت مشترک، مکان مناسب، وجود مجموعه قطعی مینیمال، مکان مناسب
- نتایج، نتایج نهایی و توصیه‌ها

قلم‌های داده‌های مکمل که می‌تواند گنجانده شود عبارتند از :

- نمودارهای بلوک یا دیاگرام مدار
- خلاصه داده‌های و منابع قابلیت اطمینان و قابلیت نگهداری مانند بانک‌های اطلاعاتی، اطلاعات حاصل از تولیدکنندگان اجزاء، اطلاعات دسته بندی شده و غیره
-تحلیل FMEA/FMECA یا رجوع به تحلیلها.

جدول FMEA می‌تواند یک روش مفید برای ارائه یک مساله، پیشنهادات برای بهبود طراحی، پیشنهادات برای تایید و اطلاع یک مساله، مانند یک آزمون و برای ادامه در این فعالیت‌ها می‌باشد.

پیوست الف

(اطلاعاتی)

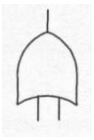
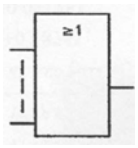
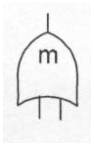
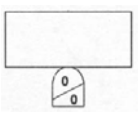
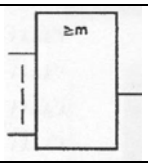
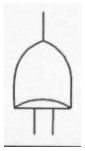
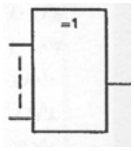
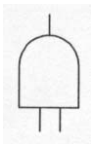
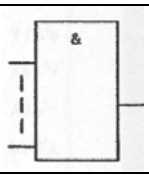
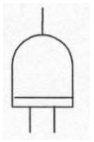
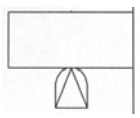
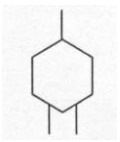
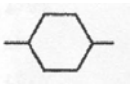
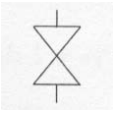
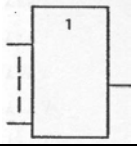
نمادها

نمادهای ارائه شده در جدول الف-۱ عموما مورد استفاده قرار می‌گیرند

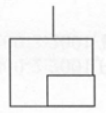
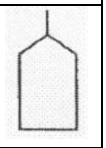
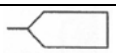
جدول الف-۱ نمادهای معمول بکار رفته در درخت خرابی

	نماد		نام	توصیف	همبستگی قابلیت اطمینان	تعداد ورودی‌ها
			رخداد اصلی	رخداد پایین ترین سطح که برای آن احتمال وقوع یا اطلاعات قابلیت اطمینان موجود است	مُد وقوع خرابی جز یا علت وقوع خرابی	۰
			رخداد مشروط	رخدادی که شرط وقوع یک رخداد دیگر باشد آنگاه که هر دو باید رخ دهند تا خروجی رخ دهد	وقوع رخدادی که باید وقوع یابد تا رخداد دیگری رخ دهد–احتمال مشروط	۰
			رخداد خاموش	رخداد اولیه که معرف یک وقوع خرابی خاموش می‌باشد رخدادی که بلافاصله شناسایی نمی‌شود بلکه احتمالا توسط بازرسی یا تحلیل مضاعف شناسایی شود	مُد وقوع خرابی خاموش جز یا علت وقوع خرابی خاموش	۰
			رخداد توسعه نیافته	یک رخداد اولیه که معرف بخشی از سیستم می‌باشد که هنوز توسعه نیافته است	یک عامل موثر در احتمال وقوع خرابی ساختار آن بخش از سیستم هنوز تعریف نشده است	۰
		انتقال به خارج OUT انتقال به داخل IN	دروازه انتقال	دروازه که نشان می‌دهد این بخش از سیستم در بخش دیگری یا صفحه‌ای دیگر از نمودار ایجاد شده است	نمودار درخت خرابی جزیی که در نقطه‌ای دیگر از سیستم نشان داده شده است. این معنی که دروازه توسعه یافته در این نقطه در جایی دیگر هم استفاده می‌شود IN به این معنی است که دروازه توسعه یافته در جایی دیگر است OUT به این معنی است که همین دروازه توسعه یافته در این مکان، در جای دیگری هم استفاده می‌شود	۰

