جزوات آموزشی

صنایع ایمن فراز ارک

عنوان محتوا:

ارزیابی ریسک FTA

کد محتوا:

ARK-FO-159-097

تهیه و تدوین: گروه تولید محتوای صنایع ایمن فراز ارک

مقدمه

تجزیه و تحلیل درخت خطا (Fault Tree Analysis)

تجزیه و تحلیل درخت خطا (FTA) یک **تکنیک قیاسی** است که بر روی یک حادثه خاص یا خرابی سیستم اصلی تمرکز می‌کند و به شیوه‌ای منطقی سازماندهی و به صورت تصویری نمایش داده می‌شود. درخت خطا یک **مدل گرافیکی** است که **ترکیبات مختلفی از خرابی تجهیزات و خطاهای انسانی را نشان می‌دهد که می‌تواند منجر به خرابی اصلی سیستم مورد نظر شود (رویدادهای اصلی)**. این امر به تحلیلگر خطر اجازه می‌دهد تا اقدامات **پیشگیرانه** یا **کاهشی** را روی دلایل اساسی مهم برای کاهش احتمال وقوع یک حادثه متمرکز کند. با داده‌های مناسب می‌توان از آن برای تعیین **کمیت** احتمال یا **فراوانی** یک رویداد استفاده کرد.

این روش تجزیه و تحلیل عمدتاً در مهندسی ایمنی برای درک **چگونگی** خرابی سیستم‌ها، **شناسایی** بهترین راه‌ها برای کاهش ریسک و **تعیین** (یا دریافت احساس) نرخ رویدادهای ایمنی حوادث می‌باشد و در حمل و نقل نیز کاربرد دارد. FTA در هوافضا، انرژی هسته‌ای، شیمیایی، فرآیند داروسازی، پتروشیمی و در سایر صنایع پرخطر نیز استفاده می‌شود.

با شروع رویداد اصلی، علل احتمالی یا حالت‌های خطای عملکردی که در سطح پایین‌تر سیستم قرار گرفته شناسایی می‌شوند. FTA یک رویکرد منضبط را ارائه می‌دهد که **بسیار سیستماتیک** است، اما در عین حال **به اندازه کافی انعطاف پذیر** است تا امکان تجزیه و تحلیل عوامل مختلف، از جمله **تعاملات انسانی و پدیده‌های فیزیکی** را فراهم کند.

FTAیک رویکرد از بالا به پایین است. استفاده از رویکرد **"بالا به پایین"**، تکنیک توجه را بر آن دسته از اثرات شکست متمرکز می‌کند که مستقیماً با رویداد بالا مرتبط هستند. این یک مزیت منحصر به فرد است. **نمایش تصویری** منجر به درک آسان رفتار سیستم می‌شود، اما از آنجایی که درختان اغلب بزرگ هستند، پردازش درختان خطا ممکن است به سیستم‌های کامپیوتری نیاز داشته باشد. این ویژگی همچنین تأیید درخت خطا را دشوار می‌کند. FTA ممکن است برای شناسایی خطر استفاده شود، اگرچه در درجه اول در ارزیابی ریسک به عنوان **ابزاری برای ارائه تخمینی از احتمالات یا فرکانس‌های خرابی** استفاده می‌شود.

تاریخ

از دهه ۱۹۶۰، روش‌های FTA کاربرد روزافزونی در بخش‌های تولید و خدمات پیدا کردند و اکنون **یکی از ساده‌ترین و مؤثرترین روش‌ها برای تجزیه و تحلیل ایمنی سیستم‌ها محسوب می‌شوند.** (FTA) در ابتدا در سال ۱۹۶۲ در آزمایشگاه-های بل به منظور ارزیابی سیستم کنترل پرتاب موشک بالستیک قاره پیما توسعه یافت. استفاده از درختان خطا از آن زمان پشتیبانی گسترده‌ای به دست آورده است و اغلب به عنوان ابزار تجزیه و تحلیل شکست توسط کارشناسان استفاده می‌شود.

