# تحلیل درخت خطا

## Fault Tree Analysis

با مثال های کاربردی
در صنایع نفت و گاز


ترجمه و تألیف :

مهندس سیّد حسن اصفهانی

## مقدمه مترجم :

رشد روزافزون صنعت و فن آوری در سالهای اخیر ، نیازمند تغییر نگرش و رویکرد مدیران نسبت به موضوعات ایمنی ، بهداشت و محیط زیست ( HSE ) ، در سازمان ها و صنایع است . شرط لازم برای این تغییر نگرش و همگام شدن با سازمان های موفق بین المللی ، استقرار نظام مدیریت HSE در شرکت ها می باشد و گام اول در استقرار این نظام ، تعهد مدیریت ارشد سازمان است . منشور تعهد مدیریت در خط مشی نمود پیدا می کند . مثلاً مدیر سازمان ، مسئولیت تامین منابع مورد نیاز را می پذیرد و به تمامی ذی نفعان اطمینان می دهد که منافع آنها را با افزایش ایمنی ، ارتقاء سلامت و کاهش یا حذف آلودگی ، تأمین نماید .
یکی از مهم ترین عناصر HSE-MS ، مدیریت ریسک است . کلمه ریسک را بارها شنیده اید . واژه ای که در محاوره ها بسیار مورد استفاده قرار می گیرد . مثلاً برای کاری که ممکن است عواقب سنگینی بدنبال داشته باشد ، گفته می شود که از ریسک بالایی برخوردار است . اما ریسک چیست و چرا کاهش یا حذف آن به این اندازه مهم است ؟ این سئوال را تحلیل گران سیستم به خوبی پاسخ داده اند . تحلیل گرانی که به بقاء سیستم و ارتقاء عملکرد آن می اندیشند ، بر این باورند که سازمان هایی که مملو از رویدادهای مخاطره آمیز باشند ، دوام نخواهند یافت . آنها به این درک مشترک رسیده اند که بایستی سیستمی برای شناسایی مخاطرات و ارزیابی ریسک های سازمان ، به شکل پیش فعال وجود داشته باشد . سیستمی که مخاطرات را شناسایی کرده و مخاطرات پر ریسک را غربال کند و در نهایت راهکارهایی را برای کنترل و یا حذف آنها ارائه نماید . در این ارزیابی که ابتدا به شکل کاملاً کیفی انجام می پذیرد ، ریسک ها بر اساس یک جدول از پیش تعریف شده ، طبقه بندی می شوند و ریسک هایی که در ناحیه قرمز (ناحیه ریسک های غیر قابل قبول ) واقع می شوند ، برجسته شده و به منظور تحلیل دقیق تر از نظر شدت و احتمال مورد ارزیابی کمّی قرار می گیرند . ارزیابی کمّی در واقع یک خط کش و معیار قابل اعتماد در اختیار تحلیل گران قرار می دهد تا به شکل منطقی و با محاسبه ، روش های کاهش سطح ریسک را امتحان کنند . از طرفی به مدیران در تخصیص منابع و اعتبارات کمک می نماید . هدف از این مقدمه آماده نمودن ذهن خوانندگان در مورد موضوع کتاب بود . ارزیابی درخت خطا ، نه تنها به ارزیابی کیفی یک رویداد مخاطره آمیز با ریسک بالا می پردازد ، بلکه ابزار بسیار کارآمدی برای تجزیه و تحلیل کمّی ریسک می باشد . در این تحلیل رویدادهای مخاطره آمیزی که بر اساس نتایج حاصل از ارزیابی های قبلی یا سوابق سازمان ، نامطلوب تشخیص داده شده اند ، توسط تحلیل گران سیستم هدف قرار می گیرند و دلایل وقوع آنها به شکل منطقی ردیابی می شود و تمامی مراحل تحلیل ، قدم به

قدم به شکل گرافیکی و با استفاده از معادلات جبری ، ثبت می گردد . بدین طریق نه تنها احتمال بروز رویداد نامطلوب ، محاسبه می شود ، بلکه میزان کاهش آن در صورت انجام اقدامات کنترلی نیز ، معلوم می گردد . بخش اعظم این کتاب از کتاب **مرجع تحلیل درخت خطای سازمان ناسا** ، ترجمه و اقتباس شده است . بخش هایی از کتاب نیز حاصل تجربیات اینجانب در طراحی و اجرای پروژه های ارزیابی ریسک به روش FTA در سازمان های مختلف بوده است . از ویژگیهای جالب این کتاب رسم ده ها نمودار و گراف درختی است که با استفاده از نرم افزار visio رسم شده و به فارسی برگردانده شده است و نمونه این کار را در کتب دیگر کمتر مشاهده می کنید . هدف این کتاب علاوه بر آشنایی خوانندگان با تحلیل درخت خطا ، توانمند کردن آنها در اجرایی نمودن این روش در سازمان شان می باشد . بدین منظور سعی شده که مطالب کتاب با مثال ها و مطالعاتی که مرتبط با صنایع فرآیندی مانند صنایع نفت وگاز است ، درک متقابلی در ذهن خوانندگان ایجاد کند و تنها ارائه مطالب صرف تئوری نباشد

در پایان لازم است از تمامی عزیزانی که به طریقی در تهیه و ترجمه این کتاب ، مرا یاری داده و مشّوق من بوده اند ، تشکر نمایم . همچنین از گروه مدیریت ریسک شرکت ملی نفت ایران کمال تشکر را دارم و از تمامی عزیزانی که کتاب را مطالعه می کنند ، تقاضا دارم ، راهنمای من در ادامه مسیر باشند و پیشنهادات خود را از طریق ایمیل به آدرس زیر ارسال نمایند :
hse.esfahani@yahoo.com

**و من الله توفیق**

سید حسن اصفهانی

دی ماه ۸۸

## پیشگفتار :

بیش از دو دهه است که تحلیل احتمالی ریسک[1] (PRA ) و تکنیک های زیر مجموعه آن از جمله تحلیل درخت خطا[2] ( FTA )، روش های قابل اعتمادی در ارزیابی ایمنی بوده و بخاطر داشتن نگرش جامع و سیستمی ، بارها قابلیت خود را در آشکار کردن نقاط ضعف طراحی و عملیاتی اثبات کرده اند. نقاط ضعفی که حتی از چشم زبده ترین کارشناسان و مهندسین ایمنی بدور مانده است . این روش ها نشان دادند که نه تنها بایستی رویدادهای منفرد با احتمال کم و شدت بالا را بررسی کرد بلکه بایستی سناریوهای بد فرجامی که در نتیجه بروز رویدادهای کم خطر اما پر احتمال بوجود می آیند را نیز مد نظر قرار داد .

بر خلاف درک عموم ، این رویدادهای ظاهراً کم خطر ، اغلب زیانبارتر از رویدادهای اولی هستند . بزرگترین نقطه قوت PRA و تکنیک تحلیلی پایین دست آن FTA ، این است که آنها ابزار پشتیبان نیرومندی در فرآیند تصمیم گیری هستند . در کاربری های ایمنی ، این روش ها به مدیران و مهندسین کمک می کنند تا نقاط ضعف طراحی و عملیاتی را در سیستم های پیچیده پیدا کرده و به شکل مؤثری در جهت بهبود ایمنی سیستم تلاش کنند .

به منظور بهره گیری بیشتر از PRA و FTA ، مهم است که مدیران و کارکنان آنها با ارزش و کاربرد این روش ها آشنایی داشته باشند . این کتاب با همین هدف ترجمه و تالیف شده است و نسخه بروز شده و کاربردی تر کتاب مرجع تحلیل درخت خطا می باشد که برای اولین بار در سال ۱۹۸۱ میلادی توسط کمیته تنظیم مقررات هسته ای ایالات متحده (NRC) با عنوان NUREG-0492 منتشر گردید . و می تواند به عنوان یک کتاب راهنما در دوره های آموزشی

[1] Probabilistic Risk Assessment
[2] Fault Tree Analysis

FTA برای دانشجویان ، مهندسین ، کارشناسان HSE و تمامی علاقه مندان مورد استفاده قرار گیرد .

سعی شده که بیشتر جنبه های کاربردی این روش مد نظر قرار گیرد و خوانندگان با استفاده از مطالب و مثال های کتاب ، آشنایی نسبتاً خوبی با این تکنیک پیدا کنند و از آن به عنوان ابزاری در جهت ارتقاء ایمنی سیستم و بهبود عملکرد آن بهره بگیرند . همچنین مواردی به محتوای کتاب اضافه شده که در نسخه اصلی موجود نیست . این موارد عبارتند از :

- مطالبی درباره دیاگرام تصمیم گیری دودوئی (BDD) برای حل درخت خطا در مقابل روش های کلاسیک نظیر استفاده از جبر بول[۱] و مجموعه برش های حداقل[۲] .
- بحث مفصلی در رابطه با شکست های علت مشترک[۳] (CCF) و خطاهای انسانی در FTA .
- شرح مدلسازی حلقه های بازخورد[۴] بگونه ای که بتوان آنها را به شکلی مناسب از درخت خطا جدا کرد .
- توصیف درخت موفقیت[۵] که متمم منطقی درخت خطا می باشد و یک ضمیمه کامل به آن اختصاص داده شده است .
- شرحی برمعیارهای اهمیت ( نسبی و مطلق ) که از FTA حاصل می شوند و از قابلیت های جالب این روش می باشد .

---

۱ Boolean algebra
۲ Minimal Cut Sets
۳ Common Cause Failures
4 Feedback Loops
5 Success Tree

## فهرست مطالب

## فهرست اصطلاحات

**BDD =**Binary decision Diagram

**BE =**Basic Event

**CCF =**Common Cause failure

**ETA =**Event Tree Analysis

**FMEA =** Failure Mode and Effect Analysis

**FT =**Fault Tree

**FTA =**Fault Tree Analysis

**HAZID =**Hazard Identification

**HAZOP =**Hazard & Operability Study

**HRA =**Human Reliability Analysis

**MCS =**Minimal Cut Set

**PRA =** Probabilistic Risk Assessment

**TE =**Top Event

# فصل اول : مقدمه

## ۱-۱) سخنی با خوانندگان

این کتاب نسخه بروز شده مرجع تحلیل درخت خطا می باشد و برای خوانندگانی نوشته شده که آشنایی مختصری با تحلیل سیستمی و ریاضیات پایه داشته باشند . هیچگونه دانش یا آموزش قبلی در زمینه آمار ، تحلیل ریسک و قابلیت اطمینان مورد نیاز نیست . مفاهیم پایه

تحلیل آماری و قابلیت اطمینان و ریسک در فصل های مربوطه و ضمائم کتاب آورده شده است .

بخش اول کتاب به شرح مفاهیم ، مراحل و کاربردهای FTA می پردازد . تحلیل درخت خطا ، یک تکنیک مبتنی بر شکست و جزءگرا می باشد. جزءگرا از این جهت که با یک رویداد نامطلوب شروع شده و سپس با استفاده از یک فرآیند سیستمی رو به عقب ، علل وقوع این رویداد ناخواسته را مشخص می کند و در طی این فرآیند ، درخت خطایی به منظور توصیف گرافیکی رویداد ها و ارتباط آنها برای وقوع رویداد نامطلوب یا رویداد رأس ، رسم می شود . در این درخت از نمادهایی استفاده می شود که نوع رویداد ها و نوع ارتباط آنها را با یکدیگر نشان می دهد . در واقع FT ، یک مدل کیفی است که اطلاعات مفید بسیاری از علل بروز یک رویداد نامطلوب ارائه می دهد و از طرفی می توان آن را کمّی نمود و اطلاعات بیشتری درباره احتمال وقوع رویداد رأس و میزان اهمیت تمامی علل و رویداد های مدل شده ، بدست آورد .

علاوه بر FTA ، روش های کل گرا نیز در تحلیل ریسک و قابلیت اطمینان ، بکار برده می شوند . تفاوت این روش ها با تحلیل درخت خطا در منطق رو به جلو آنهاست . بدین معنی که شروع آنها با یک رویداد آغازین بوده و در نهایت به بررسی آثار و پیامدهای حاصل از این رویداد می پردازند . شباهت این روش ها با FTA در این است که همگی نگرشی مبتنی بر شکست دارند . در این کتاب نقش FTA در فرآیند تصمیم گیری آورده شده و بر روی اطلاعات ذی قیمتی که می توان از این روش برای اولویت بندی اهمیت رویداد های سهیم در وقوع رویداد رأس بدست آورد ،تأکید شده است . چرا که با مشخص شدن میزان اهمیت یک رویداد پایه و سهم آن در بروز رویداد رأس ، تصمیم گیری در مورد تخصیص منابع و امکانات برای بهبود عملکرد سیستم ، سهل ترخواهد شد .

تکنیک FTA را می شود هم برای سیستم موجود و هم سیستمی که در حال طراحی است ، بکار برد. تنها تفاوتی که وجود دارد سطح دسترسی به داده ها می باشد . در سیستم های در حال طراحی ، بدلیل فقدان داده های مورد نیاز ، از داده های عام استفاده می شود . اما در یک سیستم موجود با توجه به وجود سابقه تعمیر و نگهداری تجهیزات و دیگر اطلاعات ثبت شده ، دسترسی به داده ها ساده تر است . با اجرای FTA در یک سیستم ، نقاط ضعف سیستم مشخص شده و می توان ارزیابی لازم را برای ارتقاء و بهبود سیستم انجام داد . همچنین می توان رفتار سیستم را پیش بینی کرده ، بر آن نظارت نمود. علاوه بر این با شناسایی نقاط ضعف سیستم و علل آن ، شرح اقدامات شفاف تر شده و مسئولیت بخش ها و افراد مشخص می شود . بخش دوم این کتاب شامل مثالی از کاربرد تحلیل درخت خطا در صنایع شیمیایی است . تا خواننده درک و بینش عمیق تری نسبت به این تکنیک پیدا کند .

این کتاب پنج ضمیمه دارد که به شرح مبانی ریاضی مورد نیاز برای کمّی کردن درخت خطا پرداخته و خواننده را از این لحاظ از مراجعه به کتب دیگر بی نیاز می کند . همچنین درخت موفقیت و طریقه حصول آن از درخت خطا با ذکر دو مثال در ضمیمه د نشان داده شده است در ضمیمه آخر نیز مثال دیگری از نحوه رسم و تفسیر درخت خطا آورده شده که کاربرد این تحلیل را حتی در زندگی روزمره نشان می دهد .

### ۱-۲) تحلیل درخت خطا

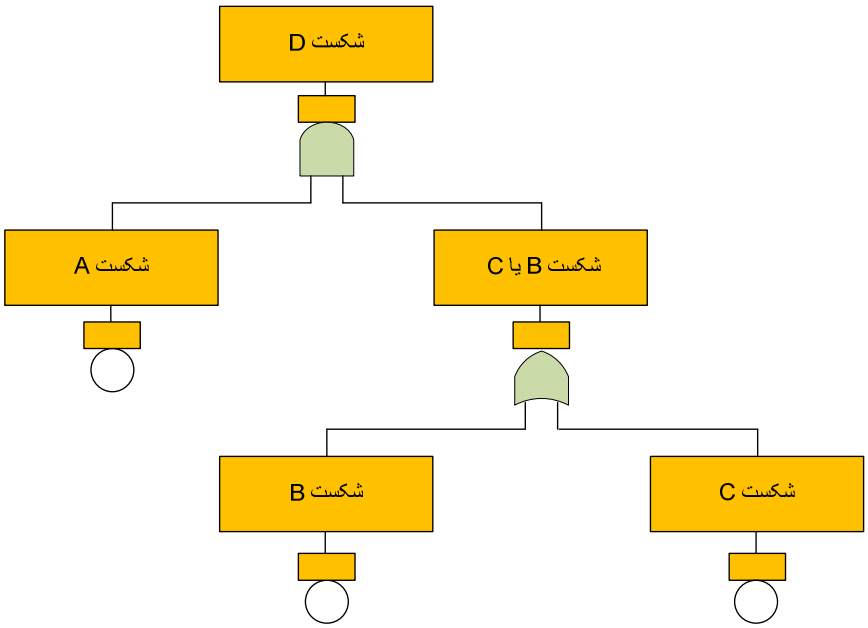
تکنیک FTA را می توان خیلی ساده به عنوان یک روش تحلیلی در نظر گرفت که در آن وضعیت نامطلوبی از سیستم ( معمولاً وضعیتی که از نقطه نظر ایمنی بحرانی تلقی می شود )

مشخص شده و سیستم در زمینه محیطی و عملیاتی خود تحلیل می شود تا تمامی راه های واقعی که منجر به بروز این رویداد نامطلوب ( رویداد رأس[1] ) می شود ، کشف گردد .

**درخت خطا مدل گرافیکی از ترکیبات سری و موازی خطا هایی است که باعث وقوع رویداد ناخواسته از پیش تعریف شده ای می گردد** . خطا ها ممکن است رویداد هایی باشند که مرتبط با شکست سخت افزاری قطعات ، خطا های انسانی ، و یا هر رویداد دیگری باشد . بنابراین درخت خطا ارتباط منطقی رویداد های پایه ای که منجر به رویداد رأس می شوند را ترسیم می کند . نکته قابل توجه این است که درخت خطا به تنهایی یک مدل کمی نیست ، بلکه یک مدل کیفی است که می توان ( و اغلب چنین است) آن را بطور کمی ارزیابی نمود .

خروجی درخت خطا در اصل یک رویداد دودوئی[2] است ، یعنی به دو حالت شکست یا موفقیت ، خلاصه می شود. شناسه های[3] درخت خطا گیت هایی[4] هستند که منطق جاری در درخت را مشخص می کنند . گیت ها ارتباط منطقی بین رویداد های پایین دست ( ورودی گیت) و بالادست(یعنی خروجی گیت) معلوم می کند . تصویر ۱-۱ یک درخت خطای ساده را نشان می دهد .

[1] Top Event
[2] Binary
[3] Entities
[4] Gates




تصویر ۱-۱ : مثالی ساده از یک درخت خطا

### ۱-۳) ارزیابی کمّی و کیفی درخت خطا

هر دو ارزیابی کمی و کیفی را می توان بر روی درخت خطا انجام داد . درخت خطا (FT )به خودی خود یک ارزیابی کیفی از رویداد هایی است که منجر به رویداد رأس می شوند. هنگام تشکیل FT ، بینش و درک قابل توجه ای از علل وقوع رویداد رأس بدست می آید و هر چه بیشتر بر روی این علل و ارتباط آنها دقت شود ، اطلاعات بدست آمده دقیق تر و با ارزش تر می گردد .

