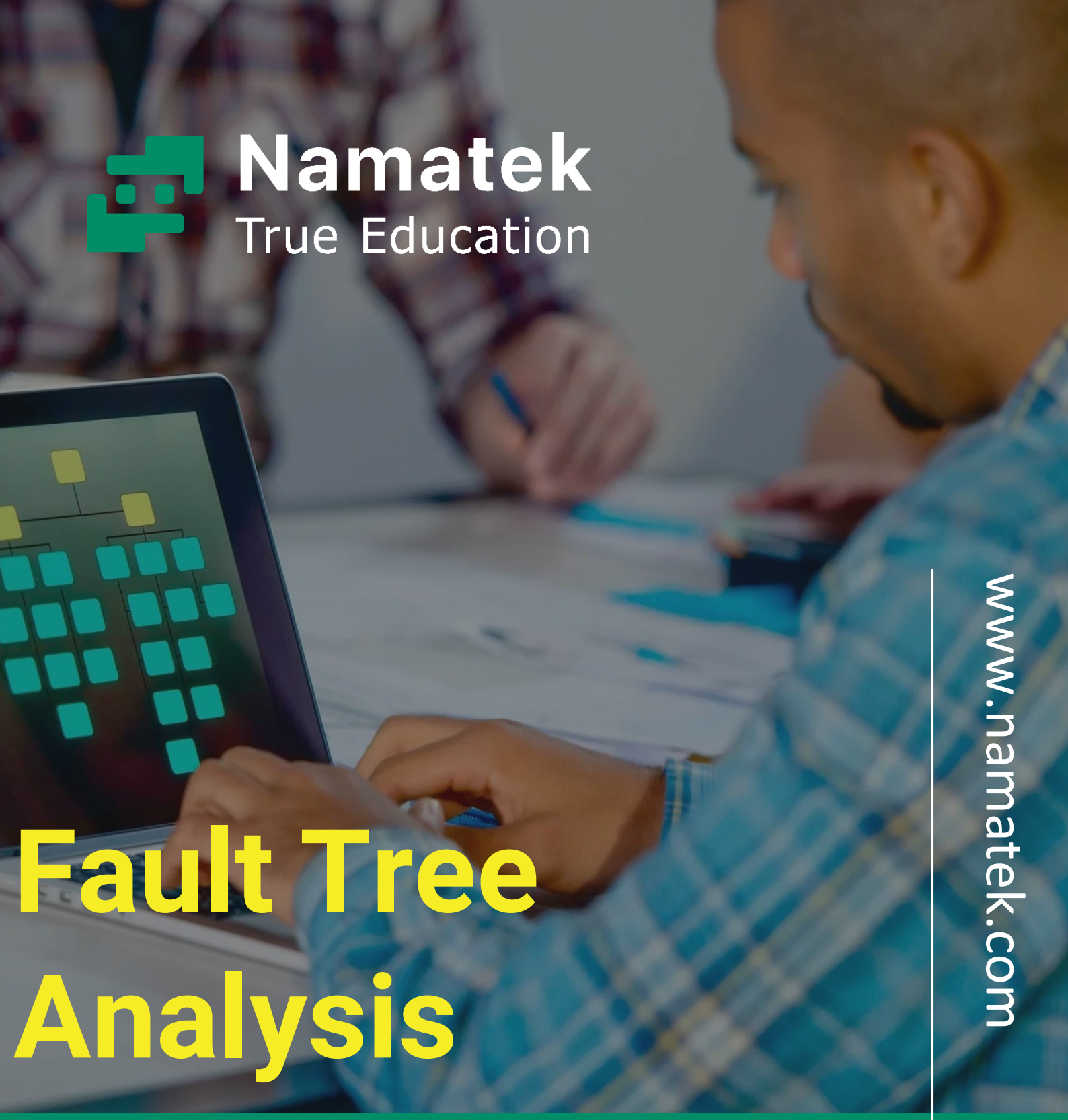


Namatek
True Education

Fault Tree Analysis

www.namatek.com

تحلیل درخت خطا

فهرست مطالب

مهندسان وظیفه دارند قبل از اینکه محصول به دست مصرف‌کننده برسد، شکست آن را پیش‌بینی کنند. شکست بالقوه باید در اوایل چرخه توسعه محصول شناسایی شود تا با موفقیت، خطر را کاهش دهد. این فعالیت پیشگیری از شکست برای محافظت از مصرف‌کننده در برابر یک تجربه غیرقابل‌قبول در نظر گرفته شده است. ابزارهای زیادی برای شناسایی خرابی‌های بالقوه و علل و مکانیسم‌های آن‌ها استفاده می‌شود. یکی از این ابزارها، تحلیل درخت خطا (FTA) است.

FTA یک تحلیل قیاسی است که مسیر بصری شکست را نشان می‌دهد.

همانطور که فناوری محصول و فرایند پیچیده‌تر می‌شود، رویکردهایی همچون FTA بصری به‌عنوان یک تکنیک ریسک مستقل یا مکملی برای تحلیل حالت و اثرات شکست برای تحلیل بهتر معرفی شده‌اند. در این مقاله با ارائه توضیحاتی در مورد تحلیل درخت خطا و ویژگی‌های آن به بررسی مزایا و معایب آن می‌پردازیم.

تحلیل درخت خطا (FTA) چیست؟

تحلیل درخت خطا یا FTA که مخفف Fault Tree Analysis است، یک تحلیل قیاسی از بالا به پایین است که به صورت بصری یک مسیر شکست یا زنجیره شکست را به تصویر می‌کشد.