جدول الف-۱ (ادامه)

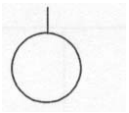
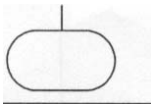
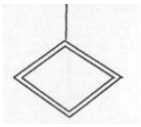
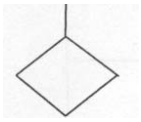
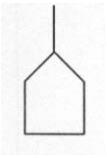
	نماد		نام	توصیف	همبستگی قابلیت اطمینان	تعداد ورودی‌ها
			دروازه **OR**	رخداد خروجی در صورتی رخ می‌دهد که یکی از رخدادهای ورودی رخ دهد	خرابی رخ می دهد که هر یک از بخش‌های این سیستم خراب باشند سیستم سری	≥۲
			دروازه اکثریت	خروجی رخ می‌دهد اگر **M** یا ورودیهای بیشتری از کل ورودیهای **n** رخ می‌دهد	ردوندانسی **k** از **n** که در آن **m=n-k+1**	≥۳
			دروازه انحصاری **OR**	رخداد خروجی در صورتی رخ می‌دهد که یکی از دو ورودی رخ دهد ولی ورودی دیگر رخ ندهد	وقوع خرابی سیستم واقع می‌شود فقط در صورتی که یکی از دو خرابی ممکن رخ دهند	≥۲
			دروازه **AND**	رخداد خروجی فقط رخ می‌دهد اگر همه رخدادهای ورودی رخ دهند	ردوندانسی موازی یکی از **n** تعداد شاخه‌های مساوی یا متفاوت	≥۲
			دروازه اولویت دار **AND** (**PAND**)	رخداد خروجی فقط در صورتی رخ می‌دهد که رخدادهای ورودی در توالی از چپ به راست رخ دهند	این مورد برای نمایش خرابی‌های ثانویه یا برای امکان‌پذیر کردن توالی رخدادها مناسب است	≥۲،۲ به (توضیح مربوط به دروازه متوالی رجوع شود)
			دروازه **INHIBIT**	رخداد خروجی فقط در صورتی رخ می‌دهد که هر دو رخداد ورودی رخ دهند، که یکی از آنها مشروط باشد	احتمال مشروط وقوع رخداد نهایی	۲
			دروازه **NOT**	رخداد خروجی فقط در صورتی رخ می‌دهد که رخداد ورودی رخ ندهد	رخدادهای انحصاری یا اقدام پیشگیرانه رخ نمی‌دهد	۱

جدول الف-۱ (ادامه)

	نماد		نام	توصیف	همبستگی قابلیت اطمینان	تعداد ورودی‌ها
	 این نماد بخشی از گروه نمادهای استاندارد قبلی نیست، این نماد نسبتا جدیدی برای نمایش این دروازه است		دروازه متوالی SEQ	رخداد خروجی(وقوع خرابی) فقط در صورتی رخ می‌دهد که کلیه رخدادهای ورودی به‌طور متوالی از چپ به راست رخ دهد. این دروازه مشابه دروازه PAND است به شرطی که تعداد خروجی ها در دروازه PAND محدود به ۲ نباشد که بعضی تحلیلگران انجام می‌دهند	این مورد برای نمایش وقوع خرابی‌های متوالی مناسب می‌باشد. (وقوع خرابی‌های زنجیر وار).همچنین توالی تنش‌هایی که عامل یک رخداد یا خرابی می‌باشند مستلزم تحلیل مارکوف است	>۲
			دروازه SPARE	رخداد خروجی رخ می‌دهد اگر تعداد و اجزا یدکی کمتر از تعداد مورد نیاز باشد	نمایش اجزا یدکی سرد، گرم و داغ اگر همه آنها دارای توزیع توان باشند. آنگاه راه حل مشکل بسته وجود خواهد داشت. اگر احتمال وقوع ثابت باشد به تحلیل مارکوف نیاز خواهد بود. توزیع ممکن است مستلزم احتمالات مشروط یا شبیه‌سازیهای مشروط باشد.	≥۱
			رخداد محلی	رخدادی که رخ داده یا با قطعیت رخ خواهد داد		
			رخداد صفر	رخدادی که نمی‌تواند وقوع یابد		