تجزیه و تحلیل درخت خطا می‌تواند در موارد زیرمورد استفاده قرار گیرد:

- اولویت بندی مشارکت کنندگان منجر به رویداد برتر
- ایجاد لیست تجهیزات / قطعات / رویدادهای مهم برای معیارهای مختلف
- نظارت و کنترل بر عملکرد ایمنی سیستم پیچیده (به عنوان مثال، آیا یک هواپیمای خاص برای پرواز در هنگام خرابی سوپاپ ایمنی دارد؟ برای چه مدت مجاز است که با نقص دریچه پرواز کند؟).
- به حداقل رساندن و بهینه سازی منابع
- به عنوان یک ابزار تشخیصی برای شناسایی و اصلاح علل رویداد برتر عمل می‌کند. این عملکرد می‌تواند به ایجاد دستورالعمل‌ها و فرآیندهای تشخیصی کمک کند.

روش شناسی

هر سیستم به اندازه کافی پیچیده، در مواجهه با خرابی یک یا چند زیر سیستم قرار می‌گیرد. با این حال، احتمال شکست اغلب می‌تواند از طریق بهبود طراحی سیستم کاهش یابد. تجزیه و تحلیل درخت خطا، رابطه بین خطاها، زیرسیستم‌ها و عناصر طراحی ایمنی اضافی را با ایجاد یک نمودار منطقی از سیستم کلی ترسیم می‌کند.

نتیجه نامطلوب به عنوان ریشه ("رویداد برتر") درخت منطق در نظر گرفته می‌شود. با عقب‌رفتن از این رویداد بالا، ممکن است مشخص شود که این اتفاق از دو طریق می‌تواند رخ دهد: **در حین عملیات عادی یا در حین عملیات تعمیر و نگهداری**.

هنگامی که درختان خطا با اعداد واقعی برای احتمالات شکست برچسب گذاری می‌شوند، برنامه‌های کامپیوتری می‌توانند احتمال شکست را از درختان خطا محاسبه کنند. هنگامی که یک رویداد خاص بر روی بیش از یک رویداد اثر دارد، یعنی روی چندین زیرسیستم تأثیر می‌گذارد، به آن علت مشترک یا حالت مشترک می‌گویند. از نظر گرافیکی، به این معنی است که این رویداد در چندین مکان در درخت ظاهر می‌شود. **علل مشترک روابط وابستگی بین رویدادها را معرفی می‌کند**. محاسبات احتمال درختی که دارای برخی علل رایج است بسیار پیچیده‌تر از درختان معمولی است که در آن همه رویدادها مستقل در نظر گرفته می‌شوند. همه ابزارهای نرم افزاری موجود در بازار چنین قابلیتی را ندارند.

درخت معمولاً با استفاده از نمادهای **دروازه منطقی** معمولی نوشته می‌شود. برخی از صنایع هم از درختان خطا و هم از درختان رویداد استفاده می‌کنند.

نمادهای گرافیکی

نمادهای اصلی مورد استفاده در FTA به عنوان **رویدادها**، **دروازه‌ها** و **نمادهای انتقال** دسته بندی می‌شوند. تغییرات جزئی ممکن است در نرم افزار FTA استفاده شود.

نمادهای رویداد برای رویدادهای **اولیه** و رویدادهای **میانی** استفاده می‌شوند. رویدادهای اولیه، بیشتر روی درخت خطا توسعه نمی‌یابند. رویدادهای میانی در خروجی یک دروازه یافت می‌شوند. برخی از **نمادهای رویداد در زیر نشان داده شده است:**

ردیف	نماد رویداد	توضیحات
۱		رویداد شکست اولیه یا پایه. این یک رویداد تصادفی است و اطلاعات کافی در دسترس است.
۲		وضعیت سیستم، زیر سیستم و اجرا
۳		پیشامد ثانویه، می تواند بیشتر مورد بررسی قرار گیرد ولی به دلیلی انجام نمی شود.
۴		رویداد شرطی و مطابق با رویداد دیگر
۵		نشان دهنده وقوع یا عدم وقع یک واقعه است. (احتمال ۱ یا ۰)
۶		نماد انتقال برای تکرار یک شاخه یا زیر درخت از FTA

۱-نمادهای رویداد

نمادهای رویداد اولیه معمولاً به صورت زیر استفاده می شوند:

رویداد اساسی – خرابی یا خطا در یک جزء یا عنصر سیستم. (به عنوان مثال: سوئیچ در موقعیت باز گیر کرده است)

رویداد خارجی – معمولاً انتظار می‌رود رخ دهد. (به خودی خود یک خطا نیست)

رویداد توسعه نیافته – رویدادی که اطلاعات کافی در مورد آن در دسترس نیست، یا هیچ نتیجه‌ای ندارد.