FTA از مفهوم منطق بولی پیروی می‌کند که اجازه ایجاد یک سری عبارات بر اساس True / False را می‌دهد. وقتی این عبارات در یک زنجیره به هم متصل می‌شوند، نمودار منطقی شکست را تشکیل می‌دهند. رویدادها در دنباله‌ای از روابط سری («OR») یا روابط موازی («AND») مرتب می‌شوند. نتایج برای هر رویداد در یک نمودار درخت مانند با استفاده از نمادهای منطقی برای نشان دادن وابستگی بین رویدادها ارائه می‌شود.

رویدادها مربوط به اجزای مکانیکی، نرم‌افزار یا الکترونیک مورد استفاده در طراحی محصول است. رویدادهای ناخواسته سطح بالا موضوع اصلی مورد مطالعه در FTA است. معمولاً طبقه‌بندی شدت رویداد سطح بالا در یک تحلیل خطر در سطح سیستم تعیین می‌شود. تحلیل درخت خطا همچنین اطلاعات ارزشمند عیب‌یابی را هنگام اعمال برای حل مسئله ارائه می‌دهد.

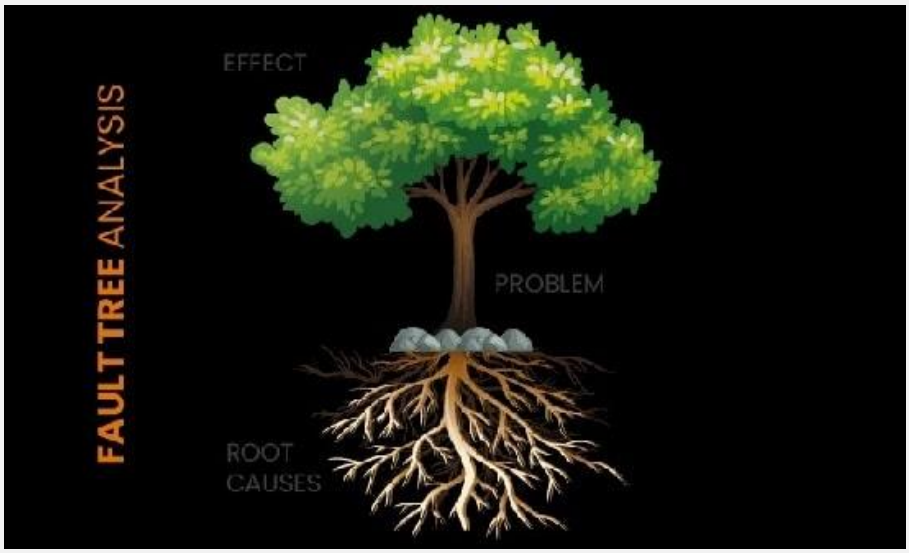
نمودار FTA اغلب از احتمالات خرابی در هر سطح، از اجزا و نرم‌افزار گرفته تا رویدادهای سطح بالای نامطلوب، استفاده می‌کند. تحلیل درخت خطا توسط طراحان سیستم، طراحان فرایند، مدیران پروژه و مهندسان در تولید استفاده می‌شود. این پرسنل اغلب از FTA در کنار روش کایزن و تحلیل علت اصلی برای جلوگیری یا حل خرابی‌های سیستم استفاده می‌کنند.