در ارزیابی های کمّی ، منطق حاکم بر FT به شکل منطق عددی در می آید که اطلاعات متمرکزتری را بدست می دهد . نتایج اصلی که حاصل می شود ، مجموعه برش های حداقل[1] (MCSs) رویداد رأس می باشد . یک مجموعه برش[2] ، ترکیبی از رویداد های پایه است که

[1] Minimal Cut Sets
[2] Cut Set

منجر به وقوع رویداد رأس می شوند و یک مجموعه برش حداقل ، ترکیبی حداقل از این مجموعه است . رویداد های پایه ، رویداد های انتهایی درخت هستند . بنابراین MCS ها ، تمامی مسیرهای منتهی به وقوع رویداد رأس را مشخص می کنند .

مجموعه MCS ها را نه تنها برای رویداد رأس ، بلکه برای رویداد های میانی ( یعنی رویداد های گیت ) نیز می توان بدست آورد . از ساختار MCS ها ، می توان حجم اطلاعات قابل توجه ای را کسب کرد . هر MCS که تنها یک رویداد پایه داشته باشد ، نشان دهنده یک شکست یا رویداد **منفرد** است که به تنهایی منجر به وقوع رویداد رأس می گردد . این شکست های منفرد اغلب پیوندهای ضعیفی هستند که بایستی هدف اقدامات پیشگیرانه قرار بگیرند .

مثال هایی از این قبیل شکست ها ، یک خطای انسانی منفرد یا خرابی یک قطعه خاص می باشد که باعث شکست سیستم شود . یک مجموعه برش حداقل که شامل رویداد هایی با مشخصات یکسان باشد ، نشان دهنده آمادگی سیستم برای شکست های وابسته یا **علت مشترک**[1] است . مثالی از این نوع MCS ، شکست شیرهای یکسان[2] می باشد . یک نقص[3] مشترک در قطعات یک کارخانه ، یا یک حساسیت محیطی[4] منفرد (مثلاً حساسیت تجهیزات یکسان به درجه حرارت بالا) می تواند باعث شود تا تمامی قطعات بطور همزمان دچار شکست گردند .

ارزیابی کمی درخت خطا شامل تعیین احتمال وقوع رویداد رأس و میزان اهمیت[5] و نقش رویداد های پایه در بروز رویداد رأس می باشد . همچنین می توان عدم قطعیت ها را در هر یک از نتایج کمی حاصله بدست آورد . درخت خطا با محاسبه احتمال هر یک از مجموعه برش

[1] Common Cause
[2] Identical valves
[3] Defect
[4] Environmental sensitivity
[5] Importance

های حداقل و جمع نمودن تمامی احتمالات محاسبه شده ، کمی می شود. سپس مجموعه برش ها بر حسب عدد احتمال خود دسته بندی می شوند . مجموعه برش هایی که سهم عمده تری در احتمال رویداد رأس دارند ، مجموعه برش های غالب[1] نامیده می شوند . گرچه محاسبه احتمال رویداد رأس ، هدف اصلی تحلیل می باشد اما احتمال هر یک از رویداد های میانی را نیزمی توان محاسبه نمود . همچنین علاوه بر مقدار احتمال رویدادها ، احتمالات وابسته به زمان[2] ، نظیر تابع توزیع احتمال[3] رویداد رأس ، تواتر بروز رویداد رأس ، نرخ شکست[4] رویداد ها و میزان دسترسی[5] ، از جمله پارامترهای قابل محاسبه می باشند .

در ارزیابی کمّی درخت خطا علاوه بر شناسایی مجموعه برش ها ، میزان اهمیت رویداد های پایه ، رویداد های میانی و برش های حداقل نیز بدست می آید ، البته در کاربردهای مختلف ، معیارهای متفاوتی برای تعیین اهمیت وجود دارد . یکی از این معیارها تعیین سهم هر رویداد در احتمال رویداد رأس است . معیار دیگر میزان کاهش احتمال بروز رویداد رأس در اثر پیشگیری از وقوع یکی از رویداد ها است . معیار سوم افزایش احتمال وقوع رویداد رأس در اثر وقوع حتمی (با عدد احتمال یک) یکی از رویداد ها است . کاربرد اصلی این معیارها در اولویت بندی منابع ، طرح ریزی اقدامات پیشگیرانه ، ارتقاء فعالیت ها و در فعالیت های تعمیر و نگهداری می باشد .

[1] Dominant
[2] Time-related
[3] Probability distribution
[4] Failure rate
[5] Availability

### ۱-۴ درخت موفقیت ، مکمل منطقی درخت خطا

به دلیل ارتباط بین موفقیت و شکست ، درخت خطا را می توان به راحتی به مکمل منطقی آن یعنی درخت موفقیت تبدیل کرد . دیدیم که درخت خطا در ابتدای کار ، یک رویداد ناخوشایند را هدف قرار داده و آن را رویداد رأس می نامد . حال اگر رویداد رأس این سیستم به شکل عدم شکست تجهیز ، تعریف شود ، تبدیل به یکی از حالت های موفقیت سیستم می شود . در واقع عدم رخداد رویداد رأس یک درخت خطا ، رویداد رأس یک درخت موفقیت خواهد بود( روش تبدیل FT به ST ، در بخش بعد خواهد آمد).

به عنوان مثال اگر رویداد رأس یک FT ، دیر رسیدن به محل کار باشد ، رویداد رأس درخت موفقیت معادل آن ، به موقع رسیدن به محل کار خواهد بود . از طرفی ، مشاهده کردید که مجموعه ای حداقل از رویداد که رخداد آنها به وقوع رویداد رأس ختم شود ، برش های حداقل نامیده می شوند . با همین تعبیر ، در یک ST ، مجموعه ای حداقل از رویدادها که با وقوع خود از بروز رویداد رأس جلوگیری کنند ، مسیرهای حداقل نامیده می شوند .البته به این مجموعه رویدادها ، بازدارنده های حداقل نیز می گویند چرا که با وقوع خود از وقوع رویداد رأس جلوگیری کرده و موفقیت سیستم را به ارمغان می آورند . مسیرهای حداقل حتی اگر کمّی هم نشوند ، اطلاعات ذی قیمتی در مورد راه های جلوگیری از وقوع رویداد رأس در اختیار تحلیل گران قرار می دهند . البته درخت موفقیت را هم مانند درخت خطا می توان کمّی کرده و احتمال موفقیت سیستم را محاسبه نمود. خواننده می تواند برای مشاهده یک مثال از درخت موفقیت و ارتباط آن با درخت خطا ، به ضمیمه **د** مراجعه نماید .

### ۱-۵) نقش FTA در تصمیم گیری

اطلاعات متنوعی از FTA حاصل می شود که نقش بسزایی در تصمیم گیری مدیران دارد . در این بخش به بعضی از این ویژگیها اشاره می شود . البته مطالب این قسمت به نوعی مرور گفته های پیشین می باشد :

۱- **کاربرد FTA در ردیابی مسیر منطقی منتهی به وقوع رویداد رأس** : FTA یک مدل منطقی از مسیر علت های اصلی و رویدادهای میانی منتهی به رویداد رأس را پیش روی تحلیل گر قرار می دهد . با مشاهده رویدادهای خطا در این مسیر منطقی ، تحلیل کیفی درخت خطا براحتی امکان پذیر می گردد و رویدادهای منفرد مجموعه برش ها ، برجسته می شوند . در واقع می توان ادعا کرد که اطلاعات کیفی حاصل از درخت دست کمی از اطلاعات کمی بدست آمده ، نخواهد داشت .

۲- **کاربرد FTA در اولویت دهی به رویدادهایی که بیشترین سهم را در وقوع آن دارند** : مطمئناً یکی از اساسی ترین منافع حاصل از تحلیل درخت خطا در یافتن رویدادهایی است که بالاترین نقش را در بروز رویداد رأس دارند . اگر درخت خطا کمی شود ، رویدادهای پایه و قطعاتی که میزان اهمیت بیشتری دارند ، مشخص شده و می توان آنها را به ترتیب درصد سهم شان در بروز رویداد رأس ، اولویت بندی نمود . بر اساس تجربه ، تنها ۱۰ تا ۲۰ درصد از رویدادهای پایه پر اهمیت و قابل توجه هستند . از مزایای اولویت بندی رویدادها ، تخصیص حسابگرانه هزینه ها است . با شناسایی قطعات ، تجهیزات و سیستم های بحرانی و دردسرآفرین ، براحتی می توان هزینه ها را به منظورکاهش و یا حذف این رویدادها ، متمرکز نمود و از صرف آنها در بخش های غیر ضروری پرهیز کرد . بدین ترتیب علاوه بر کاهش هزینه ها ، احتمال بروز رویداد نامطلوب نیز کاهش خواهد یافت .

۳- **کاربرد FTA به عنوان یک ابزار پیش فعال[1] در پیشگیری از وقوع رویداد رأس** : تحلیل درخت خطا ، اغلب در شناسایی مناطق آسیب پذیر مورد استفاده قرار می گیرد . بدین ترتیب می توان قبل از بروز حادثه در این مناطق مستعد آسیب پذیر ، اقدامات اصلاحی و پیشگیرانه را طراحی نمود . بدین شکل ، می توان از همان ابتدای طراحی سیستم ، ابتکار عمل را بدست گرفت و سطح ایمنی آن را ارتقاء داد . همچنین گروه اجرایی ، با ارائه نتایج حاصل از تحلیل ، توجیه خوبی در طرح و اجرای اقدامات اصلاحی خواهد داشت .

۴- **کاربرد FTA به عنوان ابزار نظارتی عملکرد سیستم** : به علت ویژگی منحصر به فرد FTA ، می توان از آن در پایش سیستم ، بهره برد . آنچه که مسلم است با گذشت زمان و بروز برخی تغییرات اجتناب ناپذیر در سیستم و از طرفی فرسوده شده تدریجی تجهیزات ، احتمال شکست آنها افزایش خواهد یافت . با استفاده از درخت خطای موجود و ورود اطلاعات جدید ، احتمال وقوع رویداد رأس مجدداً محاسبه شود و تغییرات عددی آن مورد ارزیابی قرار گیرد . بدین ترتیب با نظارت منظم بر تغییرات ، می توان برنامه مناسب جهت تعمیر یا تعویض قطعات و تغییر روش های کنترلی را از قبل طرح ریزی نمود و از افزایش احتمال وقوع رویداد نامطلوب جلوگیری کرد .

۵- **کاربرد FTA در بهینه سازی و به حداقل رساندن منابع** : به این کاربرد تحلیل درخت خطا اغلب کمتر توجه می شود . FTA نه تنها میزان اهمیت و سهم رویدادها را مشخص می کند ، بلکه رویدادهای قابل اغماض را نیز نمایان می سازد. در مورد این رویدادها ، نیازی به اختصاص بودجه و منابع نیست و گاهی بعد از اجرای تحلیل و تخصیص مجدد منابع ، مقدار آن تا ۴۰ درصد کاهش پیدا می کند .

[1] proactive

۶- **FTA به عنوان ابزار کمکی در طراحی سیستم:** بهنگام طراحی سیستم ، از تحلیل درخت خطا می توان در انتخاب طرح مناسب بهره برد. طریقه کار بدین شکل است که ابتدا فهرستی از الزامات عملکردی تهیه شده و برای هر طرح از درخت خطا جهت بررسی بهترین طرح ، که بیشترین الزامات را برآورده می سازد، استفاده می گردد . البته در صورتیکه داده های طراحی کافی نباشد ، می توان از داده های عام[1] استفاده نمود .

۷- **کاربرد FTA به عنوان یک ابزار تشخیص دهنده علل وقوع رویداد رأس و برطرف کننده آن :** این نوع کاربرد FTA ، کاملاً متفاوت با کاربردهای پیشگیرانه یا پیش فعال آن است . با بسط درخت خطا ، علل بروز رویداد رأس و رویدادهای میانی بطور تفضیلی آشکار شده و مورد تأکید قرار می گیرد . در هر مرحله از کشف علل ، می توان اقداماتی را جهت کاهش یا حذف آنها ، پیشنهاد نمود . مزیت FTA در این بخش این است که می توان از آن برای ارزیابی اثربخشی پیشنهادات مختلف بهره برد . حتی می شود جلوتر رفت و یک ارزیابی کاملاً احتمالی را پایه گذاری نمود . یعنی حتی برای قطعاتی که کمتر علت خطا می شوند نیز یک احتمال شکست در نظر گرفت . همچنین در فهرست اقدامات کاهنده ریسک ، می توان زمان های توقف[2] و یا تعمیر[3] را نیز مد نظر قرار داد .

همانطور که مشاهده گردید تحلیل درخت خطا نقش به سزایی در فرآیند تصمیم گیری دارد . از این تحلیل می توان در تمامی چرخه حیات[4] سیستم از مرحله طراحی تا توسعه و تولید ،

[1] Generic data
[2] Downtime
[3] Repair
[4] Lifecycle

استفاده نمود . با پیشروی طرح و دسترسی به داده های بیشتر ، از این روش به منظور ردیابی و بازبینی خطاها و حذف یا کاهش ریسک آنها استفاده کامل می شود .

### ۱-۶) نقش FTA در ارزیابی احتمالی ریسک[1] (PRA)

در تکنیک ارزیابی احتمالی ریسک یا PRA ، توالی رویدادها تا رسیدن به یک وضعیت نهایی[2] مدل می کند . این توالی رویدادها اغلب یک رشته حادثه نامیده می شود. به عنوان مثال توالی رویدادها از زمان وقوع یک آتش سوزی کوچک تا یک انفجار عظیم ( به این علت که سیستم های بازدارنده و حفاظتی عمل نکرده اند ) ، یک رشته حادثه تلقی می گردد . در شکل زیر یک مدل ساده از توالی رویدادها نمایش داده شده است .

مشاهده می کنید که در این مدل ، شکست یک سیستم در کنار موفقیت سیستم دیگر ، آورده شده است . این که چه سیستم حفاظتی بدرستی عمل کند یا دچار شکست شود ، وضعیت نهایی را مشخص می کند . برای کمی سازی این توالی رویدادها ، نیاز به تعیین مقادیر احتمالی رویداد آغازین و رویدادهای میانی به استثنای وضعیت نهایی داریم . البته رویدادها اغلب به هم وابسته اند ، بدین معنی که احتمال موفقیت مثلاً سیستم B در مدل بالا ، مشروط به عدم موفقیت سیستم حفاظتی A و وقوع رویداد آغازین[3] دارد . برای رویدادهایی که مستقل هستند می توان بطور مستقیم داده احتمال را از سوابق و جداول مربوطه بدست آورد . اما اهمیت تحلیل درخت خطا زمانی بارز می شود که بخواهیم مقدار احتمال یک رویداد با وابستگیهای بسیار و پیچیدگی زیاد را بدست آوریم . در این حالت این رویداد در رأس درخت قرار گرفته و با روش منطقی رو به پایین ( از کل به جزء) ، علت ها و ریشه های وقوع رویداد رأس مشخص

[1] Probabilistic Risk Assessment
[2] End state
[3] Initial Event

می گردد . سپس این درخت خاص ، کمّی می شود تا مقدار دقیق احتمال رویداد رأس معلوم گردد . با مشخص شدن تمامی مقادیر احتمال رویدادها از ابتدا تا انتها ، مقدار احتمال رخداد یک وضعیت نهایی و اغلب اسف بار سیستم تعیین می شود.بنابر این به جرأت می توان گفت ، تحلیل درخت خطا موتور ماشین ارزیابی احتمالی ریسک می باشد .

### ۱-۷) نرم افزار FTA

نرم افزارهای تجاری بسیاری برای انجام تحلیل درخت خطا ، ابداع و بسط داده شده است و هر از گاهی نرم افزار جدیدی با قابلیت های بالاتر وارد بازار می شود.برخی از این نرم افزارها صرفاً به خود روش درخت خطا می پردازند . اما نرم افزارهای جدیدی ابداع شده اند که چندین تکنیک تحلیل و ارزیابی ریسک را بصورت یکپارچه در خود دارند و تحلیل درخت خطا تنها یکی از ورودی های آنها می باشد . هدف این کتاب بررسی و معرفی تمامی نرم افزارهای مرتبط با FTA نیست چرا که شرح همه آنها مستلزم صرف صفحات زیادی از کتاب است. خواننده می تواند با یک جستجوی ساده در اینترنت به مرجع بسیاری از این نرم افزارها ، دسترسی پیدا کند.

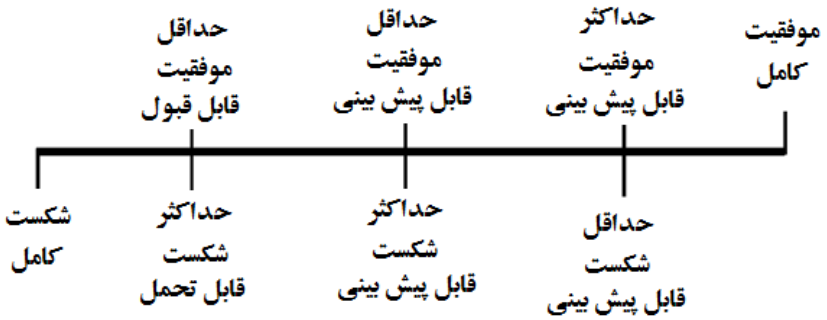
## مراجع

1. W. Vesely et al., *Fault Tree Handbook*, NUREG-0492, Nuclear Regulatory Commission, 1981.
2. K. Sullivan, J. Dugan and D. Coppit, “The Galileo Fault Tree Analysis Tool,” Proceedings of IEEE International Symposium of Fault Tolerant Computing, FTC-29, June 1999, pp 232-235.

# فصل دوم : نگرش[1] های مدل سازی منطقی سیستم

## ۲-۱ ) نگرش های شکست[2] در برابر موفقیت[3]

عملیات یک سیستم را از دو منظر می توان بررسی نمود : راه های مختلف موفقیت سیستم و مسیرهای منتهی به شکست آن. البته برای همه مسیرها ، چه شکست و چه موفقیت ، بایستی حالت های بینابین را نیز در نظر گرفت . به عنوان مثال حداقل شکست یا حداکثر موفقیت ، به ترتیب در ابتدای طیف شکست و انتهای طیف موفقیت قرار می گیرد . تصویر ۲-۱ مفهوم طیف شکست/موفقیت را نشان می دهد .




**تصویر ۲-۱ : طیف شکست/موفقیت یک سیستم**

همانطور که در این تصویر مشاهده می کنید ، هر نقطه از طیف موفقیت متناظر با نقطه ای مشابه از طیف شکست سیستم می باشد . به عنوان مثال حداقل موفقیت قابل پیش بینی همزمان با حداکثر شکست قابل پیش بینی خواهد بود . در واقع طیف موفقیت تعبیر خوش بینانه و طیف شکست تعبیر بدبینانه از سیستم است .