جدول ۱- در بالا شامل همه موارد نیست، بعضی از دروازه‌های گرافیکی یا نمایش رخداد که قابل مقایسه با سایر نمایش‌های گرافیکی نمی‌باشند از این جدول حذف شده‌اند، اما در جداول الف-۲ و الف-۳ و الف-۴ درج شده اند

جدول الف ۲- نمادهای رایج برای رخدادهای و توصیف رخدادها

نماد	نام نماد	تعریف	توصیف
	رخداد اصلی	پایین‌ترین سطح رخداد که برای آن احتمال وقوع یا اطلاعات قابلیت اطمینان موجود است.	مد خرابی یک جز یا یک علت خرابی منفرد
	رخداد مشروط	رخدادی که شرط وقوع رخداد دیگری می‌باشد آنگاه که هر دو رخداد باید رخ دهد تا رخداد خروجی واقع شود	رخداد مشروط مورد نیاز برای وقوع رخداد خروجی ، که با دروازه‌های AND اولویت دار و INHIBIT مورد استفاده قرار می‌گیرد.
	رخداد خاموش	رخداد اولیه که شاخص خرابی خاموش است، رخدادی که بلافاصله شناسایی نمی‌شود بلکه شاید با بازرسی مضاعف یا تحلیل تشخیص داده شود	یک رخداد اولیه که ممکن است از طریق تحلیل، بازرسی یا آزمایش ردیابی شود
	رخداد توسعه نیافته	رخداد اولیه که شاخص قسمتی از سیستمی است که هنوز توسعه نیافته است	یک شرکت کننده بالقوه در وقوع بالاترین رخداد است. اما اطلاعات وابسته برای توسعه رخداد در حال حاضر در دسترس نیست
	رخداد محلی	یک رخداد که درست (روشن) یا غلط (خاموش) است که می‌تواند بخشی از درخت خرابی باشد که در تحلیل گنجانده شده یا از آن حذف شده است.	یک رخداد تحت کنترل کاربر که تحلیل را تحت شرایط سیستم تعریف شده دیگری امکان‌پذیر می‌سازد

دروازه‌های استاتیک از قبیل OR، AND، EXCLUSIVE OR،INHIBIT، و دروازه‌های MAJORITY VOTE در جدول الف-۳ نشان داده شده است.

دروازه‌های دینامیک مانند PRIORITY AND، SPARE در جدول الف-۴ نشان داده شده است.

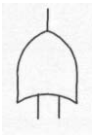
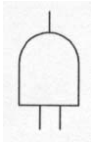
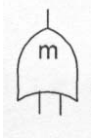
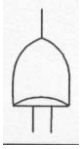
مثالی از دروازه AND اولویت دار

توصیف رخدادها

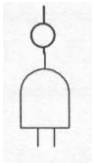
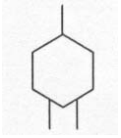
دیود D1 از IC در برابر ضربه ولتاژ منبع، حفاظت می‌کند. IC با افزایش ولتاژ آسیب نخواهد دید به شرطی که دیود ابتدا در مد باز خراب نشود.

اگر دیود باز شود و رخداد دوم رخ دهد در حالیکه ضربه ولتاژ وجود دارد انگاه بالاترین رخداد رخ می‌دهد (انفجارIC) این مدار در شکل الف-۱ نشان داده شده است.