تاریخچه تحلیل درخت خطا

تحلیل درخت خطا یک تکنیک برای تجزیه‌وتحلیل قابلیت اطمینان و ایمنی است. آزمایشگاه‌های بل اولین کسانی بودند که این روش را اتخاذ کردند.

در سال ۱۹۶۲، H.Watson به همراه A.Mearbs از آزمایشگاه‌های بل در حال طراحی پادمان‌هایی برای سیستم موشک‌های بالستیک قاره‌پیما (ICBM) برای نیروی هوایی ایالات متحده به نام سیستم Minuteman بودند. برای چنین فناوری پیچیده و خطرناکی، ایمنی کامل یک نگرانی عمده بود. برای بهبود تجزیه‌وتحلیل قابلیت اطمینان خود، آن‌ها روش تجزیه‌وتحلیل خطا را ایجاد کردند. یک سال بعد (۱۹۶۳)، دیو هاسل از شرکت بوئینگ، پتانسیل تجزیه و تحلیل درخت خطا را به‌عنوان یک سیستم مهم برای ارزیابی ایمنی تشخیص داد. این مفهوم امروزه به طور گسترده در هوافضا، خودرو، صنایع شیمیایی، هسته‌ای و نرم افزاری، به ویژه برای رویدادهای قابلیت اطمینان و ایمنی مورد استفاده قرار می‌گیرد.

علت استفاده از تحلیل درخت خطا



تحلیل درخت خطا مسیر مبتنی بر ریسک را به یک علت اصلی یا رویداد سطح پایه نشان می‌دهد. ریسک‌های شناسایی‌شده، اقداماتی را انجام می‌دهند که برای کاهش خطر قبل از راه‌اندازی برنامه در نظر گرفته شده است. از طرف دیگر، هنگام بررسی یک شکست، زنجیره‌ای از رویدادها که

توسط FTA به تصویر کشیده شده است، به حل کننده این امکان را می‌دهد که رویدادهایی را که منجر به یک علت ریشه یا رویداد در سطح پایه می‌شوند، ببیند.

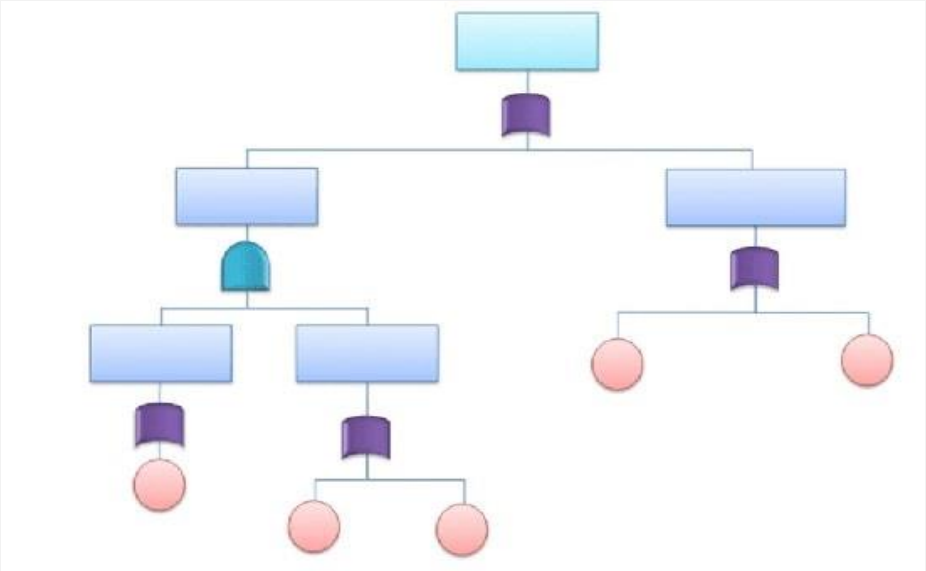
به طور کلی تحلیل درخت خطا زمانی اعمال می‌شود که:

- یک تحلیل خطر قبلاً یک نگرانی ایمنی را نشان می‌داد.
- یک طرح جدید با محتوای جدید وجود دارد.
- یک طرح فعلی با تغییراتی وجود دارد که ممکن است شامل تغییراتی به دلیل شکست گذشته باشد.
- یک طرح فعلی در حال استفاده در یک محیط جدید یا تغییر در چرخه وظیفه (بدون تغییر فیزیکی در طراحی) باشد.
- نگرانی ایمنی یا نظارتی در حال بررسی است.
- تصویری تولید شده از خطا، سودمندتر از یک تحلیل استقرایی نوشتاری باشد.

نمودار درخت خطا

نمودار درخت خطا (FTD) بلوک دیاگرام‌های منطقی هستند که وضعیت یک سیستم و اجزای آن را نمایش می‌دهند. در این نمودار از یک مدل گرافیکی برای مسیرهای درون یک سیستم استفاده می‌کنند که منجر به رویدادهای زیان قابل‌پیش‌بینی و ناخواسته می‌شود. مسیرها رویدادها و شرایط کمکی را با استفاده از نمادهای منطقی استاندارد به هم متصل می‌کنند. ساختارهای اساسی در نمودار درخت خطا، دروازه‌ها و رویدادهایی هستند که رویدادها معنای یکسانی به‌عنوان یک بلوک دارند و دروازه‌ها شرایط هستند.

نمادهای نمودار درخت خطا



هر صنعتی از مجموعه نمادها و قراردادهای نام‌گذاری یکسانی برای درختان خطا استفاده می‌کند. رویدادها و دروازه‌ها دو دسته‌ای هستند که فعالیت‌ها را نشان می‌دهند.

1) نمادهای رویداد

رویدادها زمانی رخ می‌دهند که یک سیستم یا فرایند با شکست مواجه شود. انواع رویدادهایی که در درختان خطا ظاهر می‌شوند در زیر به تفصیل توضیح داده شده است.

- **رویداد بالا (TE):** این نوع رویدادها در بالای درخت خطا قرار دارند و باعث بررسی خرابی سیستم می‌شوند. یک ورودی دارد؛ اما خروجی نسبی ندارد زیرا شروع خرابی است.
- **رویدادهای میانی (IE):** این رویدادها عموماً توسط یک یا چند رویداد ایجاد می‌شوند. هم ورودی و هم خروجی دارند. رویداد دیگری ممکن است باعث شکست آن شود و به احتمال زیاد باعث خرابی‌های بیشتر در درخت خطا می‌شود.