[1] Approach
[2] Failure
[3] Success

البته طیف شکست در بررسی سیستم ، مرزهای تحلیل را به شکل واضح تری مشخص می کند و کمتر جای بحث و جدل باقی می گذارد . به عنوان مثال در مورد یک هواپیما شاید پارامترهایی نظیر پرواز در مسافت های طولانی ( و بدون نیاز به سوختگیری مجدد )، یا پرواز سریع و در ارتفاع بالا ، جزء موفقیت های سیستم پرواز محسوب شود . حال اگر هواپیمای جدیدی وارد چرخه پروازی شود و بدلیل برخی ملاحظات اقتصادی ، تعادلی بین مزیت های آن برقرار شود و مثلاً سرعت پرواز آن از هواپیمای شرکت رقیب کمتر باشد ، شاید بحث های زیادی در مورد میزان موفقیت ، پیش بیاید . اما در صورت سقوط هواپیما ، همگان در مورد شکست کامل آن بدون هیچگونه اختلافی اتفاق نظر خواهند داشت .

از طرفی موفقیت سیستم بیشتر به راندمان ، مقدار خروجی ، میزان تولید و سهم بازار نسبت داده می شود و برای توصیف این مشخصه ها از متغیرهای پیوسته استفاده می گردد که براحتی با رویدادهای ساده ای که در طیف شکست قرار دارد (نظیر شیر باز نمی شود) مدل نمی شوند . دقت کنید رویداد شیر باز می شود(که در طیف موفقیت قرار دارد) ، می تواند شامل باز بودن مثلاً ۱ تا ۱۰۰ درصد شیر باشد که یک متغیر پیوسته است . بنابراین مدلسازی رویدادهای شکست بسیار ساده تر از مدلسازی رویدادهای موفقیت است و این مسئله ارزش طیف شکست را بیشتر نمایان می کند .

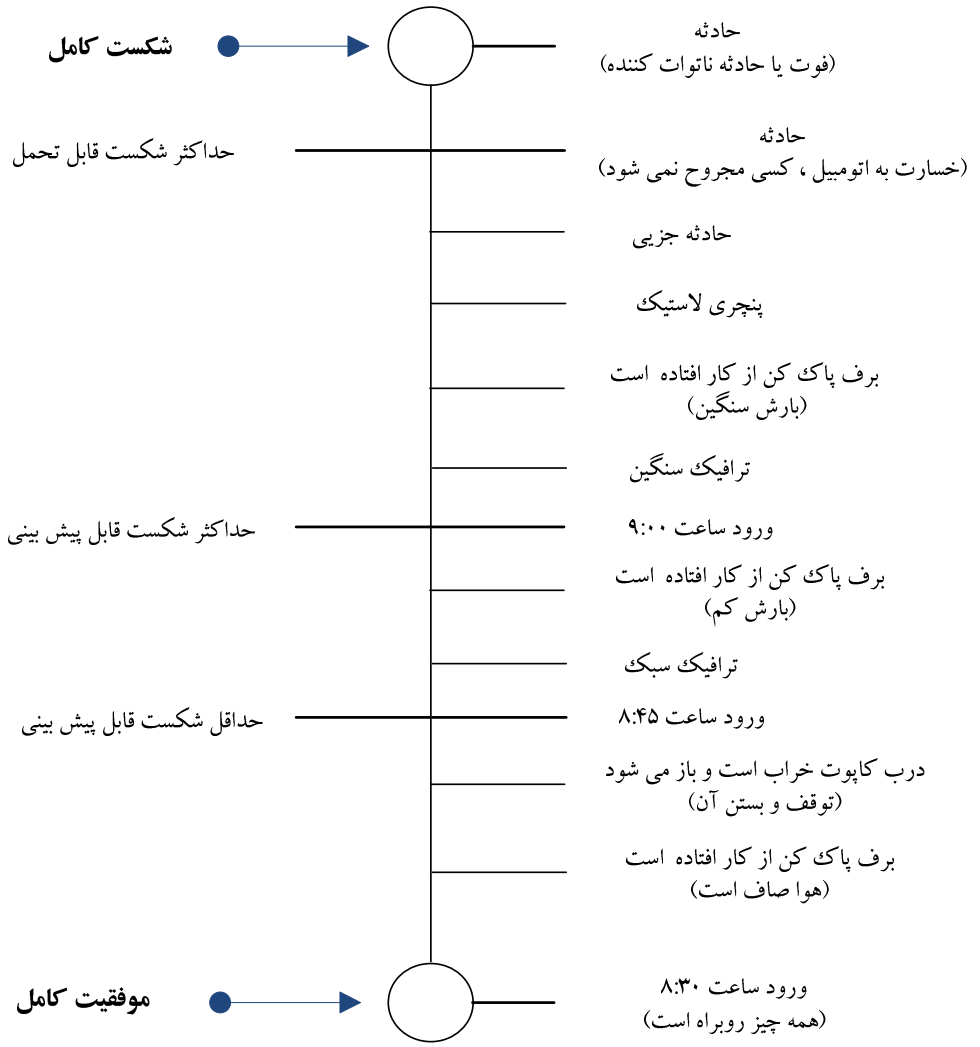
از دیگر امتیازات دیگر مدلسازی رویدادهای شکست ، این است که علیرغم وجود مسیرهای نامحدود منتهی به موفقیت یا شکست سیستم از نظر تئوری ، مسیرهای موفقیت سیستم از نظر عملی بسیار بیشتر از مسیرهای شکست است . یعنی طیف شکست عملاً باریک تر است و بهتر است برای انجام محاسبات کمتر در این طیف قرار بگیریم .

مزیت آخر طیف شکست به ماهیت محاسبات احتمال وقوع رویدادها ، بر می گردد. بیشتر مقادیر احتمال شکست بسیار کوچک هستند (کمتر از 0.1) که این مسئله به تقریب های

کارآمد و دقیق در هنگام محاسبه احتمالات ترکیبی ، کمک شایانی می کند . در حالیکه مقادیر احتمال رویدادهای موفقیت به عدد 1 نزدیک بوده و این مسئله محاسبات تقریبی را منتفی می سازد . برای همین است که محاسبه احتمال موفقیت سیستم با استفاده از مقادیر احتمال رویدادهای موفقیت (قرار گرفتن در طیف موفقیت) بسیار مشکل تر و طولانی تر است .

همانطور که بحث شد ، طیف شکست مزایای بسیاری دارد . از طرفی رسم نمودارهای منطقی موفقیت یا شکست سیستم ، مستلزم صرف وقت و هزینه است . حال اگر تعداد و اندازه این نمودارها زیاد باشد ، این موضوع نمود بیشتری پیدا می کند . به علت اینکه ، حالت های موفقیت سیستم زیاد است ، نمودارهای منطقی بسیاری برای توصیف هر یک از این حالت ها بایستی رسم شود . در صورتیکه حالت های شکست سیستم ، محدود بوده و نمودارهای کوچکتری دارد .

برای روشن تر شدن مطلب ، طیف شکست/موفقیت تصویر ۲-۲ را در نظر بگیرید .




**تصویر ۲-۲: طیف شکست/موفقیت رویداد رسیدن به محل کار**

مأموریت تعریف شده ، انتقال فرد X از خانه به اداره است . ساعت ورود مطلوب ۸:۳۰ دقیقه است ، اما ورود تا ساعت ۹:۰۰ نیز در حاشیه موفقیت قرار دارد . ورود در ساعت ۸:۳۰ ، برچسب موفقیت(عدم شکست) ، در ساعت ۸:۴۵ حداقل شکست پیش بینی شده و در ساعت ۹:۰۰ ، برچسب حداکثر شکست پیش بینی شده را دارد . ورود در فاصله ۳۰ دقیقه بین این دو ساعت نشاندهنده تأخیر نسبی است . رویدادهایی که بعد از ورود در ساعت ۹:۰۰ قرار دارند

، ممکن است تا جراحت و مرگ فرد (شکست کامل) ، امتداد داشته باشند . رویداد عدم کارایی برف  پاک کن ، بسته به شرایط محیطی ، در آن ساعت خاص تعریف می شود .

شما می توانید برای هر سیستمی ، طیفی شبیه به تصویر ۲-۲ ، رسم کنید . به عنوان مثال در صنایع نفت  ، گاز خروجی از تفکیک گرهای نفت وگاز ، به منظور استفاده بهینه به ایستگاه تقویت فشار گاز فرستاده می شود . در این ایستگاه ها علاوه بر تقویت مرحله ای فشار ، رطوبت گاز نیز گرفته می شود و خروجی ایستگاه ، گازی با فشار بالا و خشک خواهد بود . برای چنین کارخانه ای می توان حالت های شکست متفاوتی از حداقل شکست پیش بینی شده (افت فشار گاز در خروجی به اندازه $x_1$ ) ، حداکثر شکست پیش بینی شده (افت فشار گاز در خروجی به اندازه $x_2$) ، حداکثر شکست قابل تحمل (افت فشار گاز در خروجی به اندازه $x_3$ ) و شکست کامل ( از کار افتادن و توقف کامل ایستگاه) ، در نظر گرفت .

## ۲-۲)  FTA یک روش جزءگرا[1]

در روش های جزءگرا ، استدلال از کل به جزء است . در تحلیل سیستم با روش های جزءگرا و با فرض شکست سیستم (به هر طریقی) ، سعی بر این است که زیرسیستم هایی که در این شکست ، نقش داشته اند ، شناسایی شوند . روشی که در بین مردم به روش کارآگاهی مشهور است . کارآگان با توجه به شواهد و مدارک بدست آمده ، طوری آنها را با استدلال و منطق کنار هم می چینند تا به مجرم برسند .

نمونه ای از روش های جزء گرا در زندگی واقعی ، تجزیه و تحلیل حوادث است . دلیل غرق شدن کشتی تایتانیک در میانه سفر دریایی اش که تا آن زمان غرق نشدنی فرض می شد ، چه

[1] Deductive

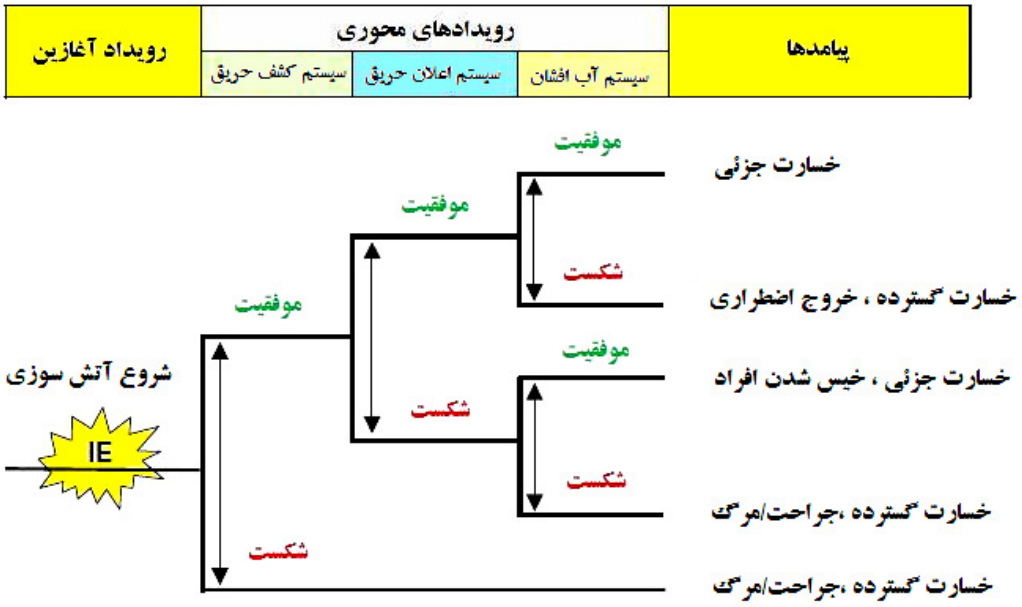
بود؟ کدامین خطاهای سخت یا نرم افزاری و حتی انسانی باعث سقوط یک هواپیما در یک منطقه مسکونی می شود؟

تحلیل درخت خطا که در این کتاب به تفضیل مورد بحث قرار می گیرد ، نمونه ای از تحلیل های جزءگراست . در این تحلیل ، همانطور که در فصل قبل گفته شد ، وضعیت نامطلوبی از سیستم در نظر گرفته شده و مسیر منطقی رویدادها (که در برگیرنده شکست زیرسیستم ها ، تجهیزات و قطعات است) تا رسیدن به علل اصلی ، دنبال می شود . از طرف دیگر در روش های کل گرا[1] ، وضعیت های شکست نهایی سیستم یا سناریوهای شکست ، مد نظر هستند . بخش بعد به شرح روش های کل گرا می پردازد .

## ۲-۳) روش های کل گرا

در این روش ها با توجه به جزییات ، کلیات نتیجه گیری می شود. به عنوان مثال در تحلیل های کل گرا یک رویداد آغازین[2] تعیین شده و عکس العمل های متفاوت سیستم در مقابله با این رویداد ، بررسی می شود. مثلاً با شروع یک آتش کوچک (رویداد آغازین) در بخشی از یک واحد فرآیندی ، پیامد های مختلفی ممکن است به وجود بیاید مورد تحلیل قرار می گیرد . در تصویر ۲-۳ سناریوهای ممکن ، در یکی از تحلیل های کل گرا (تحلیل درخت واقعه یا ETA[3] ) ، نمایش داده شده است .

[1] Inductive
[2] Initial Event
[3] Event Tree Analysis




**تصویر ۲-۳ : یافتن سناریوها در یک تحلیل کل گرا**

در واقع در روش های کل گرا در جستجوی پاسخ به سئوال **چه می شود اگر**؟ هستیم . به عنوان مثال چه می شود اگر ورودی خوراک یک واحد فرآیندی قطع شود ؟ چه می شود اگر کمپرسور بخش تغذیه هوا از کار بیفتد ؟ چه می شود اگر اپراتور متوجه آلارم سطح پایین مخزن V-200 نشود ؟ پاسخ به هر یک از این سئوالات و سناریوهایی که ممکن است بوقوع بپیوندد ، بستگی به عملکرد حفاظ های ایمنی سیستم دارد .

از نظر منطقی جهت گیری تحلیل در روش های کل گرا از پایین به بالا[1] یا رو به جلو[2] است.یعنی تحلیل گر از علت به اثر می رسد . در صورتیکه در روش های جزء گرا این منطق رو به عقب[3] است یعنی تحلیل گر از اثر به علت می رسد . از آنجاییکه تحلیل درخت خطا کاربرد وسیعی در تمامی سیستم ها دارد و محدود به یک مورد خاص نمی شود ، از این روش می توان

[1] Button Up
[2] Forwards
[3] Backwards

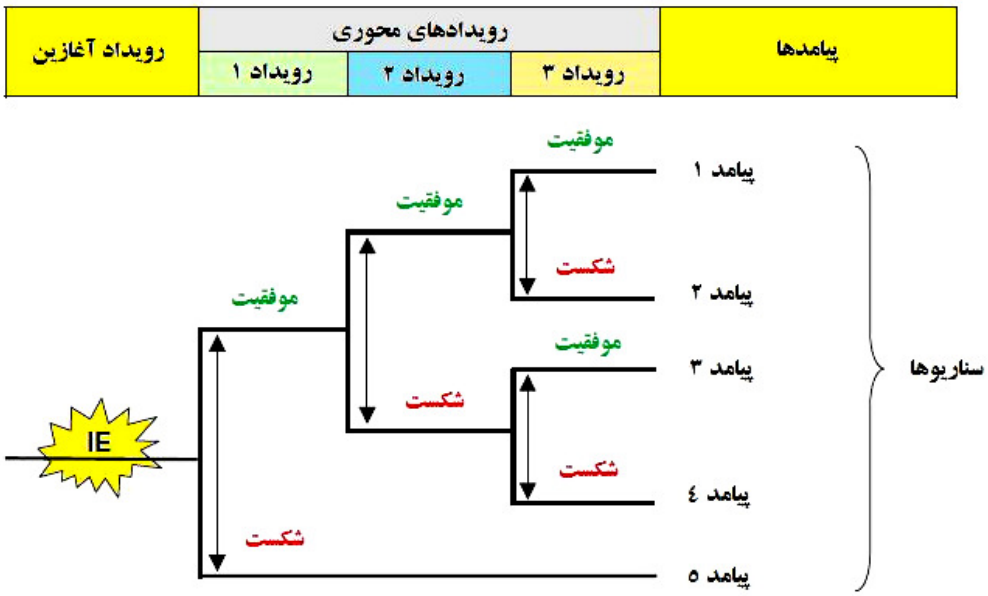
به عنوان مکمل در کنار رو ش های کل گرا استفاده کرد . مثلاً اگر در یک واحد عملیاتی HAZOP انجام شود و خروجی آن سناریوهای پر ریسک فرآیندی باشد ، می شود برای هر سناریو ، یک درخت خطا رسم نمود و مجدداً از اثر به علل برگشت . مزیت این کار این است که مقدمات ارزیابی کمّی ریسک فراهم آمده و احتمالاً اگر عللی از چشم دور مانده باشند ، پدیدار می شوند . در ادامه به شرح مختصری در مورد تحلیل درخت واقعه که ساختار آن در تصویر ۲-۳ آمده است ، می پردازیم . برای مطالعه دیگر روش ها ، می توانید به مراجع معرفی شده در بخش آخر این فصل مراجعه کنید .

## ۲-۴ تحلیل درخت واقعه (ETA)

تحلیل درخت واقعه اولین بار در مطالعات ایمنی نیروگاه های هسته ای مورد استفاده قرار گرفت . (پروژه WASH-1400 سال ۱۹۷۴) در این تحقیقات تیم پروژه بهنگام تحلیل ریسک نیروگاه ها با درخت خطاهای بزرگ و طاقت فرسایی مواجه گردید و برای مدیریت بهتر و خلاصه نمودن تحقیقات ، تحلیل درخت واقعه را ابداع کرد . تحلیل درخت واقعه ، تکنیکی است قوی و ساختار یافته که از جبر بولی ، نظریه مجموعه ها و منطق ، استفاده می کند . درخت واقعه یک نمودار شاخه ای از رویدادهای آغازین است که منجر به وقوع سناریوهای متفاوتی بسته به عملکرد پادمان[1] های موجود در سیستم می گردند .

رویداد های آغازین می توانند رویدادهای مخاطره آمیز(رویداد رأس یک درخت خطا) و یا هر رویداد نامطلوب دیگری باشند که سبب شروع یک اغتشاش ( مثلاً آتش سوزی) در سیستم شوند . در تصویر ۲-۴ ساختار منطقی یک درخت واقعه را می بینید .