رویداد شرطی‌سازی– شرایطی که گیت‌های منطقی را محدود یا تحت تأثیر قرار می‌دهند (مثال: حالت عملکرد در حال اجرا)

یک دروازه رویداد میانی را می‌توان بلافاصله بالای یک رویداد اولیه استفاده کرد تا فضای بیشتری برای تایپ شرح رویداد فراهم کند. نمادهای گیت، رابطه بین رویدادهای ورودی و خروجی را توصیف می‌کنند.

عملکرد دروازه‌ها به شرح زیر است:

دروازه OR – خروجی در صورتی رخ می‌دهد که دقیقا یک ورودی رخ دهد.

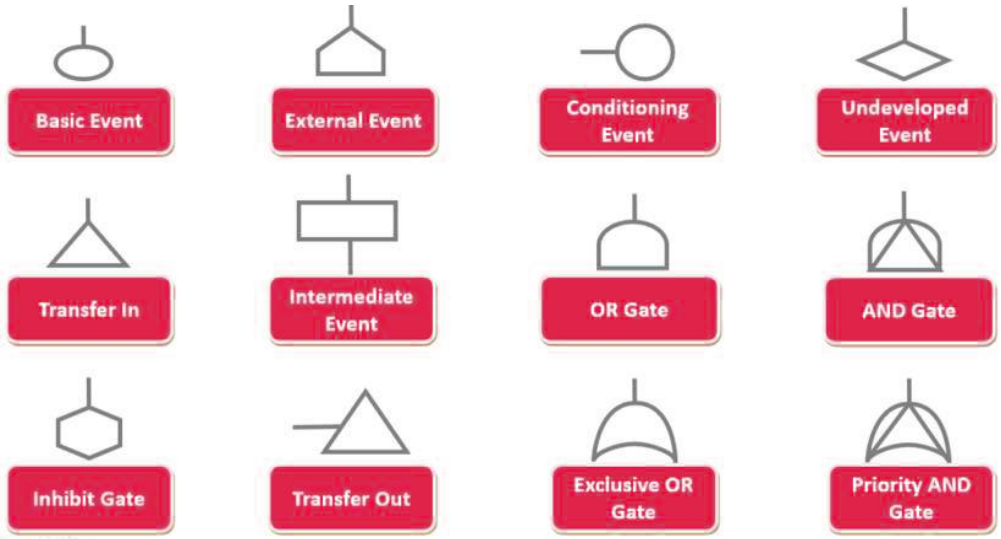
دروازه AND – خروجی تنها در صورتی رخ می‌دهد که همه ورودی‌ها رخ دهند (ورودی‌ها مستقل از منبع هستند).

دروازه اولویت AND – خروجی در صورتی رخ می‌دهد که ورودی‌ها در یک توالی خاص مشخص شده توسط یک رویداد شرطی رخ دهند.

دروازه مهار – خروجی در صورتی رخ می‌دهد که ورودی تحت یک شرایط فعال کننده مشخص شده توسط یک رویداد شرطی سازی رخ دهد.

نمادهای انتقال

نمادهای انتقال برای اتصال ورودی و خروجی درختان خطای مرتبط استفاده می‌شوند. (مانند درخت خطای یک زیر سیستم که به سیستم اصلی آن متصل می‌شود.)