- **رویدادهای اساسی (BE):** این نوع رویدادها به طور کلی علت اصلی رویداد برتر هستند. آن‌ها در پایین درخت خطا می‌نشینند.
- **رویدادهای توسعه نیافته (UE):** این رویدادها اطلاعات کافی ندارند و به‌عنوان یک درخت فرعی قرار می‌گیرند.
- **رویدادهای انتقال (TE):** این نوع رویدادها زمانی اتفاق می‌افتند که درخت خطا بیش از حد طولانی باشد که روی کاغذ قرار نگیرد. قسمت‌های بزرگ‌تر درخت با یک نماد پنهان شده و در یک درخت جداگانه گسترش می‌یابد. دو نوع وجود دارد: رویدادهای انتقال به بیرون و انتقال ورودی. انتقال به بیرون دارای یک مثلث و خروجی به سمت راست است و رویدادهای انتقال ورودی دارای ورودی در بالای مثلث هستند.
- **رویدادهای شرطی (CE):** این رویدادها به‌عنوان شرایط برای نوعی از دروازه به نام دروازه بازدارنده رخ می‌دهند.
- **رویدادهای خانه (HE):** این نوع رویدادها برای خاموش و روشن کردن یک رویداد استفاده می‌شوند. اگر رویداد روی ۰ تنظیم شود به این معنی است که رخ نمی‌دهد؛ اما اگر روی ۱ تنظیم شود به این معنی است که رخ خواهد داد. رویدادهای خانه برای اجازه دادن یا عدم گنجاندن بخش‌هایی از درخت خطا استفاده می‌شوند.

برخی از نمادهای پرکاربرد، به اختصار در جدول زیر دسته‌بندی شده‌اند:

نماد	نام	توضیحات
	رویداد پایه	یک خطای اصلی شروع کننده شکست
	رویداد خارجی (رویداد خانه)	رویدادی که معمولاً انتظار یا تضمین می‌شود که رخ دهد. به طور کلی، آن‌ها یک احتمال ثابت 0 یا 1 دارند.
	رویداد توسعه نیافته	رویدادهای توسعه نیافته نیازی به تجزیه بیشتر ندارند. این رویدادی است که بیشتر توسعه نمی‌یابد زیرا تجزیه و تحلیل بیشتر به دلیل کمبود اطلاعات امکان‌پذیر نیست. این یک رویداد اساسی است که نیازی به حل ندارد.
	رویداد تهویه	یک رویداد شرطی‌سازی یک شرط یا محدودیت خاص است که می‌تواند برای هر دروازه اعمال شود.
	انتقال در	انتقال، نماد تحلیل درخت خطا نشان می‌دهد که درخت در نقطه دیگری از درخت توسعه‌یافته است.
	انتقال به بیرون	انتقال به بیرون نشان می‌دهد که این بخش از درخت به مکان دیگری در همان درخت متصل است.

2) نمادهای دروازه

گیت‌ها نشان دهنده راه‌های مختلفی هستند که خرابی‌ها در یک دارایی یا سیستم رخ می‌دهد. گاهی اوقات یک رویداد واحد می‌تواند باعث شکست سطح بالا (یا شکست فاجعه بار) شود. گاهی اوقات ترکیبی از رویدادهای مختلف می‌تواند منجر به یک رویداد شکست سطح بالا شود.

نماد	نام	توضیحات
	دروازه AND	در یک گیت AND، اگر همه رویدادهای ورودی رخ دهند، رویداد خروجی مثبت است. از نظر قابلیت اطمینان سیستم، می‌توان گفت که تمام اجزا باید از کار بیفتند تا سیستم از کار بیفتد.
	دروازه OR	در یک دروازه OR، رویداد خروجی اتفاق می‌افتد. حتی اگر یکی از رویدادهای ورودی رخ دهد. از نظر قابلیت اطمینان سیستم، این بدان معناست که اگر هر جزء ورودی خراب شود، سیستم از کار خواهد افتاد.
	دروازه OR انحصاری	هر کدام اما نه همه، این قانون دروازه انحصاری OR است. یک رویداد خروجی تنها در صورتی رخ می‌دهد که یکی از شرایط ورودی برآورده شود، اما اگر همه شرایط برآورده شوند، اتفاق نمی‌افتد.
	دروازه اولویتAND	دروازه اولویت AND به این معنی است که خروجی تنها پس از وقوع چندین رویداد ورودی در یک دنباله خاص رخ می‌دهد.
	دروازه مهار	یک رویداد تنها در صورتی رخ می‌دهد که همه رویدادهای ورودی رخ دهند و یک رویداد شرطی اضافی نیز رخ دهد. دروازه مهار یک گیت AND با یک رویداد اضافی است.