[1] Safegaurd

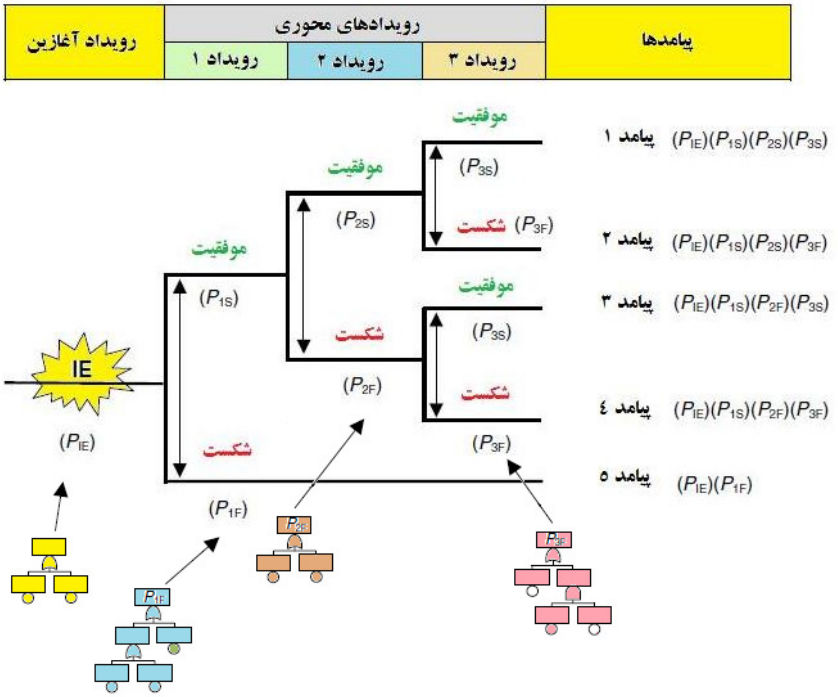



**تصویر ۲-٤ : ساختار یک درخت واقعه**

رویدادهای محوری ، رویدادهایی هستند که عکس العمل سیستم را در برابر شروع رویداد آغازین ، توصیف می کند . به عنوان مثال در تصویر ۲-۳ بعد از شروع آتش سوزی ، اولین پادمان موجود سیستم کشف حریق است ( مانند آشکارسازهای دود و حرارت که در مناطق از پیش تعیین شده نصب شده اند و به محض وقوع آتش سوزی ، مثلاً آب افشان ها[1] را بطور خودکار فعال می کنند) . اگر این سیستم از همان ابتدا ، بدلیلی متوجه آتش سوزی نشود ، بدترین سناریوی ممکن (خسارت گسترده/مرگ) ، بوقوع می پیوندد . بهترین سناریو وقتی است که تمامی سیستم های دفاعی بدرستی عمل کرده و آتش به پا شده را مهار کنند .همانطور که قبلاً گفته شد می توان از درخت خطا برای ارزیابی دقیق تر سناریوها بهره برد . حتی می شود احتمال وقوع تمامی مسیرهای شکست را با استفاده از تحلیل درخت خطا ،

[1] sprinklers

بصورت کمی ، بدست آورد . تصویر ۲-۵ ، کاربرد FTA را در تحلیل درخت واقعه نشان می دهد :




**تصویر ۲-۵ : کمّی نمودن درخت واقعه**

## مراجع

1. *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners,*NASA, Version 1.1, August 2002.

## فصل سوم : جایگاه تحلیل درخت خطا در ارزیابی ریسک

در فصل اول گفته شد که تحلیل درخت خطا یک روش ارزیابی ریسک کیفی است که به دلیل ساختار منطقی براحتی کمّی می شود . البته این کار زمانی انجام می شود که تحلیل گران اطلاعات کافی در مورد نرخ و احتمال شکست تجهیزات ، جمع آوری کرده باشند .

به دلیل ماهیت جزء گرای این تکنیک ، بهتر است قبل از انجام آن ، از روش های دیگری استفاده شود تا سیستم به شکل کلان دیده شود . نمونه ای از این روش ها ، تکنیک **شناسایی مخاطرات** یا **HAZID** [1] است . در این تکنیک عوامل بالقوه آسیب رسان[2] سیستم یا کارخانه با با استفاده از روش های مختلف ، نظیر تهیه چک لیست ، کد و استاندارد ، تجربیات موجود یا دیگر روش های ساختار یافته ، شناسایی می گردد . سپس عوامل شناسایی شده در برگه های مخصوص به همراه اطلاعات دیگری از قبیل پیامد حاصل از عامل (مخاطره) ، علت بوجود آمدن پیامد ، پادمان[3] های موجود ، سطح ریسک ، شرح اقدامات کاهنده ریسک ، فرد (سازمان) مسئول پیگیری اقدامات و سطح ریسک بعد از انجام اقدامات ، آورده می شود .البته روش فوق کیفی بوده و تنها بخش محاسباتی آن ، تعیین سطح ریسک (حاصلضرب احتمال وقوع در شدت پیامد ) می باشد که حالت نیمه کمّی به آن می بخشد . مراحل انجام HAZID از ابتدا تا انتها توسط گروهی از کارشناسان ، متخصصین و پرسنل مجرب سیستم و با استفاده از تکنیک خردجمعی[4] انجام می پذیرد .

بعد از اجرای HAZID و ثبت نتایج آن ، توجه گروه متخصصین به سمت راهکارهایی جهت کاهش یا حذف ریسک های برجسته (ریسک هایی که در ناحیه غیر قابل قبول یا غیر قابل

[1] **HAZ**ard **ID**entification
[2] Hazards
[3] Safeguard
[4] Brain Storming

تحمل قرار می گیرند ) معطوف می گردد . طبیعی است بـرای کـاهش انـدازه یـک کمیـت دو بعدی نظیر ریسک ، می توان به کاهش هر یک از ابعاد آن فکر کرد . در این مرحلـه اسـت کـه تحلیل درخت خطا به عنـوان یـک تکنیـک قـوی و کارآمـد وارد فرآینـد شناسـایی و ارزیـابی مخاطرات می شود .

این تکنیک ، بُعد احتمال ریسک را هدف قرار می دهد . پیامد پر ریسک شناسایی شده کـه در HAZID به آن رویداد مخاطره آمیز[1] می گویند ، این بار بـا نـام **رویـداد رأس** در بـالاترین نقطه درخت خطا قرار می گیرد و با جزییات بیشتری به آن پرداخته می شود . در واقـع FTA به ما کمک می کند تا راه های کاهش احتمال وقوع یک رویداد مخاطره آمیـز را بیـابیم و بعـد نتایج حاصله را به تکنیک بالا دست (HAZID ) ارجاع دهیم .

همانند دیگر روش های ارزیابی ریسک ، FTA نیز مراحل انجام مخصوص به خـود را دارد . البته این روش ها ، اغلب مراحل مشترکی دارند . به عنوان مثال شناسایی سیستم تحت مطالعه و بررسی اقدامات اصلاحی ، بین تمامی روش ها مشـترک اسـت . در ادامـه بـه شـرح مختصـر مراحل انجام تحلیل درخت خطا می پردازیم :

### ۳-۱) مراحل انجام تحلیل درخت خطا

یک FTA موفق بایستی مراحل زیر را به دنبال داشته باشد:

**۱- شناخت سیستم :**

در این مرحله سیستم تحت مطالعه به عنوان یک بلوک در نظر گرفته شده و ابتدا ورودی ها و خروجی های آن مشخص می گردد . مثال هایی از ورودی ها ، مسیر های خوراک[2] ، سرویس

[1] Hazardous Event
[2] Feed

های جانبی[1] ، محصولات میانی ، محصولات فرعی و افزودنی ها[2] و خروجی ها شامل مواردی مانند محصول[3] ، محصولات میانی یا جانبی و پسماند می باشد . سپس فرآیندی که در سیستم برای رسیدن به محصول وجود دارد شرح داده می شود . این فرآیند شامل شرح وظایف و نوع تجهیزات و ادواتی است که مستقیماً در تولید نقش دارند . البته در ابتدای کار نیازی به شرح و بسط کامل فرآیند نیست و تنها جریان مواد[4] بررسی می شود . بدین منظور می توان از نقشه جریان مواد واحد استفاده نمود .

**۲- انتخاب بخشی از سیستم :**

در این مرحله بخشی از سیستم که بر اساس به تجربه و سوابق دارای اشکال یا نقص است ، انتخاب می گردد . این انتخاب همچنین می تواند بر اساس کاهش شدت پیامدهای حاصل از بروز رویداد های مخاطره آمیز در بخش فوق باشد . در این مرحله معیار تصمیم گیری بایستی شرح داده شود .

**۳- تعیین رویداد نامطلوب :**

در بخش انتخاب شده یک رویداد نامطلوب که دارای عدد ریسک بالا بوده و وقوع آن آثار خسارت باری را بر روی سیستم می گذارد ، بطور دقیق مشخص می گردد و رویداد رأس نامیده می شود . البته همانطور که در مقدمه این بخش گفته شد ، تعیین این رویداد ممکن است از طریق یکی از روش های شناسایی عوامل بالقوه آسیب رسان مانند HAZID ، صورت پذیرد .

[1] Utility
[2] Additives
[3] Product
[4] Process Flow

**۴- رسم درخت خطا :**

در این مرحله با استفاده از گیت های منطقی و مجموعه ای از قواعد پایه ، درخت خطای مرتبط با رویداد رأس تعیین شده در مرحله قبل ، رسم می گردد . بدین منظور در ابتدا رویداد هایی که بی واسطه و بلافصل منجر به رخداد رویداد رأس می شوند ، تحت عنوان رویداد های فرعی فهرست شده و در ساختار درخت قرار می گیرند . سپس روند یافتن علل رویداد ها تا رسیدن به رویداد های پایه (رویدادهایی که به دلیل نداشتن اطلاعات و یا قرار گرفتن در بیرون مرزهای تحلیل ، بسط داده نمی شوند ) ، ادامه پیدا می کند

**۵- مشخص نمودن مجموعه برش های حداقل[1] :**

بعد از رسم درخت خطا ، با استفاده روش های ریاضی ( نظیر جبر بولی ) یا روش های گرافیکی ( مانند روش گیت ها ) ، برش های حداقل مشخص شده و رویداد رأس بر حسب حاصل جمع این برش ها نوشته می شود .

**۶- محاسبه احتمال وقوع رویداد رأس :**

در این مرحله با استفاده از اطلاعات و جداول مربوط به نرخ شکست تجهیزات و ادوات و نیز داده های مربوط به خطاهای انسانی ، احتمال وقوع رویداد رأس محاسبه می گردد .

**۷- تعیین سطح ریسک[2] :**

در این مرحله سطح ریسک با استفاده از حاصلضرب احتمال وقوع رویداد رأس و شدت پیامد آن ، محاسبه می شود . ( فرض ما بر این است که شدت پیامد قبلاً با استفاده یکی از تکنیک های آنالیز پیامد یا روش های شناسایی عوامل بالقوه آسیب رسان ، معلوم شده است )

[1] Minimal Cut Set
[2] Risk Level

**۸ – ارزیابی سطح ریسک :**

اگر سطح ریسک بدست آمده در مرحله قبل با توجه به یک معیار ارزشیابی از پیش تعریف شده ( مانند ماتریس ریسک[1] ) ، در ناحیه قابل قبول قرار داشت ، نتایج تحلیل ثبت شده و به مرحله ۲ می رویم . در غیر اینصورت ، مرحله ۹ را اجرا می کنیم .

**۹ – تعیین رویدادهای فرعی :**

رویداد های فرعی که اولین دلایل بلافصل بروز رویداد رأس هستند را از درخت خطا استخراج می کنیم .

**۱۰ – رتبه بندی[2] رویدادهای فرعی :**

در این مرحله رویدادهای فرعی بر حسب مجموع برش های حداقل خود نوشته شده و احتمال وقوع هر یک محاسبه می گردد . سپس با تقسیم عدد احتمال فوق بر احتمال وقوع رویداد رأس و نوشتن جواب تقسیم بر حسب درصد ، سهم هریک از رویدادهای فرعی در رخداد رویداد رأس تعیین می گردد و به شکل نزولی در جدولی با عنوان " **رتبه بندی رویداد های فرعی** " آورده می شود .

**۱۱– تعیین رویدادهای فرعی با اولویت ( رتبه ) بالا :**

از جدول رتبه بندی مرحله قبل ، رویدادهایی که بیشترین سهم در بروز رویداد رأس را دارند ، در جدولی مجزا با عنوان " **رویدادهای فرعی با اولویت بالا** " ، فهرست می شوند .

**۱۲– رتبه بندی برش های حداقل :**

رویداد های فهرست شده در مرحله قبل ، هریک شامل مجموعه ای از برش های حداقل هستند که حاصل جمع عدد احتمال این برش ها ، احتمال بروز رویداد فرعی مورد نظر را بدست می دهد . در این مرحله با روشی شبیه به مرحله قبل ، اولین رویداد فرعی جدول از

[1] Risk Matrix
[2] Ranking

فهرست جدا شده و رتبه بندی برش های حداقل آن در جدولی تحت همین عنوان آورده می شود . این عمل برای رویدادهای فرعی که عناوین بعدی را دارند تکرار می شود . البته تعداد رویداد های انتخابی ، بستگی به مجموع سهم آنها در وقوع رویداد رأس دارد . به عنوان ممکن است جمع رویدادهای فرعی با سهم ۷۰ درصد ، معیاری برای انتخاب آنها باشد .

**۱۳ – بررسی پادمان ها / تحلیل سیستم :**

در این مرحله با استفاده از جداول ثبت شده در مرحله قبل ، با شروع از اولین برش حداقل که در صدر جدول اولین رویداد فرعی قرار دارد ، به بررسی رویداهای پایه آن برش می پردازیم . به دلیل اینکه رویدادهای پایه عموماً شامل شکست تجهیزات و یا پادمان های موجود می باشد ، توجه ما به کاهش نرخ شکست آنها معطوف می شود . در این مرحله بهره گیری از خرد جمعی و نظرات کارشناسی متخصصین عضو تیم FTA ، همچنین استفاده از روش های مهندسی تحلیل حالت های شکست قطعات ( مانند تکنیک FMEA ) و تحلیل لایه های حفاظتی [1]، می تواند بسیار سودمند باشد .

**۱۴ – بررسی اقدامات اصلاحی :**

اقدامات اصلاحی پیشنهاد شده برای کاهش نرخ شکست تجهیزات و پادمان ها ( و در نتیجه کاهش وقوع احتمال رویداد رأس ) ، در این مرحله مورد بررسی قرار گرفته و در برگه ای با عنوان **" اقدامات اصلاحی "** ثبت می گردد . در این برگه علاوه بر ثبت اقدام ، چگونگی پیگیری انجام آن نیز مشخص می گردد .

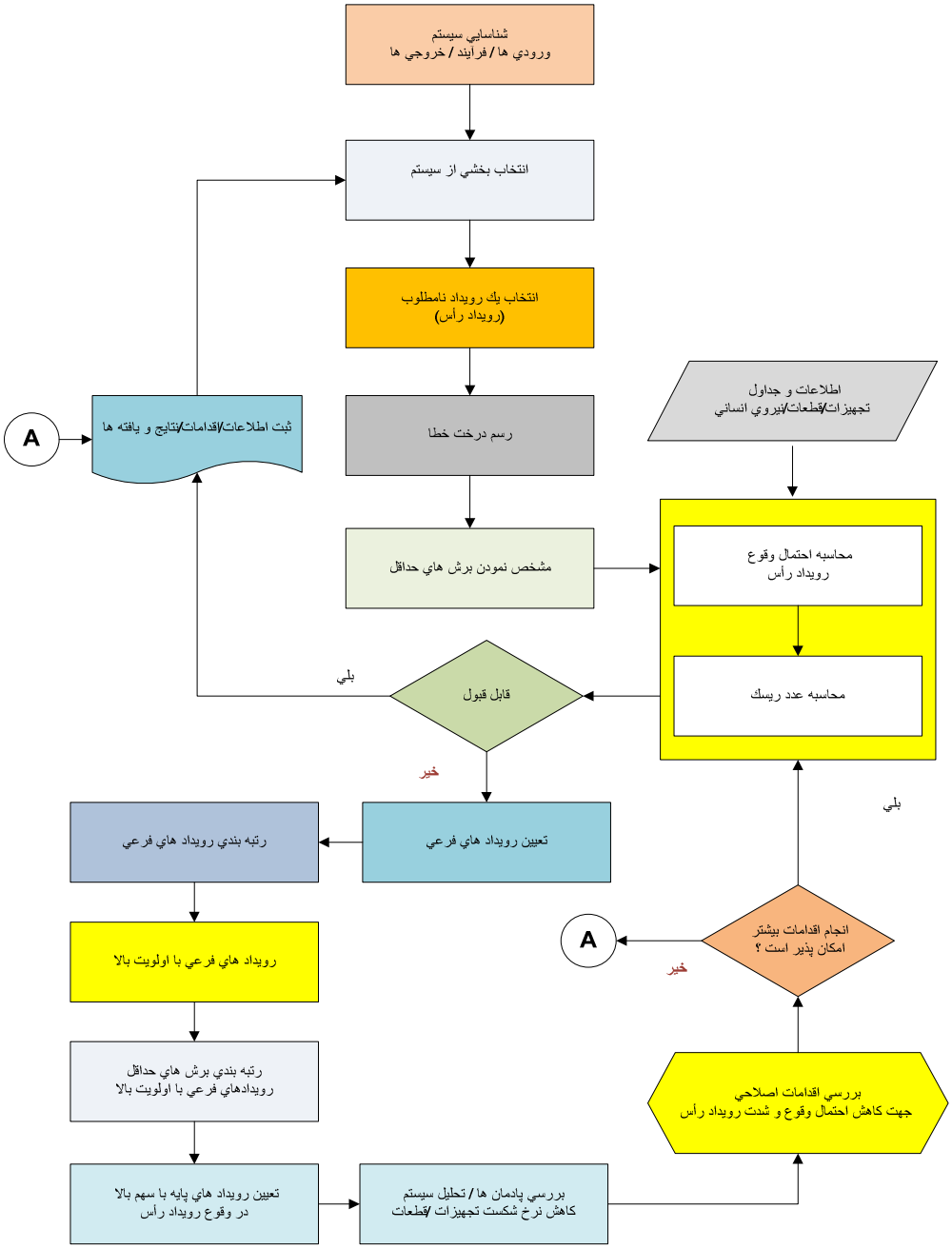
**۱۵ – بررسی امکان انجام اقدامات بیشتر :**

برای اینکه چرخه پایش اقدامات و تحلیل درخت خطا ، در نقطه ای قابل قبول پایان پذیرد ، در این مرحله امکان انجام اقدام بیشتر مورد بررسی قرار می گیرد . در صورتیکه این امکان با

[1] Layer Of Protection Analysis=LOPA

توجه به شرایط و معیار های موجود ، وجود نداشته باشد به مرحله ثبت نتایج / یافته ها و اقدامات اصلاحی می رویم . در غیر اینصورت مرحله ۷ اجرا می شود .