۲-تعدادی از نمادهای دروازه و انتقال

رویدادهای یک درخت خطا با احتمالات آماری یا نرخ‌های ثابت توزیع شده به صورت نمایی مرتبط هستند. به عنوان مثال، خرابی قطعات معمولاً ممکن است با نرخ شکست ثابت λ (یک تابع خطر ثابت) رخ دهد. در این ساده‌ترین حالت، احتمال شکست به نرخ λ و زمان قرار گرفتن در معرض t بستگی دارد:

$$p=1-e^{-\lambda t}$$

درخت خطا اغلب به یک بازه زمانی معین، مانند یک ساعت پرواز یا یک زمان متوسط ماموریت، بستگی دارد. احتمالات رویداد نیز به رابطه تابع خطر رویداد با این بازه بستگی دارد.

تحلیل و بررسی

بسیاری از رویکردهای مختلف را می‌توان برای مدل سازی FTA استفاده کرد، اما رایج‌ترین و محبوب‌ترین روش را می‌توان در چند مرحله خلاصه کرد. یک درخت خطای منفرد برای تجزیه و تحلیل تنها یک رویداد **نامطلوب** استفاده می‌شود که ممکن

است متعاقباً به درخت خطای دیگری به عنوان یک اصلی یا اساسی وارد شود. اگرچه ماهیت رویداد نامطلوب ممکن است به طور چشمگیری متفاوت باشد، **یک FTA برای هر رویداد نامطلوب از همان رویه پیروی می‌کند.**

تجزیه و تحلیل FTA شامل پنج مرحله است:

۱- رویداد نامطلوب برای مطالعه را تعریف کنید. اگرچه مشاهده برخی از رویدادها بسیار آسان و واضح است، یک مهندس با دانش گسترده‌ای از طراحی سیستم، بهترین فردی است که به تعریف و شماره گذاری رویدادهای ناخواسته کمک می‌کند. سپس از رویدادهای نامطلوب برای ایجاد FTA استفاده می‌شود. هر FTA محدود به یک رویداد ناخواسته است.

۲- شناختی از سیستم به دست آورید. پس از انتخاب رویداد نامطلوب، همه علل با احتمال تأثیرگذاری بر روی رویداد نامطلوب ۰ یا بیشتر مورد مطالعه و تجزیه و تحلیل قرار می‌گیرند. بدست آوردن اعداد دقیق برای احتمالات منجر به رویداد معمولاً غیرممکن است، زیرا ممکن است انجام آن بسیار پرهزینه و زمان‌بر باشد. نرم افزار کامپیوتری برای مطالعه احتمالات استفاده می‌شود. این امر ممکن است منجر به تحلیل سیستم با هزینه کمتری شود. تحلیلگران سیستم می‌توانند به درک سیستم کلی کمک کنند

۳-درخت خطا را بسازید. پس از انتخاب رویداد نامطلوب و تجزیه و تحلیل سیستم، می‌توانیم درخت خطا را بسازیم. درخت خطا بر اساس دروازه‌های AND و OR است که ویژگی‌های اصلی درخت خطا را تعریف می‌کنند.

۴-درخت خطا را ارزیابی کنید. پس از اینکه درخت خطا برای یک رویداد نامطلوب خاص مونتاژ شد، برای هر گونه بهبود احتمالی مورد ارزیابی و تجزیه و تحلیل قرار می‌گیرد یا به عبارت دیگر مدیریت ریسک را مطالعه می‌کند و راه‌هایی برای بهبود سیستم پیدا می‌کند. طیف گسترده‌ای از روش‌های تحلیل کمی و کیفی را می‌توان به کار برد. این مرحله به عنوان مقدمه‌ای برای مرحله نهایی است که کنترل خطرات شناسایی شده خواهد بود. به طور خلاصه، در این مرحله تمام خطرات احتمالی مؤثر بر سیستم را به صورت مستقیم یا غیر مستقیم شناسایی می‌کنیم.