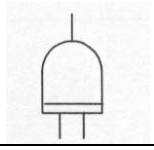
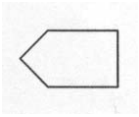
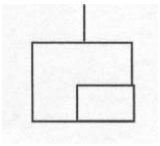
جدول الف-۳ دروازه‌های استاتیک

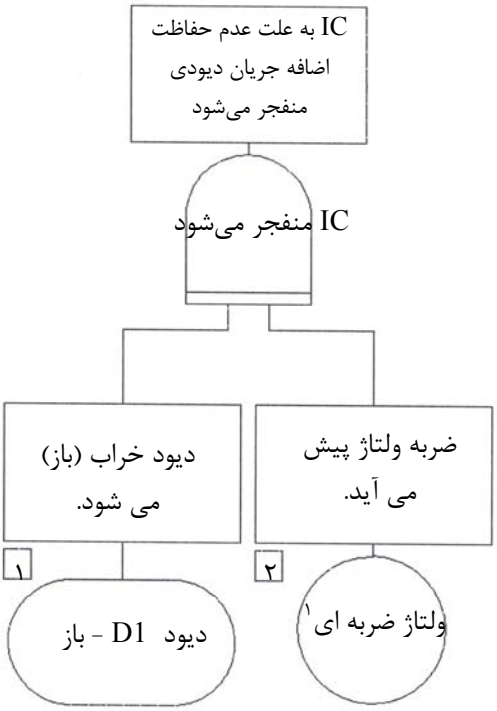
نام دروازه	توصیف	مدل قابلیت اطمینان	تعداد ورودیها
دروازه OR 	رخداد خروجی در صورتی رخ می‌دهد که هر یک از رخدادها ورودی رخ دهد	اگر رخدادهای سری مستقل باشند n از i= 2 $F(t)=1-\prod_{i=2}^{n}[1-F(t)]$ (هنگامی که رخدادها مستقل نیستند به بند ۴-۵-۵-۷ (انفصال) رجوع شود) $F(t)$ - احتمال وقوع رخداد یا وجود خرابی در زمان t است. R(t) هنگام استفاده مکمل F(t) می‌باشد	≥۲
دروازه AND 	رخداد خروجی تنها در صورتی رخ می‌دهد که همه رخدادهای ورودی رخ دهد	ردوندانسی موازی، شاخه‌های مساوی یا مستقل $F(t)=\prod_{i=2}^{n}Fi(t)$ متفاوت (هنگامی که رخدادها مستقل نیستند به بند ۴-۵-۵-۷ (انفصال) رجوع شود)	≥۲
دروازه اکثریت 	رخداد خروجی در صورتی رخ می‌دهد که m ورودی یا بیشتر از کل n تعداد ورودی رخ دهد.	ردوندانسی موازی که در آن k از n تعداد شاخه خراب نشده است. M=n-k+1 هنگامی که همه ورودیها یکسان هستند: $F(t)=\sum_{i=0}^{k-1}\frac{n!}{i!(n-i)!}[1-F_0(t)]^{t}[F_0(t)]^{n-1}$ هنگامی که رخدادها مستقل نیستند به ۴-۵-۵-۷ (انفصال) رجوع کنید	≥۲
دروازه not 	رخداد خروجی فقط در صورتی رخ می‌دهد که رخداد ورودی رخ ندهد	$F(t)=F_1(t).[1-F_2(t)]$ **یادآوری**- توصیه می‌شود که این دروازه توسط تحلیلگر مجرب و با دقت مورد استفاده قرار گیرد تا از نتایج نامطلوب اجتناب شود.	۱
دروازه انحصاری OR (دروازه XOR) 	رخداد خروجی در صورتی رخ می‌دهد که فقط یکی از دو رخداد ورودی رخ دهد	رخداد خروجی رخ می‌دهد اگر فقط یکی از رخدادهای و نه سایر رخدادها رخ دهد. $F(t)=F_1(t).[1-F_2(t)]$	≥۲

جدول الف-۳ (ادامه)