تصویر ۳-۱ مراحل انجام درخت خطا را نشان می دهد .




**تصوير ۳-۱ : مراحل انجام تحليل درخت خطا**

### ۳-۲) تفاوت بین خطا و شکست

لازم است تفاوتی بین خطا[1] و شکست[2] قائل شویم . برای روشن شدن این تفاوت به عنوان مثال یک رله الکتریکی را در نظر بگیرید . حالت موفقیت رله این است که با اعمال ولتاژ مناسب به آن، کنتاکت‌های آن بسته شود. اگر رله بدلیل عیب و نقص داخلی با اعمال این ولتاژ بسته نشود می‌گوییم رله دچار شکست شده است. در حالت دیگر اگر رله سالم باشد اما کنتاکت‌های آن بدلیل دریافت یک سیگنال ناخواسته در زمان نامناسب بسته شود، می‌گوییم رله دچار خطا شده است. روشن است هر شکست خطا نیز هست ولی هر خطایی شکست نیست. تعریف مناسب خطا نیاز به مشخص کردن وضعیت نامطلوب دستگاه و زمان وقوع آن دارد و بایستی وضعیت نامطلوب آن را با **"چگونه"** [3] و زمان وقوع این وضعیت را با **"چه وقت"**[4] مشخص نمود.

### ۳-۳) مکانیزم، حالت و آثار شکست

در تشکیل درخت خطا، مفاهیم بنیادی مکانیزم، حالت و آثار شکست در تعیین روابط بین رویدادها، اهمیت خاصی دارد. منظور از آثار شکست این است که شکست چه آثاری بر روی سیستم گذاشته است. حالتهای شکست، شکست‌های مختلف یک قطعه یا سیستم را بیان می‌کند.

از طرف دیگر مکانیزم شکست ، تمامی حالتهای شکست یک سیستم را دربرمی‌گیرد. به عنوان مثال سیستمی را در نظر بگیرید که وظیفه رساندن سوخت به یک موتور را دارد. می‌توان رویدادهای مختلفی از زاویه سیستم،زیرسیستم و قطعه در نظرگرفت. درجدول ۳-۱ چند

1. Fault
2. Failure
3. What
4. When

رویداد مربوط به شیر سوخت رسان آورده شده است . در اینجا شیر و عمل کننده آن جزئی از زیر سیستم هستند. ملاحظه می‌شود که مثلاً باز نشدن شیر برای زیرسیستم، مکانیزم شکست، برای شیر یک حالت شکست و آثار آن روی عمل کننده شیر دیده می‌شود.

**جدول۳ -۱) مثالی از مکانیزم، حالت و آثار شکست**

| Description<br>شرح رویداد | System<br>سیستم | Subsystem<br>زیرسیستم | Valve<br>شیر | Actuator<br>عمل‌کننده شیر |
|---|---|---|---|---|
| **سوخت به شیر سوخت‌رسان نمی‌رسد** | مکانیزم شکست | حالت شکست | آثار شکست | |
| **شیر باز نمی‌شود** | | مکانیزم شکست | حالت شکست | آثار شکست |
| **گیر کردن ساقه شیر** | | | مکانیزم شکست | حالت شکست |
| **خوردگی ساقه عمل‌کننده شیر** | | | | مکانیزم شکست |

## مراجع


۱- مستند " راهنمای شناسایی عوامل بالقوه آسیب رسان (HAZID) " ، مدیریت HSE شرکت ملی نفت ایران.

۲- مستند " متدولوژی شناسایی عوامل بالقوه آسیب رسان(HAZID) " ، مدیریت HSE شرکت ملی نفت ایران.

3. BS EN ISO 17776: 2002, Petroleum and natural gas industries offshore production installations-Guidelines on tools and techniques for hazard identification and risk assessment.

# فصل چهارم : مدلسازی درخت خطا

## ۴-۱) نماد شناسی[1] : بلوک های سازنده درخت خطا

یک نمونه درخت خطا در تصویر ۴-۱ آورده شده است . در این تصویر از نمادهایی استفاده شده است که در ادامه این بخش به توضیح آنها می پردازیم . جدول ۴-۱ شرح مختصری از نمادهای متداول در درخت خطا نشان می دهد .

**گیت[2] ها :**

دو نوع گیت پایه در درخت خطا وجود دارد : گیت AND [3] و گیت OR [4]

انواع دیگر گیت ها حالت های خاصی از این دو نوع گیت پایه هستند .

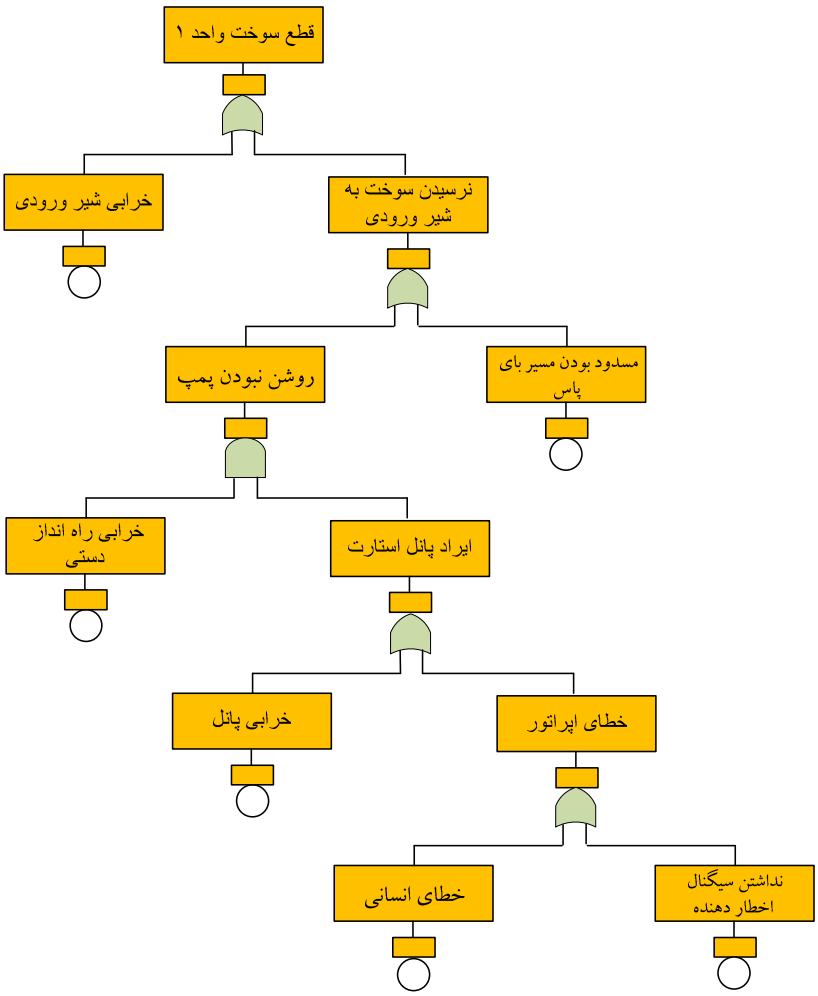
---

[1] symbology

[2] واژه Gate در فارسی ترجمه های متفاوتی بسته به کاربرد کلمه و موضوع دارد. در مدارات الکترونیکی به معنای درگاه استفاده شده است . در کاربردهای دیگر ترجمه های دریچه ، مدخل ، دروازه ، ورودیه و دربزرگ را برای این کلمه داریم . در این کتاب از گیت که بیشتر رایج است ، استفاده کرده ایم .(مترجم)

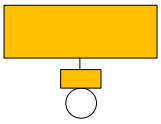
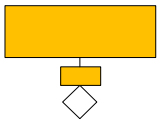
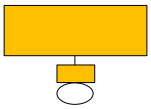
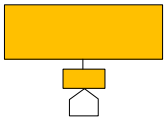
[3] **و** منطقی

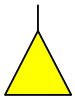
[4] **یا** منطقی



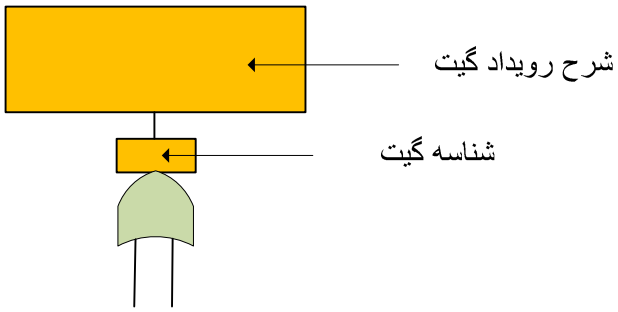

تصویر۴-۱: نمایی از یک درخت خطا

## جدول ٤-١ : نوع رویداد ها در یک درخت خطا

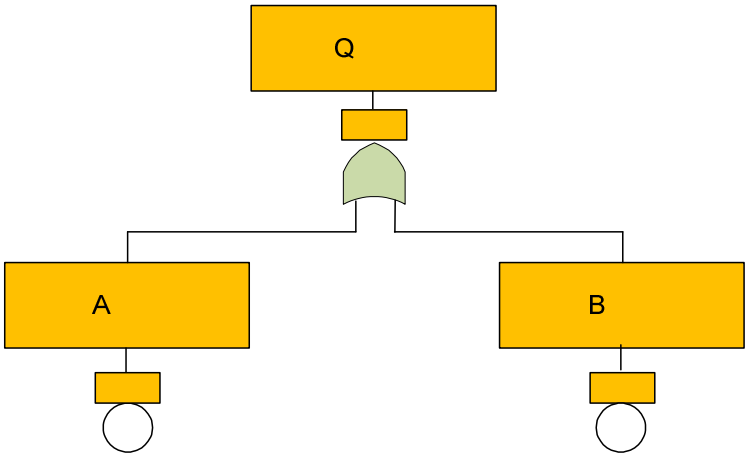
| شرح رویداد | نماد رویداد |
|---|---|
| **رویداد پایه :** یک خطای آغازین پایه که نیازی به توسعه بیشتر آن نیست . |  |
| **رویداد بسط نیافته :** رویدادی که بدلیل عدم دسترسی به اطلاعات و یا بدلیل نارسا بودن پیامدها بسط داده نمی شود . |  |
| **رویداد شرطی :** شرایط خاص یا محدودیت هایی که به هر گیت منطقی اعمال می شود . |  |
| **رویداد خانه :** رویدادی که انتظار می رود در شرایط عادی ، حتماً اتفاق بیفتد . |  |
| **شرح گیت** | **نماد گیت** |
| AND (**و** منطقی): خطای خروجی وقتی رخ می دهد که تمامی خطاهای ورودی همزمان اتفاق بیفتند. |  |
| OR (**یا** منطقی): خطای خروجی وقتی رخ می دهد که حداقل یکی از خطاهای ورودی رخ بدهد. |  |
| COMBINATION (ترکیب): خطای خروجی وقتی اتفاق می افتد که n تا از خطاهای ورودی رخ بدهند. |  |
| PRIORITY AND (**و** همراه با اولویت): خطای خروجی وقتی اتفاق می افتد که تمامی خطاهای ورودی به ترتیب خاصی رخ بدهند. |  |
| EXCLUSIVE OR (**یا** انحصاری): خطای خروجی وقتی روی می دهد که دقیقاً یکی از خطاهای ورودی رخ بدهد |  |

| شرح انتقال | نماد انتقال |
|---|---|
| TRANSFER IN (انتقال به): نشاندهنده انتقال بخشی از درخت خطا به جایی که با نماد TRANSFER OUT مشخص شده است. ( به عنوان مثال انتقال به صفحه دیگر) |  |
| TRANSFER OUT (انتقال از): نشاندهنده این است که این بخش از درخت بایستی به نماد TRANSFER IN مشابه خود متصل شود. |  |

**گیت OR**




در صورتیکه شرط وقوع رویداد خروجی گیت ، وقوع حداقل یکی از رویداد های ورودی باشد ، از گیت OR استفاده می شود . این گیت می تواند دارای تعداد ورودی های دلخواه باشد . تصویر ۴-۲ یک نمونه از گیت OR با دو ورودی را نشان می دهد .




**تصویر ٤-٢ : گیت OR**

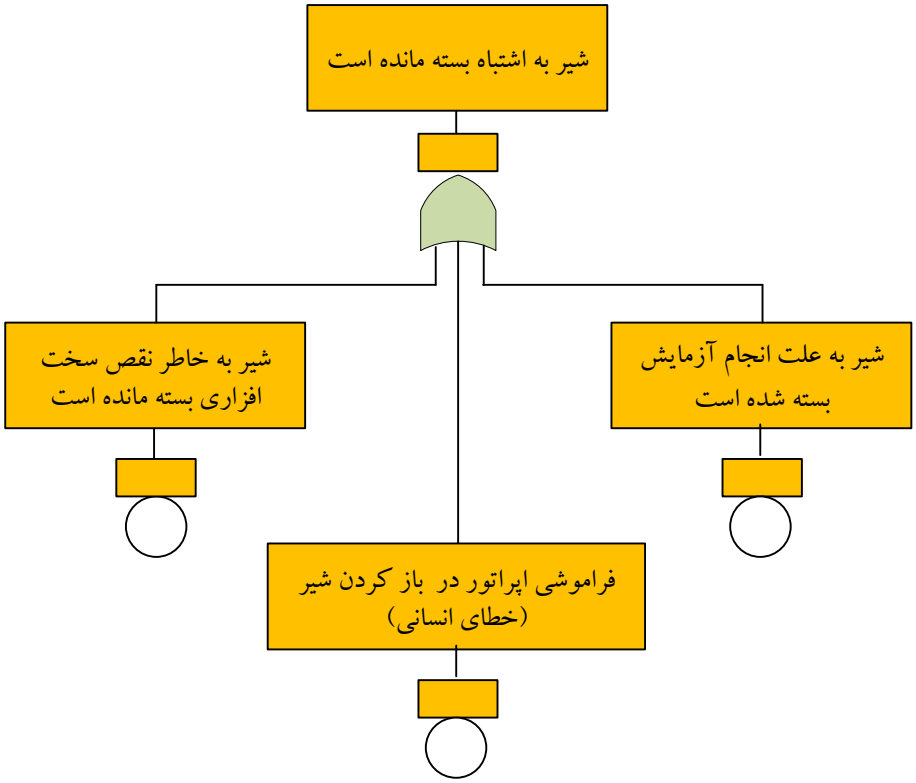
در این تصویر رویداد خروجی Q در صورتی رخ می دهد که :

رویداد A اتفاق بیفتد .

رویداد B اتفاق بیفتد .

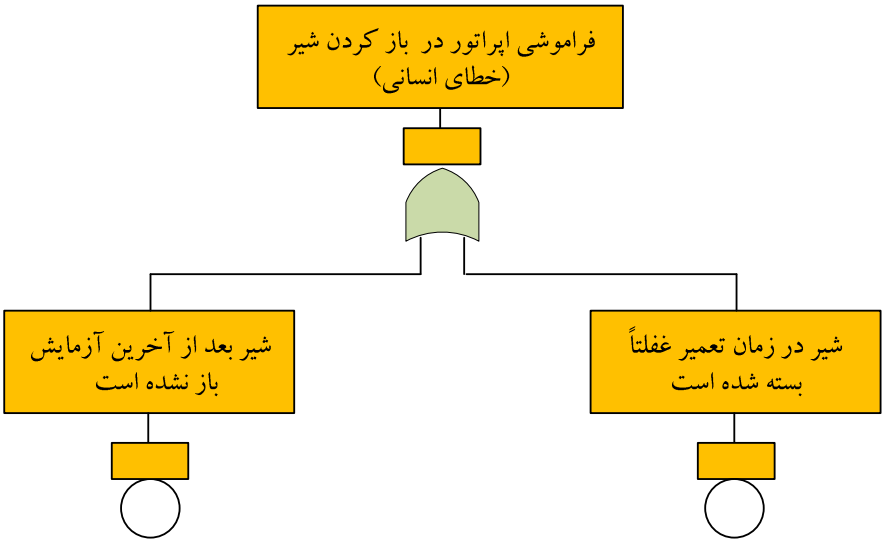
رویداد A یا B اتفاق بیفتد .

تصویر ۴-۳ مثالی از کاربرد گیت OR را نشان می دهد :



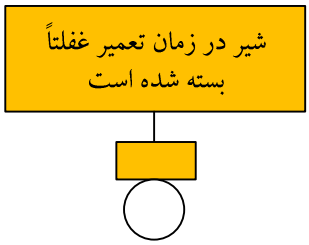

**تصویر ٤-۳ : مثالی از کاربرد گیت OR**

رویداد های فرعی تصویر ۴-۳ را می توان توسعه داد . برای نمونه تصویر ۴-۴ را ببینید :

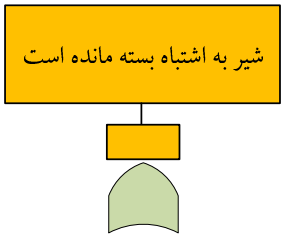



**تصویر٤-٤ : بسط رویداد مربوط به خطای انسانی**

بهر حال رویداد ،

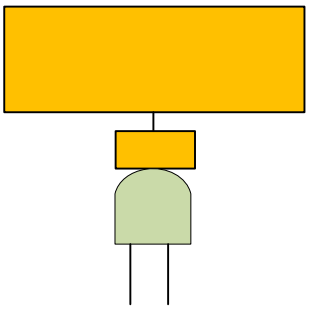



به عبارتی بیان دیگری از رویداد خروجی اولین گیت OR ، یعنی :

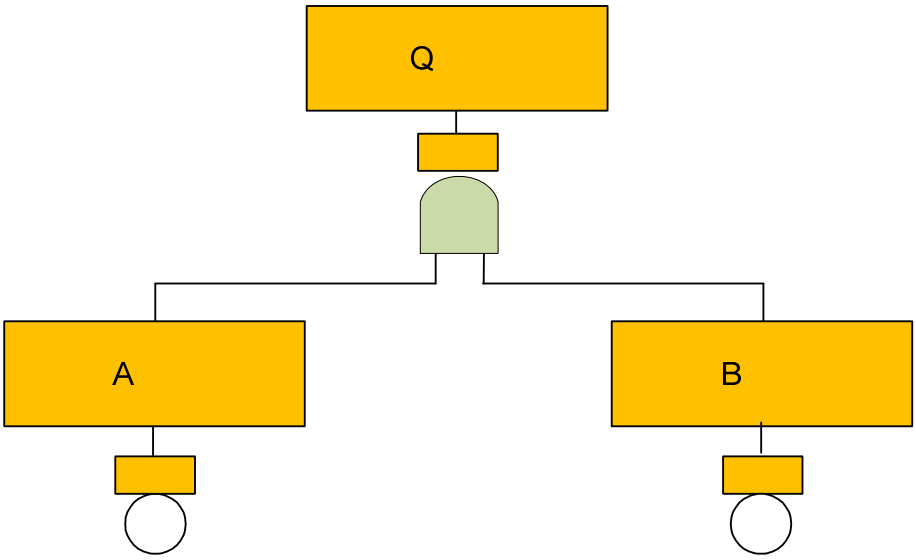



می باشد .