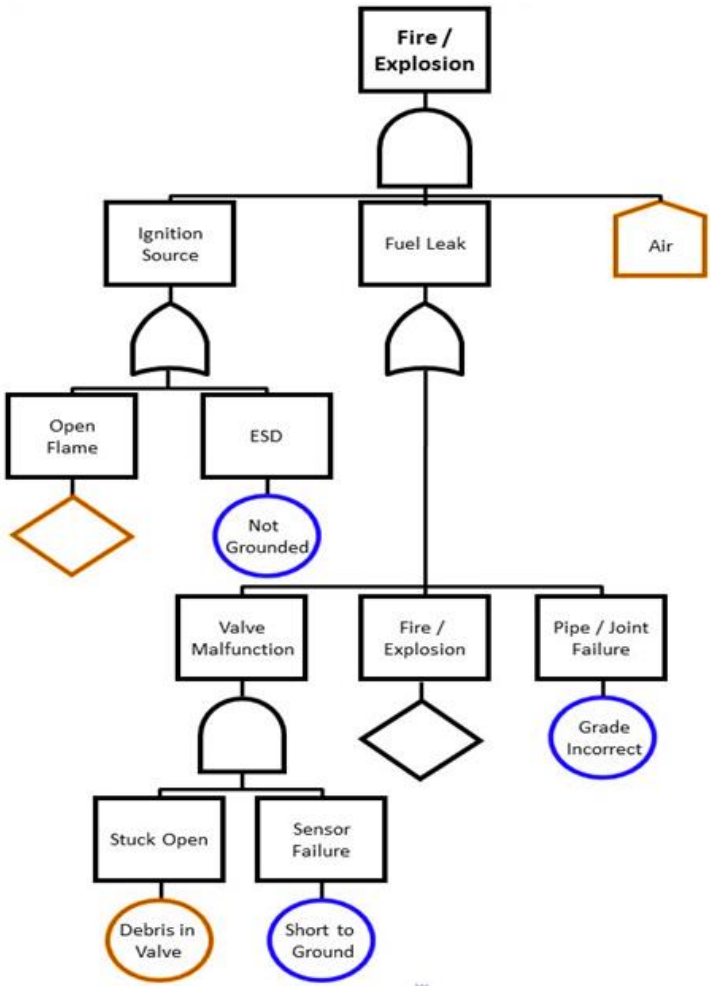
۵-خطرات شناسایی شده را کنترل کنید. این مرحله بسیار خاص است و تا حد زیادی، از سیستمی به سیستم دیگر متفاوت است، اما نکته اصلی همیشه این خواهد بود که پس از شناسایی خطرات، تمام روش‌های ممکن برای کاهش احتمال وقوع دنبال می‌شود.

مقایسه با سایر روش های تحلیلی

FTA یک روش قیاسی و از **بالا به پایین** است که با هدف تجزیه و تحلیل اثرات شروع خطاها و رویدادها بر روی یک سیستم پیچیده انجام می‌شود. این در تضاد با تحلیل حالت و اثرات خرابی (FMEA) است، که یک روش **تحلیلی استقرایی** و **از پایین به بالا** با هدف تجزیه و تحلیل اثرات خرابی‌های تک جزء یا عملکرد بر روی تجهیزات یا زیرسیستم‌ها است. FTA در نشان دادن مقاومت یک سیستم در برابر خطاهای آغازگر منفرد یا چندگانه بسیار خوب است. FMEA در فهرست نویسی کامل خطاها و

شناسایی اثرات محلی آنها کارایی بهتری دارد اما در بررسی چندین خرابی یا اثرات آنها در سطح سیستم چندان مناسب نیست. FTA رویدادهای خارجی را در نظر می‌گیرد، FMEA اینطور نیست.

جایگزین‌های FTA شامل نمودار وابستگی (Dependency diagram) است که به عنوان نمودار بلوک قابلیت اطمینان (RBD) و تجزیه و تحلیل مارکوف نیز شناخته می‌شود. یک نمودار وابستگی، معادل تجزیه و تحلیل درخت موفقیت (STA)، معکوس منطقی یک FTA است، و سیستم را با استفاده از مسیرها به جای گیت‌ها نشان می‌دهد. DD و STA احتمال موفقیت (یعنی اجتناب از یک رویداد برتر) را به جای احتمال یک رویداد برتر تولید می‌کنند.



۳-مثالی برای FTA

منابع

1) https://wikips.tamu.edu/fault-tree-analysis-fta/

2) https://news.gminternational.com/risk-analysis-fta-eta

۳) https://en.m.wikipedia.org/wiki/Fault_tree_analysis