دروازه NOR 	رخداد خروجی در صورتی رخ می‌دهد که هیچ یک از رخدادهای ورودی رخ ندهند	به عنوان ترکیبی از دروازه NOT و OR عمل می‌کند. خروجی FALSE خواهد بود که یک یا چند ورودی TRUE وجود داشته باشد $F(t)=\prod_{i=2}^{n}(1-F_i(t))$ **یادآوری**- توصیه می‌شود که این دروازه توسط تحلیلگر مجرب و با دقت مورد استفاده قرار گیرد تا از نتایج نامطلوب اجتناب شود	≥۲
دروازه NAND 	رخداد خروجی در صورتی رخ می‌دهد که حداقل یکی از رخدادهای ورودی رخ ندهد	دروازه به عنوان ترکیبی از دروازه‌های NOT و AND عمل می‌کند $F(t)=\prod_{i=1}^{k}[1-F_i(t)]\prod_{ij=k}^{n-k}[F_j(t)]$ **یادآوری**- توصیه می‌شود که این دروازه توسط تحلیلگر مجرب و با دقت مورد استفاده قرار گیرد تا از نتایج نامطلوب اجتناب شود	≥۲
دروازه INHIBIT 	رخداد خروجی تنها وقتی رخ می‌دهد که هر دو رخداد ورودی رخ دهد یکی از آنها شرطی باشد	احتمال وقوع ، احتمال وقوع رخداد ورودی در احتمال وقوع شرایطی است که باید برآورده شود	۲

جدول الف-۴ دروازه‌های دینامیک

نام دروازه	توصیف	مدل قابلیت اطمینان	تعداد ورودیها
دروازه AND اولویت دار(PAND) 	رخداد خروجی(وقوع خرابی) تنها وقتی رخ می‌دهد که کلیه رخدادهای ورودی به‌صورت متوالی از چپ به راست رخ دهد	این مورد برای نمایش وقوع خرابی‌های ثانویه یا امکان توالی دو یا چند رخداد، مناسب می‌باشد. اگر بیش از دو رخداد باشد برابر با دروازه SEQUENCE ENFORCINGخواهد بود. که به تحلیل مارکوف نیاز دارد.	۲≥ به دروازه متوالی در زیر رجوع شود
دروازه متوالی ، SEQ 	رخداد خروجی تنها در صورتی رخ می‌دهد که همه رخدادها ورودی به‌صورت توالی از چپ به راست رخ دهد، و بیش از دو رخداد ورودی وجود داشته باشد. این دروازه جایگزینی برای دروازه PAND فوق است	این دروازه بسط دروازه PAND می‌باشد و چنین محسوب می شود تا بر توالی خیلی از دروازه‌ها تاکید شود. در این صورت دروازه اصلی PAND فقط محدود به دو ورودی می‌باشد . این مورد برای نمایش وقوع خرابی‌های متوالی مناسب است(وقوع خرابی زنجیروار) توالی تنش‌هایی که عامل وقوع رخداد یا وقوع خرابی هستند که مستلزم تحلیل مارکوف است.	۲<
دروازه یدکی:SPARE 	رخداد خروجی در صورتی رخ می‌دهد که تعداد اجزای یدکی کمتر از تعداد مورد نیاز باشد(ردوندانسی حاضر به خدمت)	نمایش اجزای یدکی سرد و گرم و داغ. اگر همه‌ی آنها توزیع نمایی داشته باشند آنگاه راه حل شکل بسته می‌تواند وجود داشته باشد. اگر احتمال وقوع رخدادها ورودی ثابت باشد آنگاه به تحلیل مارکوف نیاز خواهد بود. سایر توزیع‌ها ممکن است مستلزم احتمال شرطی یا شبیه‌سازی‌های شرطی باشد. اجزای یدکی قبل طی زمان فعال شدن، دارای احتمال وقوع خرابی کاهش یافته ای هستند. (برای مدل ردوندانسی گرم و سرد به بند ۷-۵-۳ رجوع کنید)	۱≥



شکل الف-۱ مثالی برای دروازه PAND

1-Spike

پیوست (ب)

(اطلاعاتی)

روش اجرایی مشروح برای انفصال[1]

ب-۱ راهکار موفقیت

فرض کنید نمودار بلوکی قابلیت اطمینان شبکه‌ای را نشان می‌دهد که شامل پنج عنصر A، B، C، D و E بوده و این‌که a، b،c ، d و e مربوط به متغیرهای موفقیت بولی مربوط است، نیز فرض می‌شود که موفقیت سیستم(ss)[2] در عبارت بولی با عبارت زیر تعریف می‌شود که شامل جمع چهار تا حاصلضرب می باشد. $SS = ac + bd + aed + bec$