**گیت AND**

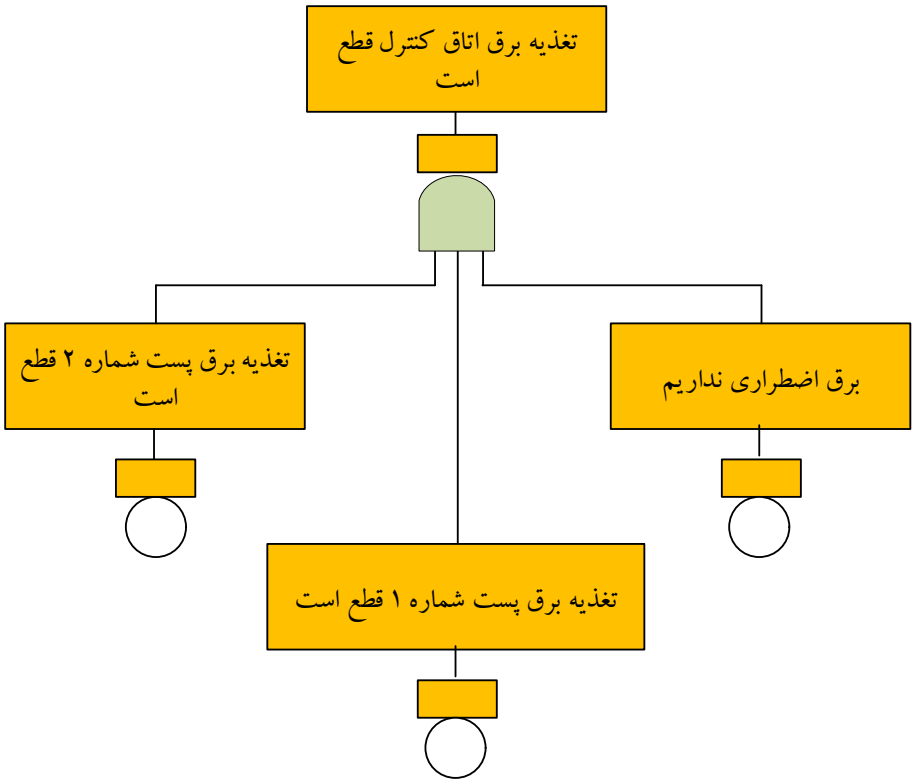


گیت AND علامت این است که وقوع رویداد خروجی مشروط به وقوع همزمان تمامی رویدادهای ورودی است . این گیت می تواند به اندازه دلخواه ورودی داشته باشد .تصویر ۴-۵ یک نمونه گیت AND با خروجی Q و دو ورودی A و B را نشان می دهد . رویداد Q وقتی رخ می دهد که ورودی های A و B ، همزمان رخ دهند .




**تصویر ٤-٥ : گیت AND**

تصویر ۴-۶ یک مثال ساده از کاربرد گیت AND را نمایش می دهد .

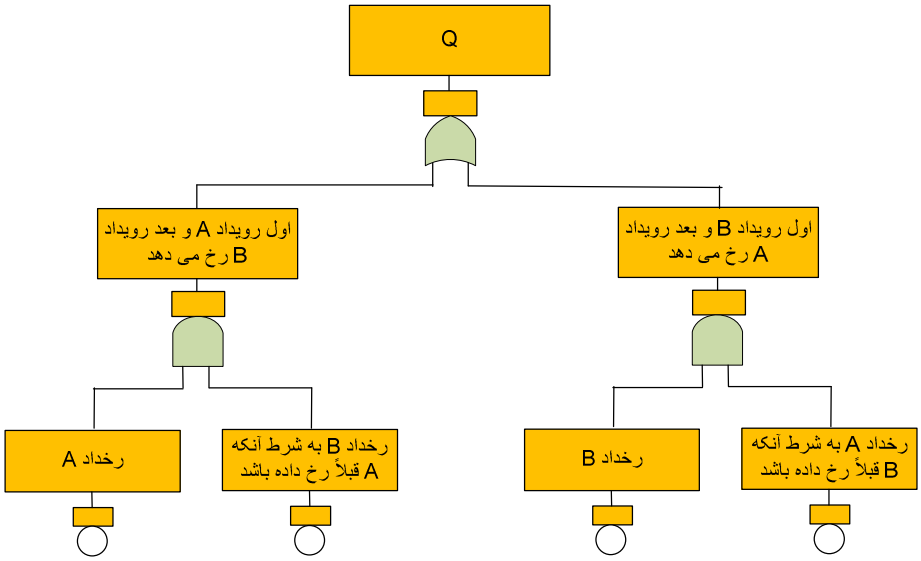



**تصویر ٤-٦ : مثالی از کاربرد گیت AND**

همانطور که مشاهده می کنید ، همزمان شدن قطع تغذیه برق پست های ۱و ۲ و برق اضطراری ، منجر به خاموشی برق اتاق کنترل خواهد شد . اگر قرار باشد وقوع رویدادی را با گیت AND توصیف کنیم ، بایستی تمامی وابستگی های بین ورودی ها را بطور واضح بیان کنیم . چرا که این وابستگی ها در ارزیابی های بعدی درخت و بر منطق جاری سیستم ، تاثیر خواهد داشت . به عنوان مثال در تصویر ۵-۴ ، در صورت بروز رویداد اول ( یعنی رویداد A) ، ممکن است سیستم به حالت آماده باش برود و شرایط وقوع رویداد دوم ( رویداد B) کاملاً متفاوت باشد . دلیل این مطلب را می توان اینگونه توجیه کرد که اگر مثلاً رویداد A و B مربوط به خرابی پمپ های مسیر خوراک ورودی به سیستم باشند و وظیفه اصلی به عهده پمپ

A بوده و پمپ B نقش پمپ بای پاس(آماده باش) را داشته باشد . انتظار می رود که پمپ A بطور دائم یا در دوره های زمانی طولانی در حال کار باشد و در صورت خرابی پمپ B بطور موقت در سرویس قرار داده شود . مطمئناً قابلیت اعتماد و نرخ شکست پمپ دوم ، متفاوت بوده و شکست آن شبیه به پمپ اول نخواهد بود و بهتر است رویداد B با عبارت دقیق تر " خرابی پمپ آماده باش B به شرط آنکه پمپ اصلی A از کار افتاده باشد " ، توصیف شود . تصویر ۴-۷ ، شکل بهتری برای توصیف وابستگی رویدادها است .

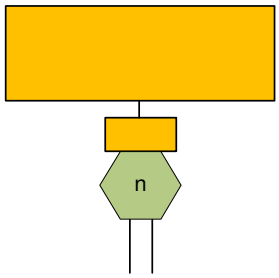
همانطور که در تصویر می بینید ، مهم است که در ابتدا کدام رویداد رخ بدهد . چون دو رویداد داریم ، پس دوحالت ممکن است اتفاق بیفتد : یا ابتدا رویداد A وسپس رویداد B (که مطمئناً از وقوع رویداد A ، تأثیر پذیرفته است) رخ می دهدو یا این قضیه بطور عکس اتفاق خواهد افتاد.



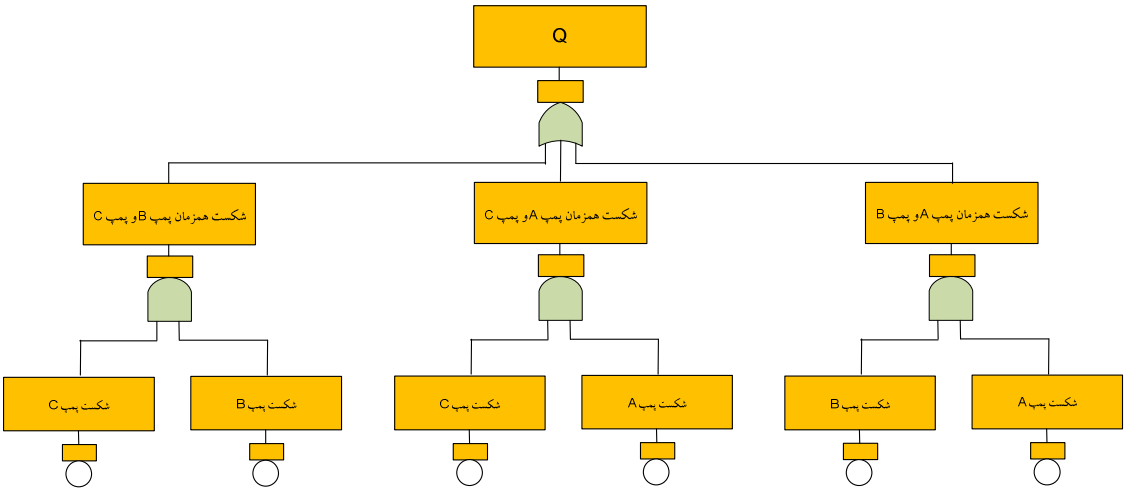

**تصویر ٤-٧: نحوه نمایش وابستگی رویدادها در تحلیل درخت خطا**

نکته آخر اینکه اگر تعداد رویدادهای وابسته به هم ، ۳ تا باشد . در اینصورت علاوه بر وابستگی های دو به دو ، بایستی وابستگی سه رویداد را نیز بیاوریم .

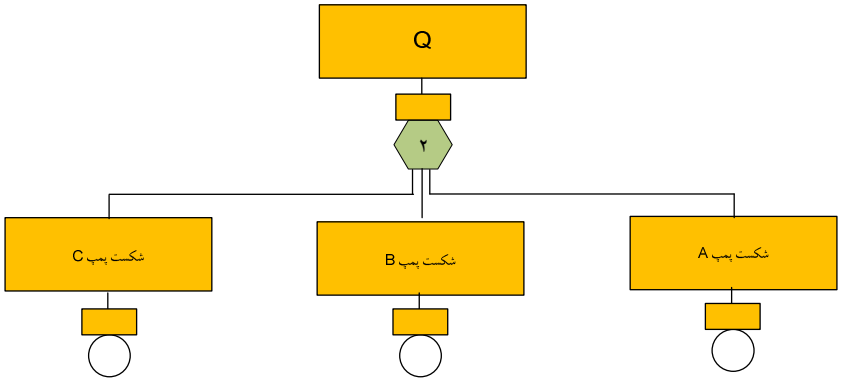
**گیت ترکیبی (Combination Gate )**




گیت ترکیبی با یک ۶ ضلعی منتظم و یک عدد ، نشان داده می شود . در مواقعی که ترکیب خاصی از چند رویداد باعث وقوع رویداد دیگری می شود ، به جای استفاده از گیت های AND و OR متعدد ، براحتی می توان تنها از یک گیت ترکیبی استفاده نمود. به عنوان مثال فرض کنید در یک واحد تقویت فشار گاز ، ۳ پمپ وظیفه انتقال گاز را به عهده دارند . بدین شکل که تنها کارکرد همزمان ۲ پمپ برای انتقال گاز مورد نیاز باشد و از پمپ سوم در زمان اضطرار استفاده شود ( مثلاً وقتی یکی از پمپ ها از کار بیفتد یا نیاز به تعمیر داشته باشد ، پمپ سوم در سرویس قرار داده شود) . واضح است که خرابی یا شکست همزمان دو پمپ ، توقف عملیات انتقال گاز را بدنبال خواهد داشت . در تصویر ۴-۸ ، توقف انتقال گاز به عنوان رویداد رأس تعریف و درخت خطای مربوط به آن رسم شده است . همانطور که مشاهده می کنید برای رسم درخت از ۳ گیت AND و یک گیت OR استفاده کرده ایم . تصویر ۴-۹ نمایشی از همین مثال است که مزیت استفاده از گیت ترکیبی را نشان می دهد . عدد ۲ داخل گیت نشاندهنده ترکیب ۲ از ۳ است . ملاحظه می کنید که استفاده از نماد گیت ترکیبی از حجم وپیچیدگی درخت ، کاسته است .

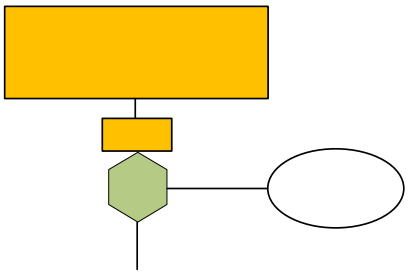



**تصویر ٤-٨ : درخت خطای مربوط به توقف عملیات انتقال گاز**

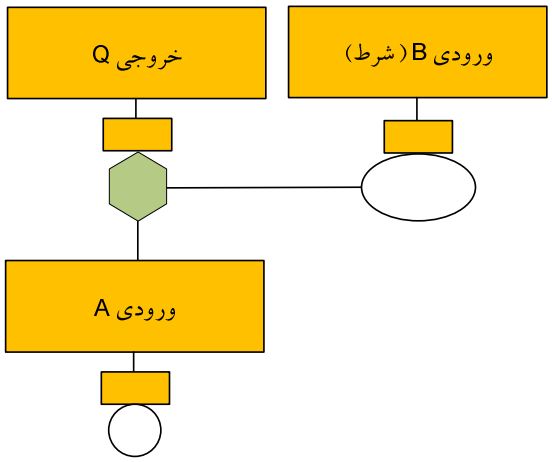



**تصویر ٤-٩ : نمایش دیگری از تصویر ٤-٨ با استفاده از گیت ترکیبی**

## گیت بازدارنده (Inhibit Gate)

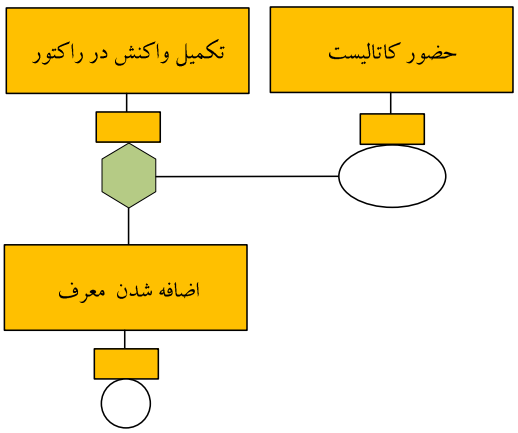


این گیت حالت خاصی از گیت AND است .خروجی گیت تنها یک ورودی دارد . اما وقوع رویداد خروجی بصورت مشروط می باشد . یعنی رویداد خروجی وقتی رخ می دهد که رویداد ورودی تحت شرایطی ، رخ دهد . رویدادی که به عنوان شرط در سمت راست نماد گیت نوشته می شود را ورودی شرطی می نامند . تصویر ۴-۱۰ نمونه کاملی از یک گیت بازدارنده را نمایش می دهد .



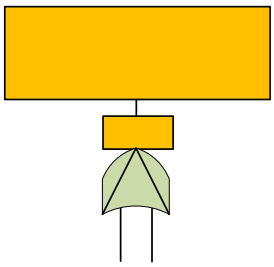

تصویر ۴-۱۰: گیت INHIBIT

در این تصویر رویداد Q در صورتی رخ خواهد داد که رویداد A پس از ارضای شرط B ، رخ دهد . همانطور که ملاحظه می کنید برای نمایش ورودی شرطی B از رویداد شرطی (جدول ۴-۱ را ببینید) استفاده شده است . برای روشن تر شدن مطلب ، راکتوری را در نظر بگیرید که قرار است در آن فرآیند خاصی شکل بگیرد . مثلاً در راکتورهای پلیمریزاسیون اتیلن ، بوتن و هیدروژن و معرف تری اتیل آلومینیوم در حضور کاتالیست ، در دما و فشار خاص ، واکنش کرده و پودر پلیمر تولید می کنند . بنابراین برای تکمیل واکنش نیاز به اضافه کردن معرف در حضور کاتالیست داریم . تصویر ۴-۱۱ کاربرد گیت بازدارنده را برای این مثال نشان می دهد .

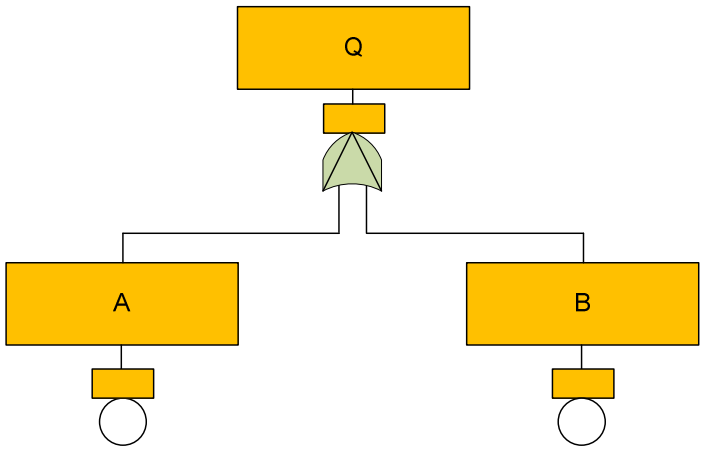



**تصویر ٤-١١ : کاربرد گیت بازدارنده**

### گیت OR انحصاری (Exclusive-OR Gate)

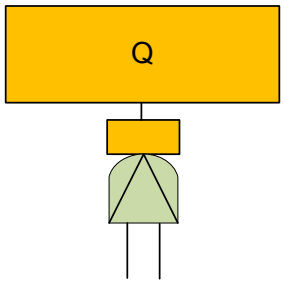


گیت OR انحصاری ، حالت خاصی از گیت OR است . در درخت خطا معمولاً این گیت دارای دو ورودی است . رویداد خروجی گیت زمانی رخ می دهد که تنها یکی از رویدادهای ورودی رخ دهند . تصویر ۴-۱۲ نمایی از گیت OR انحصاری با دو رویداد ورودی را نشان می دهد . تفاوت این گیت با گیت OR در این است که رویدادها مانع الجمع هستند . یعنی شرط وقوع رویداد خروجی Q ، رخداد رویداد A یا B و نه هر دو است .