انواع گیت‌ها در FTA به تفصیل در زیر آمده است.

- **گیت AND:** این نوع گیت به رویدادهای خروجی متصل می‌شود. رویدادها تنها در صورتی رخ می‌دهند که رویدادهای ورودی به گیت رخ دهند.
- **گیت AND ترتیب دار:** این گیت در صورتی رخ می‌دهد که تمام رویدادهای ورودی به ترتیب خاصی اتفاق بیفتند.
- **گیت OR:** این نوع گیت ممکن است یک یا چند ورودی داشته باشد و اگر یک یا چند رویداد ورودی اتفاق بیفتد یک رویداد خروجی رخ خواهد داد.
- **گیت XOR:** این گیت کمی کمتر رایج است. خروجی تنها در صورتی اتفاق می‌افتد که یک عنصر ورودی رخ دهد.
- **k/N یا گیت VOTING:** این گیت از نظر بصری شبیه دروازه OR است. تعدادی رویداد ورودی 'N' و یک رویداد خروجی 'k' وجود خواهد داشت. رویداد خروجی زمانی رخ می‌دهد که تعداد رویدادهای ورودی رخ دهد. برای راه اندازی این گیت باید تعداد دقیق ورودی‌ها برآورده شود.
- **گیت INHIBIT:** این نوع گیت زمانی یک رویداد خروجی خواهد داشت که همه رویدادهای ورودی و شرطی رخ دهند.

نحوه انجام تحلیل درخت خطا در تجزیه و تحلیل علل احتمالی یک شکست در سیستم

FTA یک تفکیک منطقی از رویداد نامطلوب سطح بالا است که به رویداد سطح پایه (علت اصلی) تبدیل می‌شود. هر مسیر یک احتمال دارد. مسیرهای مربوط به ترکیبات با بیشترین شدت و بالاترین احتمال شناسایی می‌شوند که نیاز به کاهش دارند. شروع از رویداد سطح پایه و کار کردن در مسیر تا رویداد سطح بالای نامطلوب، مجموعه برش نامیده می‌شود.

مجموعه‌های برش زیادی در FTA وجود دارند. برای هر کدام یک احتمال فردی اختصاص داده شده است. اغلب برای شناسایی سطح ریسک نشان داده شده، رویداد سطح پایه کد رنگی دارد.

5 مرحله اساسی برای انجام تحلیل درخت خطا به شرح زیر است:

۱. خطر را شناسایی کنید.
۲. درک درستی از سیستم در حال تحلیل به دست آورید.
۳. درخت خطا را ایجاد کنید.
٤. مجموعه‌های برش را شناسایی کنید.

۵. کاهش خطر را انجام دهید.

خطر را شناسایی کنید.

دانستن پیامد شکست، در تعریف رویداد سطح بالای درخت خطا مفید است. رویداد سطح بالا یا خطر باید تا حد امکان دقیق تعریف شود:

- چقدر
- چه مدت (مدت)
- تأثیر ایمنی
- تأثیر زیست‌محیطی
- تأثیر نظارتی

درک سیستم در حال تحلیل را به دست آورید.

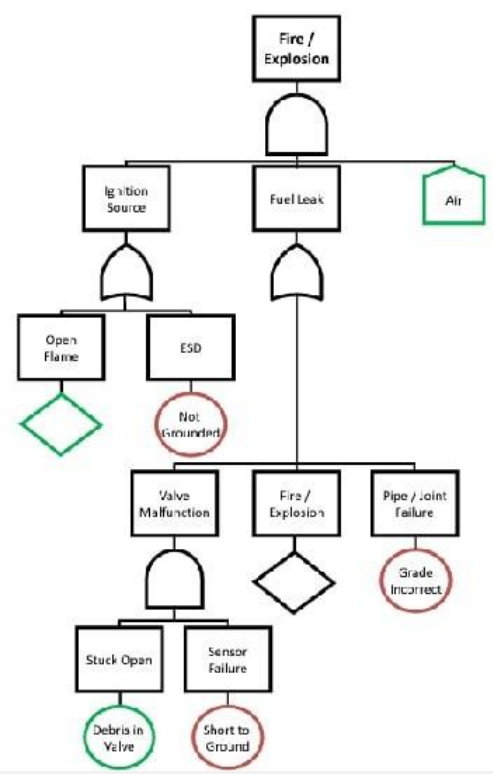
این مرحله شامل مراحل زیر است:

- ایجاد یا کسب اطلاعات پشتیبانی مناسب:
  - فهرست اجزا
  - نمودار مرزی
  - شماتیک
  - الزامات کد
  - صداها و محیط‌های مهندسی
  - نمونه‌هایی از محصولات مشابه یا خرابی
- تهیه فهرست علل احتمالی خطر
  - مهندسین طراحی سیستم را که دانش کاملی از سیستم و عملکردهای آن دارند در سطوح بالاتر تحلیل درخت خطا

بگنجانید. این دانش برای انتخاب، بسیار مهم است. این مهندسان می‌توانند در ایجاد روابط علل شکست یا خطا کمک کنند.

- تخمین احتمال علل در رویداد سطح پایه
- برچسب زدن همه علل با کد (اختیاری)
- اولویت بندی یا ترتیب علل به ترتیب وقوع یا احتمال

درخت خطا را ایجاد کنید.



این مرحله را با مثالی در مورد آتش سوزی بررسی می‌کنیم. در مثال FTA در سمت راست، تیم تحلیل را در مورد "Air Present" متوقف می‌کند؛ زیرا حضور اکسیژن خارج از کنترل تیم توسعه دهنده FTA است. تحلیل تا سطح بعدی در مورد "نشت سوخت" ادامه می‌یابد.

تیمی که FTA را انجام می‌دهد، گرد هم آمده است تا بر علل احتمالی نشت سوخت تمرکز کند. تحلیل تنها به خرابی‌های مکانیکی محدود نمی‌شود. گنجاندن الکترونیک و نرم‌افزار در طراحی پیچیده فرصت ایجاد یا کاهش خرابی‌ها را به ارمغان می‌آورد. خطرات ممکن است از طریق انتخاب‌های مهندسی جلوگیری شوند یا از طریق کنترل کیفیت کنترل شوند. درخت مثال به سطوح اضافی و جزئی‌تر ادامه می‌یابد. رویداد سطح پایه نقطه‌ای است که تیم می‌تواند خطر را برطرف کند که معمولاً به‌صورت زیر کدگذاری می‌شود:

- قرمز: ریسک بحرانی
- نارنجی: پرخطر
- زرد: خطر جزئی
- سبز: قابل قبول/خطر بسیار کم

مجموعه‌های برش را شناسایی کنید.

- ریسک برای هر رویداد تخمین زده می‌شود:
  - در صورت موجود بودن، داده‌های میزان شکست می‌توانند برای محاسبه ریسک یک زنجیره یا زنجیره‌های متعدد مورد استفاده قرار گیرند.
  - اگر داده‌ای وجود نداشته باشد، برآوردی بر اساس دستورالعمل‌های ذهنی ایجاد می‌شود.
- مجموعه‌های برش با ریسک بیشتر از تحمل سیستم (یعنی شرایط ایمنی یا غیرعملکردی) برای کاهش انتخاب می‌شوند.
- برای موارد بحرانی (قرمز) و ریسک بالا (نارنجی) اقدامات لازم است.

کاهش خطر

کاهش خطر می‌تواند اشکال مختلفی داشته باشد. یک روش رایج استفاده از روش بحرانی است. سایر تکنیک‌ها به سطحی از کاهش نیاز دارند که بر اساس نقص در هر میلیون فرصت (DPMO) محاسبه می‌شود. گزارش‌های عملیات و سوابق تجدیدنظر برای پیگیری و بسته شدن هر خطر نامطلوب نگهداری می‌شوند. هر خطری که تا حد قابل قبولی کاهش نیابد، کاندیدای اثبات اشتباه یا کنترل کیفیت است که مصرف‌کننده را از خطر محافظت می‌کند.