برای انفصال عبارت بالا، روش به صورت زیر است:

مرحله ۱-۱ : هر عبارت را با توجه به عبارت اول منفصل کنید به شیوه‌ی سیستمی کار را ادامه دهید تا عبارت دوم با توجه به عبارت اول انفصال شود. هر عبارت را بررسی کنید تا ببینید آیا هیچ متغیری در عبارت اول به شکل کامل در عبارت دوم ظاهر می‌شود یا خیر. اگر چنین باشد، دو عبارت قبلا انفصال شده اند و کار بیشتری برای انجام نیست وگرنه تمام متغیرها را در عبارت اول خارج کنید (ac) که در عبارت دوم (bd) وجود ندارند (که این شیوه در واژه شناسی تئوری مجموعه ها، مکمل نسبی عبارت دوم با لحاظ عبارت اولی نامیده می شود.) در این مرحله خاص، نتیجه متغیرهای a و c خواهد بود.

مرحله ۱-۲: عبارت دوم ، bd، را با $\bar{a}bd + a\bar{c}bd$ جایگزین کنید.

مرحله ۱-۳: عبارت سوم را با توجه به عبارت اول منفصل کنید. ابتدا دو عبارت را بررسی کنید تا متوجه شوید آیا هیچ متغیری در عبارت به شکل کامل در عبارت دوم آمده است یا خیر. اگر چنین نباشد، مکمل نسبی عبارت سوم را با توجه به عبارت اول شناسایی کنید: یعنی متغیر c. بنابراین $\bar{c}aed$ را جانشین عبارت سوم کنید.

مرحله ۱-۴: عبارت چهارم (bec) را با توجه به عبارت اول منفصل کنید. مکمل نسبی عبارت چهارم با توجه به عبارت اول، متغیر a خواهد بود. بنابراین $\bar{a}bec$ را جانشین عبارت چهارم کنید

$$SS_1 = as + \bar{a}bd + a\bar{c}bd + \bar{c}aed + \bar{a}bec$$

اکنون فرآیند را با شروع از عبارت دوم تکرار کنید.

مرحله ۲-۱ : عبارت سوم $SS_1\left(a\bar{c}bd\right)$ را با توجه به عبارت دوم منفصل کنید ($\bar{a}bd$) در این حالت، عبارات قبلا انفصال شده(با احتساب متغیر a)، بوده بنابراین کار بیشتری نمی‌توان انجام داد.

مرحله ۲-۲ : عبارت چهارم $SS_1(\bar{c}aed)$ را با توجه به عبارت دوم $(\overline{a}bd)$ منفصل کنید. در این حالت هم توجه کنید که عبارات از قبل(با احتیاب متغیر a) انفصال شده بوده و کار بیشتری نمی‌توان انجام داد.

مرحله ۲-۳ : عبارت پنجم $SS_1(\bar{a}bec)$ را با توجه به عبارت دوم($\bar{a}bd$) منفصل کنید. مکمل نسبی آن متغیر d می‌باشد بنابراین $\bar{d}\bar{a}bec$ را جانشین عبارت پنجم کنید.

---

1 -Disjoining

1-System success

$$SS_2 = ac + \bar{a}bd + a\bar{c}bd + \bar{c}aed + \bar{d}\bar{a}bec$$

عبارت موفقیت سیستم در این مرحله به این صورت خواهد بود

حال فرآیند را با شروع از جمله سوم تکرار کنید.

مرحله ۳-۱ عبارت پنجم $SS_{2(}(\bar{c}aed)$را با توجه به عبارت سوم $(a\bar{c}bd)$ منفصل کنید. مکمل نسبی، متغیر b می‌باشد بنابراین ($\bar{b}caed$)را جانشین جمله چهارم کنید

مرحله ۳-۲: عبارت پنجم $SS_2(\bar{d}\bar{a}bec)$را با توجه به عبارت سوم $(a\bar{c}bd)$ منفصل کنید. در این حالت عبارات از قبل انفصال شده، بوده، بنابراین کار بیشتری نمی‌توان انجام داد.