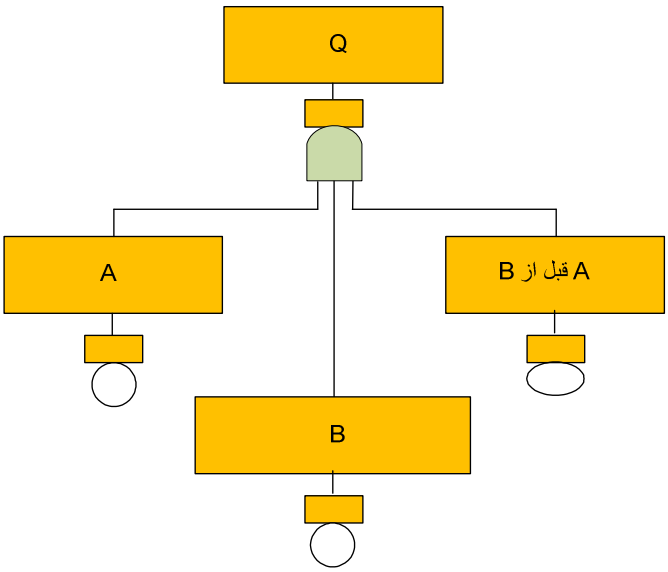



**تصویر ٤-١٢ : تصویری از  گیت بازدارنده**

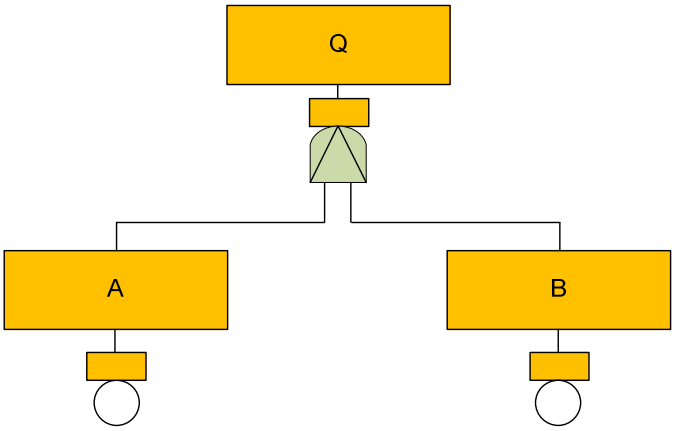
**گیت AND اولویت دار ( Priority-AND Gate)**




گیت AND اولویت دار حالت خاصی از گیت AND است با این تفاوت که رویدادهای ورودی بایستی با ترتیب معینی رخ دهند تا رویداد خروجی رخ دهد .نشان دادن این ترتیب در حالت معمولی با استفاده از رویداد شرطی در سمت راست گراف ، می باشد . اما استفاده از گیت AND  اولویت دار کار را ساده تر می کند و ترتیب از چپ به راست بطور ضمنی درآن نهفته است . تصویر ۴-۱۳ و تصویر ۴-۱۴ به ترتیب تعیین اولویت در حالت معمولی و با استفاده از گیت AND اولویت دار را نمایش داده است .



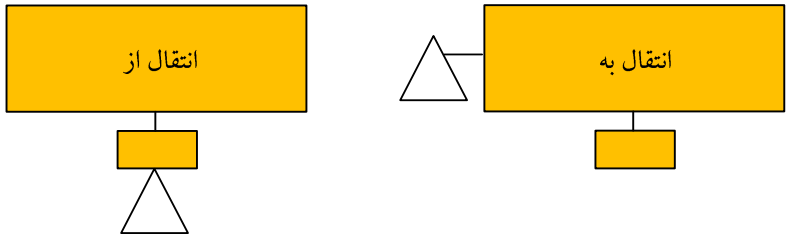

**تصویر ۴-۱۳ : تعیین اولویت با استفاده از گیت AND**




**تصویر ۴-۱۴ : تعیین اولویت با استفاده از گیت AND اولویت دار**

در تصویر ۴-۱۴ رویداد Q وقتی رخ می دهد که ابتدا رویداد A **و** بعد رویداد B رخ دهد .

### نمادهای انتقال(Transfer Symbols)



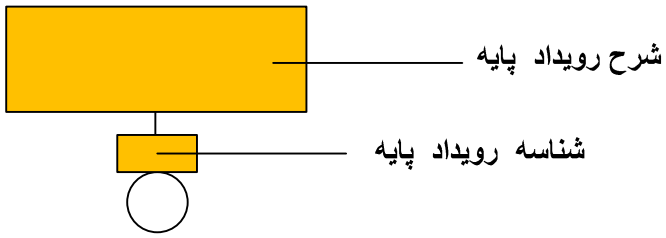
درتحلیل درخت خطا از شکل مثلث به عنوان علامت انتقال استفاده می شود . مهم ترین کاربرد نمادهای انتقال ، تفکیک کردن گراف های بزرگ درخت خطا است . هنگام ثبت درخت خطای مربوط به یک پروژه ارزیابی ریسک که شاید شامل صدها شاخه ، گیت و رویداد باشد ، بایستی به طریقی درخت را در صفحات مختلف مجزا نمود . در این وضعیت می توان ادامه هر بخش از درخت را با استفاده از نماد **انتقال به** (و قید یک شماره یا حرف ) ، به صفحه دیگری ارجاع داد و با بکارگیری نما **انتقال از** ، صفحه ای را که درخت از آنجا ادامه پیدا کرده است را مشخص نمود .

**رویدادهای پایه**[1]

رویدادهای پایه در درخت خطا رویدادهایی هستند که بدلیل رسیدن به مرزهای تحلیل یا نبود اطلاعات ، بیش از این بسط نخواهند یافت . یعنی نقاط انتهایی درخت یا به عبارتی **برگ** های آن هستند . نرخ شکست یا احتمال وقوع این رویدادها ، در حقیقت بانک اطلاعاتی درخت خطا را تشکیل می دهند که اساس وبنیاد ارزیابی کمّی ریسک می باشد . چهار نوع رویداد پایه داریم که در ادامه به شرح مختصری درباره هریک می پردازیم

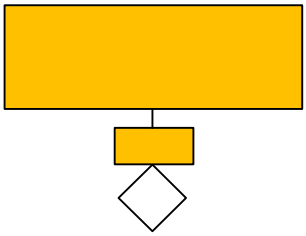
[1] Basic Events

## رویداد اولیه [1]




با قراردادن یک دایره در زیر شناسه رویداد ، شناخته می شوند . این رویدادها ، خطا یا شکست های آغازگر [2] درخت خطا بوده و در مرزهای تحلیل قرار گرفته اند و بیش از این بسط نخواهند یافت . به عنوان مثال اگر در زمان تعیین دامنه شمول و مرزهای تحلیل یک واحد فرآیندی ، این توافق به تصویب برسد که ردیابی خطاها مثلاً تا خرابی شیر کنترل ها و دیگر قطعات اصلی ادامه پیدا کند ، در این صورت خرابی مثلاً شیر کنترل LV-2052 ، یک رویداد پایه اولیه خواهد بود و دیگر نیازی به تعیین حالت های شکست شیر ( از قبیل خرابی ساقه شیر) نیست .

## رویداد بسط نیافته [3]

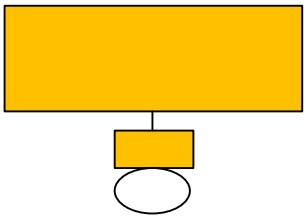


با قراردادن یک لوزی در زیر شناسه رویداد ، شناخته می شوند . این رویداد پایه ، حکایت از این دارد که بدلیل ناشناخته بودن توالی رویدادهای بعدی یا نداشتن اطلاعات کافی ، تحلیل گر قادر نیست یا نمی خواهد توالی شکست های بعدی این رویدادها را دنبال کند . ممکن است

[1] Primary Event
[2] Initiator
[3] Undeveloped Event

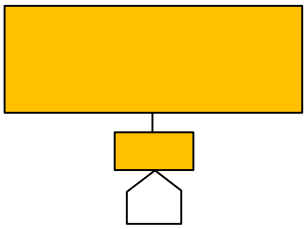
حتی علت بسط ندادن رویداد این باشد که بسط رویداد ، اطلاعات جدیدی به تحلیل اضافه نکند یا ادامه آن در ارزیابی ریسک مشابه ای آمده باشد . به عنوان مثال به هنگام ردیابی خطاهایی که منجر به عدم واکنش در یک راکتور شیمیایی می گردد ، خطای سرویس های جانبی (نظیر آب ، بخار ، نیتروژن و هوا) می تواند به عنوان رویداد بسط نیافته در گراف درخت خطا ، آورده شود .

**رویداد شرطی (Conditional Event)**



برای نشان دادن هرگونه محدویت یا شرط در گراف درخت خطا از رویداد شرطی استفاده می شود . نماد این رویداد با یک بیضی در زیر شناسه رویداد مشخص می شود . این رویداد همراه با گیت های بازدارنده و AND اولویت دار مورد استفاده قرار می گیرد . (تصویر ۴-۱۱ را ببینید)

**رویداد خانه (House Event)**



رویداد خانه وقتی بکار میرود که انتظار وقوع رویدادی را در وضعیت عادی داشته باشیم . بنابراین رویداد های خانه به خودی خود بیانگر خطای سیستم نیستند .

### ۴-۲) طبقه بندی خطا: اولیه، ثانویه و فرمان

طبقه بندی خطاها از مباحث بسیار مهم تحلیل درخت خطا است . هنگام رسم درخت خطا در فصل هشتم ، بارها و بارها به این بخش از فصل چهارم رجوع خواهیم کرد چرا که درک نوع خطای بوقوع پیوسته ، راهنمای خوبی برای شناسایی گیت هایی است که قرار است به رویدادهای این نوع خطاها ، وصل شود . تحلیل گران درخت خطا، خطاها را به ۳ گروه: اولیه، ثانویه و فرمان، تقسیم می کنند.

خطای اولیه، هرگونه خطای قطعه در محیط و شرایطی است که برای آن طراحی شده باشد. به عنوان مثال اگر یک مخزن تحت فشار که برای تحمّل فشار حداکثر $P_0$ طراحی شده است، در فشار $P \leq P_0$ (مثلاً به خاطر عیب جوش)، دچار از هم گسیختگی[1] گردد، می‌گوییم یک خطای اولیه برای مخزن رخ داده است.

خطای ثانویه، هرگونه خطای قطعه در خارج از محدودهٔ طراحی آن است. به عنوان مثال اگر مخزن ذکر شده در فشار $P > P_0$ دچار شکست شود، می گوییم مخزن دچار خطای ثانویه شده است. مثال های دیگری از خطای ثانویه شکست ناشی از نبود سیستم‌های کنترلی و ارتعاش بیش از حد، می‌باشد.

[1] Rupture

چون خطاهای اولیه و ثانویه عموماً شکست‌های مربوط به قطعه و تجهیز می‌باشند، موسوم به خطای قطعه[1] هستند. در مقابل این نوع خطا ، خطای فرمان[2] را داریم ، که به توضیح آن می پردازیم .

خطای فرمان، مربوط به عملکرد صحیح تجهیز، اما در زمان یا مکان اشتباه است . به عنوان مثال بسته شدن یک شیر کنترل، در زمان نامناسب و به علت دریافت سیگنال ناخواسته، یک خطای فرمان برای شیر محسوب می‌شود. همینطور متوقف شدن یک خط تولید، به علت خاموشی برق، مثالی دیگر از بروز خطای فرمان است. اینگونه طبقه‌بندی خطاها به هنگام رسم درخت خطا و بررسی منطق حاکم بر سیستم و علل وقوع رویداد رأس، بسیار سودمند بوده و نظم فکری خوبی به تحلیل‌گر می‌دهد. از طرفی این اطمینان بوجود می‌آید که خطایی دور از چشم نمانده و تمامی خطاهای ممکن در سیستم دیده شده است.

### ۴-۳) قطعات فعال[3] و غیر فعال[4] (عامل و غیر عامل)

در خیلی از موارد، تقسیم قطعات و تجهیزات به دو نوع عامل و غیر عامل، باعث تسهیل در مطالعه و تحلیل می‌شود. یک قطعه غیر عامل نقش کم و بیش ایستایی در کارکرد سیستم دارد. این قطعه، ممکن است یک انتقال دهنده انرژی از نقطه ای به نقطهٔ دیگر (به عنوان مثال، یک سیم حامل جریان در برق یا یک خط انتقال گاز )، یا انتقال دهنده بار باشد.

[1] Component Fault
[2] Command Fault
[3] Active
[4] Passive

برای ارزیابی عملکرد یک قطعه غیر عامل، آزمون هایی از قبیل تحلیل تنش، مطالعه انتقال حرارت و غیره، انجام می شود.

یک قطعه عامل، با ایجاد تغییرات و اصلاحاتی در سیستم، نقش پویاتری در کارکرد آن ایفا می کند. عموماً اینگونه قطعات نیاز به یک سیگنال ورودی یا محرّک دارند تا سیگنال خروجی داشته باشند. در این حالت، قطعه عامل مانند یک تابع تبدیل[1] (عبارت مصطلح در ریاضیات و الکترونیک) عمل می کند. قطعه عامل در صورت شکست، سیگنال خروجی نخواهد داشت و یا سیگنالی به اشتباه ارائه خواهد داد. به عنوان مثال یک شیر کنترل، یک قطعه عامل است چرا که به هنگام باز و بسته شدن، بر جریان سیّال اثر می گذارد و یک کلید برق نیز ، اثر مشابه ای را در مدارات الکتریکی دارد. برای ارزیابی عملکرد یک قطعه عامل، از تحلیل های پارامتری بر روی شاخص های عملیاتی قطعه، استفاده می شود.

## ۴-۴) مفهوم دلیل بلافصل[2]

در تحلیل درخت خطا، بعد از تعریف سیستم تحت مطالعه و مشخص نمودن مرزها و محدودیت‌های تحلیل، شکست خاصی از سیستم انتخاب می‌شود که جایگزین رویداد رأس در

[1] Transfer Function
[2] Immediate Cause
منظور از دلیل بلافصل ، دلیل یا علتی است که برای وقوع یک رویداد خطا ، بلافاصله در ذهن خطور می کند و از نظر منطقی اولین دلیلی است که بی واسطه باعث وقوع رویداد می گردد . به عنوان مثال اگر رویداد خطا روشن نشدن لامپ مهتابی بعد از زدن کلید باشد ، دلیل بلافصل آن ، خرابی (یا در اصطلاح برقکاران سوختن ) لامپ خواهد بود . (مترجم)

درخت خطا می‌گردد. آنچه در مرحله بعد اتفاق می‌افتد، تعیین علـل لازم و کـافی بـرای وقـوع رویداد رأس می باشد . یعنی عللی که به خاطر وجود آنها رویداد رأس اتفاق افتاده است .

لازم به ذکر است که این علل، لزوماً رویدادهای پایه و ریشه‌ای وقوع رویداد رأس نیستند بلکه تنها دلایل بلافصل وقوع آن هستند.

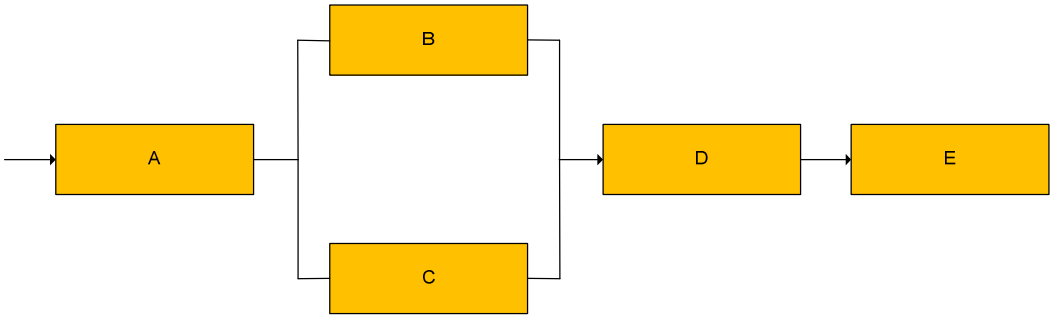
در مرحله بعد، این دلایل لازم و کافی، خود به عنوان رویدادهای فرعی رویداد رأس تلقی شده و تحلیل‌گر کار خود را با یافتن علل لازم و کافی بـرای بـروز ایـن رویـدادها دنبـال مـی‌کنـد و بگونه‌ای با رویدادهای فرعی رفتار می‌کند که گویا آنها هـر یـک بـه تنهـایی یـک رویـداد رأس مستقل هستند. تحلیل درخت خطا در مراحل بعد به همین شکل و با همـین روال ادامـه پیـدا می‌کند تا به مرزهای تحلیل (که از قبل تعریف شده اند) برسیم. رویدادهایی که در مرز تحلیل قرار گرفته‌اند، همان رویدادهای پایه هستند.

برای روشن شدن مطلب به ذکر یک مثال می‌پردازیم. تصویر ۴-۱۵ را در نظـر بگیریـد . ایـن تصویر مسیر انتقال یک سیال را نشان میدهد و شامل قطعات A ، B ، C ، D و E است[1] . فرض کنیم سیال ما آب ، قطعات A ، B ، C ، D ، شیر[2] و E مخزن باشد .طـرز کـار سیسـتم بـدین شکل است:

[1] تصویر فوق مثالی از یک سیستم انتقال به معنای عام است . آنچه انتقال می یابد بستگی به نوع سیستم دارد . به عنوان مثال در صنایع فرآیندی خطوط انتقال ، لوله هستند و قطعات ممکن است ترکیبی از شیر و پمپ باشند . در الکترونیک خطوط انتقال ، سیم هستند و قطعات ممکن است ترکیبی از کلید و مقاومت باشند . خواننده می تواند در مورد سیستم تحت مطالعه خود ، جایگاه این عناصر را مشخص کند .

2 Valve

با ورود جریان به شیر A و در صورت باز بودن آن، جریان به ورودی شیرهای B و C می‌رسد. و از آنجا در صورت باز بودن حداقل یکی از شیرها جریان وارد شیر D می‌شود و در نهایت شرط رسیدن جریان به مخزن E ، باز بودن شیر D می‌باشد.




تصویر ۴-۱۵ : سیستمی برای تشریح مفهوم دلیل بلافصل

فرض کنید رویداد رأس را اینگونه تعریف کنیم : ***نرسیدن جریان به مخزن***

همچنین فرض می کنیم که خطوط ارتباطی (در این مثال خطوط لوله)، شکست‌هایی ناچیز و قابل صرف‌نظر داشته باشند. (در اغلب کاربردها، احتمال شکست خطوط لوله و سیم ها و دیگر خطوط ارتباطی صفر در نظر گرفته می‌شود) .