1) نمونه‌هایی از استراتژی‌های کاهش

وقتی خطری غیر قابل قبول باشد، تیم ممکن است چندین گزینه در دسترس داشته باشد. در زیر چند نمونه از گزینه‌های موجود آورده شده است:

- تغییر طراحی
- انتخاب یک مؤلفه با قابلیت اطمینان بالاتر برای جایگزینی مؤلفه رویداد سطح پایه: این اغلب گران است مگر این‌که در مراحل اولیه توسعه محصول شناسایی شود.
- افزونگی فیزیکی جزء: این گزینه مؤلفه اضافی را به موازات دیگری قرار می‌دهد. هر دو باید به طور هم‌زمان شکست بخورند تا خطر تجربه شود.

  اگر مشکل ایمنی وجود داشته باشد، این گزینه ممکن است به اجزای غیر یکسان نیاز داشته باشد.
- افزونگی نرم‌افزار: افزودن یک مدار حسگر که می‌تواند وضعیت محصول را تغییر دهد، اغلب با محافظت از اجزا از طریق تغییرات

چرخه وظیفه و کاهش تنش‌های ورودی هنگام شناسایی، شدت رویداد را کاهش می‌دهد.

- سیستم هشدار: مدار ممکن است فقط درباره یک رویداد هشدار دهد. این امر مستلزم اقدام یک اپراتور یا تحلیلگر است. توجه به این نکته ضروری است که در صورت انجام این اقدام، قابلیت اطمینان عوامل انسانی نیز باید وارد ارزیابی شود.
- کنترل کیفیت: این ممکن است شامل حذف شکست بالقوه از طریق آزمایش یا بازرسی باشد. اثربخشی بازرسی باید با سطح شدتی که خطر ممکن است بر مصرف‌کننده تحمیل کند مطابقت داشته باشد.

مزایای استفاده از تحلیل درخت خطا چیست؟

تحلیل درخت خطا یک روش است که می‌تواند برای تحلیل اثرات یک شکست منفرد بر روی یک سیستم استفاده شود. در زیر برخی از مزایای دیگر استفاده از FTA آورده شده‌اند:

- علت یک رویداد شکست را محدود می‌کند که باعث صرفه جویی در وقت و هزینه شما در یافتن علت اصلی می‌شود.
- راه‌هایی را برای کاهش عواقب یک شکست قبل از وقوع آن مشخص می‌کند.

به عنوان مثال، اگر در حال طراحی پروانه هواپیما هستید، ممکن است از تحلیل درخت خطا استفاده کنید تا مشخص کنید در صورت شکستن ملخ چه اتفاقی می‌افتد و چگونه ممکن است تعمیر شود. با استفاده از این اطلاعات، می‌توانید در وهله اول نحوه جلوگیری از وقوع این شکست‌ها را بیابید.

- به شما کمک می‌کند تا تعیین کنید کدام شکست‌ها بیشتر احتمال دارد اتفاق بیفتد و این امکان را می‌دهد که تلاش‌های خود را ابتدا روی جلوگیری از آن شکست‌ها متمرکز کنید.
- حالت‌های خرابی رایج را در چندین سیستم یا محصول (مانند اجزای مشابه) شناسایی می‌کند که می‌تواند به شما کمک کند تعیین کنید که در کجا تغییرات طراحی بیشتر مورد نیاز است.

معایب تحلیل درخت خطا

- گیت‌ها و رویدادهای زیادی برای تحلیل سیستم بزرگ در نظر گرفته شود.

- نقطه ضعف اصلی این است که فقط یک رویداد برتر را بررسی می‌کند.
- شکست‌های علت رایج همیشه واضح نیستند.
- ثبت عوامل تأخیر مرتبط با زمان و سایر عوامل دشوار است.
- به افراد با تجربه برای درک دروازه‌های منطقی نیاز دارد.