عبارت موفقیت سیستم در این مرحله چنین خواهد بود:

$$SS_3 = ac + \bar{a}bd + a\bar{c}bd + \bar{b}\bar{c}aed + \bar{d}\bar{a}bec$$

و چون امکان ساده شدن بیشتر وجود ندارد، این عبارت انفصال نهایی خواهد بود.

با جانشینی‌های معمول، معادله برای اطمینان‌پذیری سیستم طبق زیر بدست می‌آید:

$$RS_1 = R_aR_C + (1-R_a)R_bR_d + R_a(1-R_c)R_bR_d + (1-R_b)(1-R_c)R_aR_eR_d + (1-R_d)(1-R_a)R_bR_eR_c$$

لازم به ذکر است که شکل نتیجه نهایی در مورد SS3 بستگی به ترتیبی خواهد داشت که جملات در عبارت اصلی بولی نوشته شده‌اند. با استفاده از برهان احتمال کل، می‌توان نشان داد که عبارت اطمینان‌پذیری سیستم را می‌توان طبق زیر نوشت:

$$R_{S2} = (R_a + R_b - R_aR_b)(R_c + R_d - R_cR_d)R_e + (R_aR_c + R_bR_d - R_aR_cR_bR_d)(1-R_e)$$

گرچه عبارات برای R_{S1} و R_{S2} کاملا متفاوت به نظر می‌آیند اما در واقع یکسان هستند

ب-۲ وقوع خرابی سیستم ، SF ، راهکار (مجموعه های قطعی)

انفصال طبق زیر توضیح داده می‌شود:

$$SF = ab + cd + aed + bec$$

برای انفصال عبارت فوق، روند مربوطه طبق زیر خواهد بود:

مرحله ۱-۱ هر عبارت را با توجه به عبارت اول منفصل کنید . به شیوه‌ای سیستمی کار را ادامه دهید تا عبارت دوم با توجه به عبارت اولی انفصال شود. دو عبارت را بررسی کنید تا متوجه شوید آیا هیچ متغیری در عبارت اول به شکل مکمل در عبارت دوم ظاهر می شود اگر چنین باشد دو عبارت انفصال شده اند و کار بیشتری نمی توان انجام داد و اگر چنین نباشد، همه متغیرها را در جمله اول (ab) که در عبارت دوم (cd) ظاهر نشده انتخاب کنید. (که این شیوه در واژه شناسی تئوری مجموعه ها، مکمل نسبی عبارت دوم با لحاظ عبارت اولی نامیده می شود.)) که در این مرحله خاص، نتیجه متغیرها a و b خواهد بود.

مرحله ۱-۲ جمله $\bar{a}cd + a\bar{b}cd$را جانشین جمله cd نمایید.

مرحله ۱-۳ جمله سوم را با توجه به جمله اول منفصل کنید. ابتدا دو جمله را بررسی کرده و ببینید آیا هیچ متغیری در جمله‌ی اول به شکل مکمل در جمله‌ی دوم آمده است یا خیر. از آنجا که چنین نیست ، مکمل جمله‌ی سوم را با توجه به جمله‌ی اول شناسایی کنید: یعنی متغیر b. در نتیجه جمله $\bar{b}aed$ را جانشین جمله سوم کنید.

مرحله ۱-۴ جمله چهارم (bac) را با توجه به جمله اول منفصل کنید. مکمل نسبی جمله چهارم با توجه به جمله‌ی اول، متغیر a می‌باشد بنابراین $\bar{a}bec$ را جانشین جمله چهارم کنید. عبارت وقوع خرابی سیستم در این مرحله چنین خواهد بود: $SF_1 = ab + \bar{a}cd + a\bar{b}cd + \bar{b}aed + \bar{a}bec$

اکنون فرآیند را با شروع از جمله دوم تکرار کنید.

مرحله ۲-۱ : جمله‌ی سوم $\left(a\bar{b}cd\right)$ را با توجه به جمله‌ی دوم $\bar{a}cd$ منفصل کنید. در این حالت جمله از قبل انفصال شده، بوده و کار بیشتری نمی‌توان انجام داد.

مرحله ۲-۲ : جمله چهارم $\left(\bar{b}aed\right)$ را با توجه به جمله دوم $\bar{a}cd$ منفصل کنید. در این حالت هم توجه داشته باشید که جملات قبلا انفصال شده و کار خاصی نمی‌توان انجام داد.

مرحله۲-۳ : جمله پنجم $\left(\bar{a}bec\right)$ را با توجه به جمله دوم $\bar{a}cd$ منفصل کنید. مکمل نسبی متغیر d می‌باشد بنابراین $\bar{d}\bar{a}bec$ را جانشین جمله‌ی پنجم کنید.

عبارت وقوع خرابی در این مرحله چنین خواهد بود:

$$SF_2 = ab + \bar{a}cd + a\bar{b}cd + \bar{b}aed + \bar{d}\bar{a}bec$$

حال فرآیند را با شروع از جمله سوم تکرارکنید.

مرحله ۳-۱ : جمله چهارم $\left(\bar{b}aed\right)$ را با توجه به جمله سوم $a\bar{b}cd$ منفصل کنید. مکمل نسبی متغیر c می‌باشد. بنابراین $\bar{b}\bar{c}aed$ را جانشین جمله چهارم کنید.

مرحله ۳-۲: جمله پنجم را $\left(\bar{d}\bar{a}bec\right)$ را با توجه به جمله سوم $a\bar{b}cd$ منفصل کنید. در این حالت، جملات قبلا انفصال شده و کار خاصی نمی‌توان انجام داد.

عبارت وقوع خرابی سیستم در این مرحله چنین خواهد بود : $SF_3 = ab + \bar{a}cd + a\bar{b}cd + \bar{b}\bar{c}aed + \bar{d}\bar{a}bec$

و چون بیش از این نمی‌توان عبارات را ساده‌تر کرد بنابراین عبارت انفصالی نهایی همین خواهد بود.

با جانشینی‌های معمول، معادله برای وقوع خرابی سیستم از طریق زیر بدست می‌آید:

$$F_{S1} = F_aF_b + (1-F_a)F_cF_d + F_a(1-F_b)F_cF_d + (1-F_b)(1-F_c)F_aF_eF_d + (1-F_d)(1-F_a)F_bF_eF_c$$

لازم به ذکر است که شکل نتیجه نهایی که SF_3 می‌باشد، بستگی به ترتیبی دارد که جملات در عبارت اصلی بولی نوشته شده‌اند.

کتابنامه

[۱]NASA Office of Safety and Mission Assurance: Fault Tree Handbook for Aerospace Applications, Version 1.1, 2002

[۲]US Nuclear Regulatory Commission: NUREG 0492, fault Tree Handbook, January, 1981

[۳]Mohame Modarres, Mark Kaminskiy, Vasiliy Krivitsov: Reliability Engineering and Risk Analysis, Marcel Dekker lnc.,new York, 1999

[۴]Alfredo H-S. Ang, Wilson H. Tang: Probability Concepts in Engineering Planning and Design, 1990

[۵]Milena Krasich: Fault Tree Analysis for Failure Mode Identification and Product Reliability Improvement, Tutorial, RAMS, 2005, Alexandria, VA

[۶]Systems" 1999 Tutorial Notes, Reliability and Maintainability Symposium, Washington, DC

[۷]Kiran Kumar Vemuri and Joanne Bechta Dugan, "Reliability Analysis of Complex Hardware-Software Systems", Proceedings, Annual Reliability and Maintainability Symposium, January 1999, Washington, DC

[۸]Géza Szabó and Peter GAspAr, "Practical Treatment Methods for Adaptive Components in the Fault-Tree Analysis", Proceedings, Annual Reliability and Maintainability Symposium, January 1999, Washington, DC

[۹]IEC 60300-3-1, Dependability management — Part 3-1: Application guide — Analysis techniques for dependability — Guide on methodology

[۱۰]IEC 60812, Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)

[۱۱]IEC 61078, Analysis techniques for dependability — Reliability block diagram and boolean methods