حال برای تشریح مفهوم دلیل بلافصل، نحوه ردیابی علل وقوع رویداد رأس (نرسیدن جریان به مخزن) را قدم به قدم، بررسی نماییم. علت فوری یا دلیل بلافصل نرسیدن جریان به مخزن، نبودن جریان در خروجی شیر D است. تحلیل گر در اینجا بایستی دقت کند و اولین علت وقوع رویداد رأس را نداشتن جریان در ورودی شیر D نبیند. **برای یافتن علل بلافصل بایستی در هر لحظه تنها یک گام رو به عقب برداشت و از برداشتن چند گام و یا پرش از چندین رویداد، حذر کرد.**

اکنون رویداد فرعی « نبودن جریان در خروجی شیر D » به عنوان رویـداد رأس فرعـی تلقّـی شده و ضرورت جدید، یافتن علت و یا علل بلافصل وقوع آن است. در ایـن مرحلـه دو احتمـال وجود دارد:

(۱) جریان به ورودی شیر D داریم، اما جریان در خروجی آن مشاهده نمی‌شود.

(۲) جریان به ورودی شیر D نمی‌رسد.

بنابر این علل وقوع رویداد فرعی تعریف شده برای شیر D اجتماع دو رویداد (۱) یا (۲) اسـت. (توجه خواننده را به این مطلب جلب می‌کنیم که اگر هنگام بررسی رویداد رأس یعنی نرسیدن جریان به مخزن، به اشتباه ، علت را نرسیدن جریان به شیر D در نظر می‌گـرفتیم، رویـداد (۱) حذف می‌شد. در واقع انگیزه توجه به مفهوم دلیل بلافصل در همین حقیقت نهفته اسـت و آن حذف نشدن و دیده شدن تمامی دلایل و رویدادها در تحلیل درخت خطا می‌باشد)

اکنون می‌توان به بررسی علل فوری وقوع رویدادهای (۱) و (۲) پرداخت. اگر در تعریف مرزها و محدودیت‌های تحلیل، تنها پیشروی و بررسی تا سیستم‌های فرعی مجاز باشد، در ایـن صـورت رویداد (۱) را با بازنویسی آن به شکل « شیر D باز نمی‌شود و ایراد دارد » می توان بـه عنـوان یک رویداد پایه، ثبت نمود. در مورد رویداد (۲) دلیل ضـروری و بلافصـل وقـوع آن، « نبـودن جریان در خروجی شیر B و C به طـور همزمـان » اسـت کـه فصـل مشـترک دو رویـداد زیـر می‌باشد:

(۳) نبودن جریان در خروجی شیر B

(۴) نبودن جریان در خروجی شیر C

بنابراین:

[ وقوع رویداد (۲)] =[ وقوع رویداد (۳)] و [وقوع رویداد (۴)] بطور همزمان

لازم است برای روشن تر شدن اصطلاحات مورد استفاده در درخت خطا یادآور شویم که اگر رویدادی به عنوان رویداد پایه تلقی شود [برگ های درخت خطا] و دیگر بسط داده نشود، به عنوان شکست و در صورتیکه بسط داده شده و علل وقوع آن موشکافی شود، تحت عنوان **خطا** در نظر گرفته می‌شود.

در مرحله بعدی، تحلیل ما با تمرکز بر روی رویداد (۳) و (۴) ادامه پیدا می کند . رویداد (۳) ناشی از وقوع حداقل یکی از دو رویداد زیر است:

(۵) جریان به ورودی شیر B داریم ، اما در خروجی آن جریانی مشاهده نمی‌شود.

(۶) جریان به ورودی شیر B نمی‌رسد.

رویداد (۵) را می‌توان براحتی به عنوان یک شکست (رویداد پایه) در نظر گرفت ( البته با جایگزین کردن آن با عبارت « خرابی شیر B »). رویداد (۶) خطایی است که بایستی بیشتر مورد بررسی قرار بگیرد. رویداد (۴) نیز به همین شکل مورد تحلیل قرار می‌گیرد.

خواننده اکنون با درک مفهوم دلیل بلافصل و علت لازم و کافی، به سادگی می‌تواند تحلیل این سیستم را ادامه دهد. تحلیل درخت خطا وقتی پایان می‌پذیرد که تمامی رویدادهای پایه شناسایی شوند. البته در مورد شیر A بدلیل عدم دسترسی به تجهیزات پایین دست شیر، رویداد « نرسیدن جریان به ورودی شیر A » ، یک رویداد بسط نیافته خواهد بود.

می بینید که بررسی و تحلیل ما برای یافتن علت وقوع رویداد رأس (در این مثال« نرسیدن جریان به مخزن») رویدادهای خطایی را مشخص نمود که با پیوندهای منطقی به هم مرتبط شده بودند. در حقیقت تمامی این رویداد و پیوندها بر روی سازه درخت خطا قرار گرفته‌اند.

### ۴-۵) قواعد رسم درخت خطا

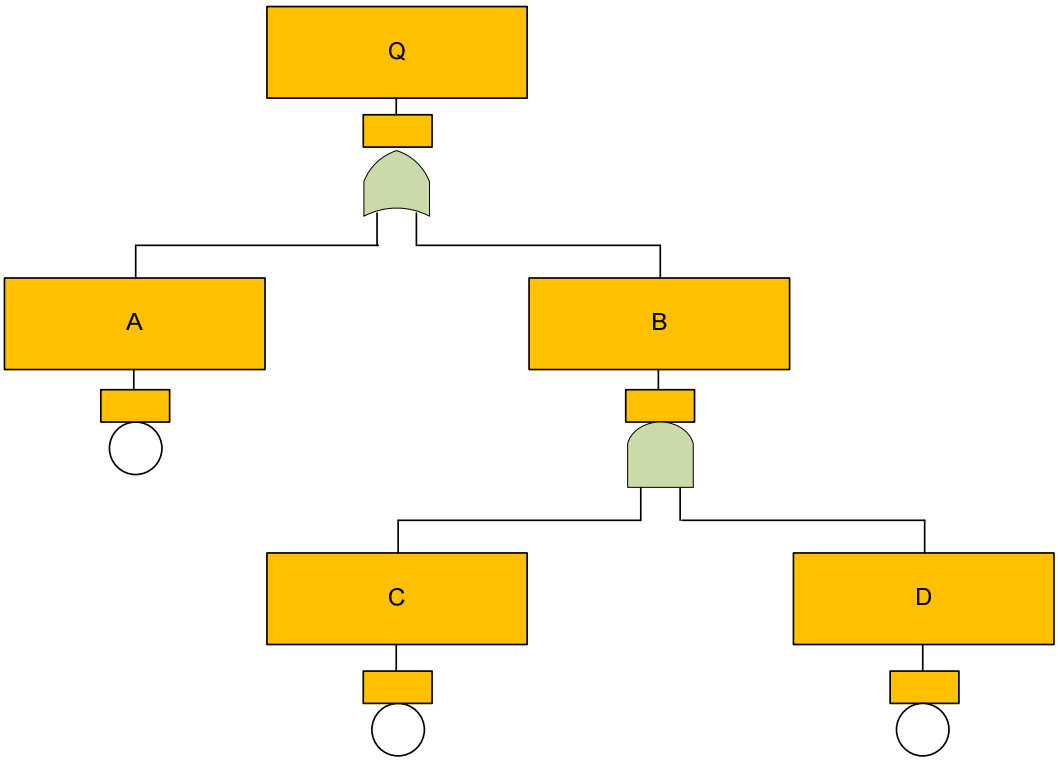
رسم درخت خطا، قدمتی ۵۰ ساله دارد. در ابتدا ، رسم درخت خطا تنها به عنوان یک کار هنری محسوب می‌شد و سلیقه افراد تأثیر زیادی در رسم آن داشت . اما بعدها پی برده شد که درخت‌هایی که بر اساس اصول و قاعده رسم شوند، تحلیل‌گران را از سردرگمی نجات داده و برای یک رویداد رأس مشخص، درخت خطای منحصر به فردی رسم می‌شود. و بدین شکل رسم درخت خطا از جنبه هنری خارج شده و بُعد علمی پیدا کرد. در اینجا به شرح این قواعد می‌پردازیم.

تصویر ۴-۱۶ را در نظر بگیرید. این تصویر درخت خطای ساده‌ای را نشان می‌دهد که ممکن است بخشی از یک درخت بزرگتر باشد. هیچکدام از رویدادهای خطا ، نوشته نشده و به جای آنها از حروف استفاده شده است. البته در مورد یک مسئله خاص، شرح دقیق رویدادها ضروری است. و بایستی به جای حروف شرح آن ها آورده شود.

این مطلب اولین قاعده رسم درخت خطا است:

**۱- عبارت‌هایی را که در داخل جعبه رویدادها می‌نویسید، بایستی از نوع خطا باشند. خطا را دقیقاً شرح داده و شرایطی که باعث وقوع آن می‌شود را مشخص کنید.**

ذکر این نکته حائز اهمیت است که تحلیل‌گر نبایستی خود را محدود به فضای جعبه رویداد کند. اگر برای شرح یک رویداد نیاز به کلمات بیشتری دارید، آنها را بنویسید حتی اگر مجبور شدید جعبه را بزرگتر یا از فونت کوچکتری استفاده کنید. اینکه از جملات مختصرتری برای شرح رویداد استفاده شود به شرطی مفید است که ایده و مفهوم رویداد خلاصه و حذف نگردد.




**تصویر ٤-١٦ : یک درخت خطای ساده**

مثال‌هایی از عبارات خطا عبارتند از:

- رله ، علیرغم اعمال میدان الکترومغناطیسی به سیم پیچی آن ، باز نمی‌شود[1].

[1] البته با این فرض که کنتاکت های رله در حالت عادی ، بسته باشد .

- شیرکنترل خط نیتروژن ، اشکال مکانیکی دارد.
- اپراتور دکمه استارت پمپ را به اشتباه فشار می دهد .
- چراغ سیگنال آلارم سطح بالای مخزن ، روشن نمی شود .
- موتور علیرغم اعمال تغذیه برق به آن، شروع به کار نمی‌کند .
- ترموکوپل داخل مخزن ، شکسته است .

گام بعدی تعیین رویدادهایی است که برای به وقوع پیوستن خطای شرح داده شده در هر جعبه رویداد، لازم و کافی هستند. یک راهنمایی سودمند این است که مشخص کنیم خطای به وقوع پیوسته مربوط به وضعیت خود قطعه و یا یک خطای سیستمی می‌باشد.

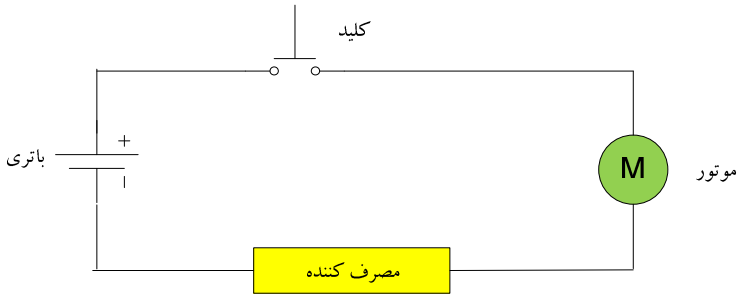
**خطای قطعه،** نشأت گرفته از خود قطعه بوده و در محل نصب آن، اتفاق می‌افتد اما **خطای سیستمی** ممکن است مربوط به بروز خطا در مرحله‌ای از فرآیند سیستم و یا وقوع خطاهای چندگانه باشد. البته نوع خطا تنها برای کمک به تحلیل‌گر در ردیابی و درک منطقی حاکم بر بروز خطا می‌باشد و ممکن است صراحتاً توسط وی بیان نشود . آنچه که مهم است مشخص نمودن وضعیت خطا می‌باشد. استفاده از این مفهوم قاعده دوم درخت خطا است:

**۲- اگر پاسخ به سئوال، «آیا خطا ، مربوط به شکست یا خرابی خود قطعه است؟» مثبت باشد، آن را به عنوان خطای قطعه و اگر پاسخ منفی باشد، به عنوان خطای سیستمی، طبقه‌بندی کنید.**

اگر رویداد خطا مربوط به وضعیت قطعه بود از گیت **یا** منطقی استفاده کنید و بدنبال حالت‌های شکست اولیه، ثانویه و فرمان بگردید و اگر مربوط به وضعیت سیستم بود ، بدنبال

علل لازم و کافی برای وقوع آن، باشید . البته برای بسط خطای سیستمی ممکن است از گیت‌های **و** یا **بازدارنده** یا دیگر گیت‌ها استفاده شود.

به عنوان یک قاعده کلی، اگر انرژی از نقطه‌ای خارج از محل قرارگیری قطعه، نشات بگیرد، رویداد در طبقه خطای سیستمی قرار می‌گیرد. برای شرح بیشتر قاعده دوم مدار ساده‌ی موتور، کلید و باتری را در تصویر ۴-۱۷ در نظر بگیرید.




تصویر ۴-۱۷ : سیستم موتور – کلید – باتری ساده

سیستم دارای دو وضعیت است :

الف ) در حال کار

ب) در حال آماده باش

خطاهای شناسایی شده سیستم برای دو حالت فوق ، با توجه به قاعده دوم ، در جدول ۴-۲ آمده است . علاوه بر دو قاعده فوق، شماره دیگری از قواعد و روال های رسم درخت خطا در سال های اخیر بسط داده شده اند که اولین آنها قاعده« **انتظار معجزه نداشتن**[1] »است:

[1] No Miracle Rule

**۳- اگر کارکرد عادی قطعه، منجر به گسترش یک رشته از خطاها می گردد، بایستی فرض را بر ایـن گذاشت که قطعه عملکرد طبیعی خود را دارد.**

ممکن است در مرحله ای از بررسی سیستم، تحلیل گر متوجه شود که توالی خاصی از خطاهـا به واسطه شکست یا خرابی غیر منتظره یک یا چند قطعه، متوقـف مـی‌شـود. بایسـتی فـرض صحیح را بر این گذاشت که عملکرد طبیعی قطعه به چه شکل بوده است و اجازه داد مسیر و

**جدول ۴-۲ : خطای قطعه و خطای سیستمی درتصویر ۴-۱۷**

| **الف) در حال کار** | |
|---|---|
| **شرح خطا** | **نوع خطا** |
| ✓ با فشار دادن کلید، اتصال برقرار نمی‌شود | خطای قطعه |
| ✓ با فشار دادن کلید، مدار به طور ناخواسته باز می‌شود. | خطای قطعه |
| ✓ با اعمال تغذیه برق، موتور روشن نمی‌شود | خطای قطعه |
| ✓ موتور علیرغم برقرار بودن تغذیه برق، از کار می‌افتد | خطای قطعه |
| **ب) در حال آماده باش** | |
| **شرح خطا** | **نوع خطا** |
| ✓ کلید بدون فشار دادن آن، وصل می‌شود | خطای قطعه |
| ✓ موتور، بطور ناخواسته روشن می‌شود | خطای سیستمی |

توالی خطاها در سیستم، ردیابی شود. راه دیگری بیان قاعده فوق این است که اگر در سیستم بنوعی و منطقی (AND) وجود داشته باشد بایستی آن را لحاظ کنیم.

دو قاعده دیگر رسم درخت خطا به **خلاف قاعده عمل کـردن**[1] و **میـان بـر زدن**[2]، اشـاره دارد .

اولین آنها قاعده **تکمیل گیت** است:

**۴- تمامی ورودی‌های به یک گیت خاص بایستی قبل از پیشروی در تحلیل ، به طـور کامـل تعریـف شوند.**

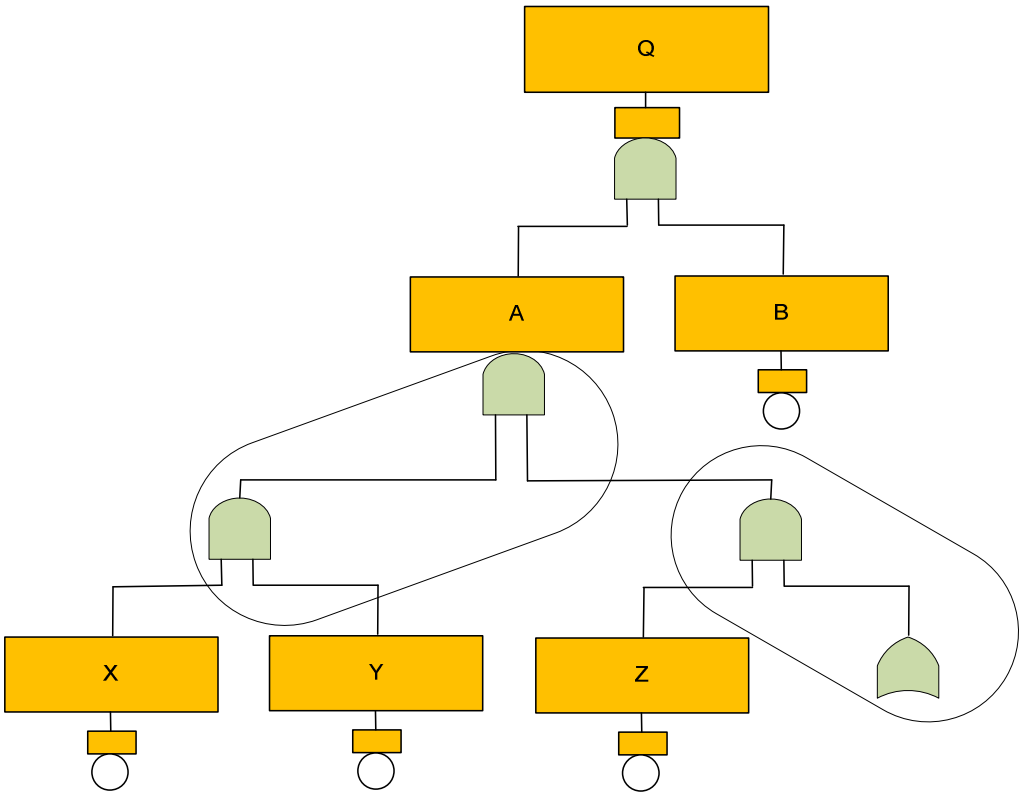
و دومی قاعده **عدم اتصال گیت به گیت** است:

**۵- ورودی‌های گیت بایستی به شکل خطا تعریف شوند و نباید گیت را بطور مستقیم و بدون واسطه به گیت دیگر وصل کرد.**

قاعده تکمیل گیت به این مسئله اشاره می‌کند که درخت خطا بایستی سطح بـه سـطح بسـط داده شود و هر سطح قبل از ملاحظه و توجه به سطوح پایین تر، کامل شود. برای توضیح قاعده عدم اتصال گیت به گیت، تصویر ۴-۱۸ را که بخشی از یک درخت خطا است ، مشاهده کنید. در این تصویر دوبار قاعده عدم اتصال مستقیم گیت به گیت ، نقض شده اسـت . البتـه در نـرم افزارهای درخت خطا ، شرح جعبه رویداد بخشی از شیء گیت می‌باشـد کـه بـه بسـط روشـن منطق درخت خطا کمک کرده و از اتصال گیت به گیت مانند تصویر ۴-۱۸ جلوگیری می‌نماید. اتصال گیت به گیت علامت یک تحلیل آشفته و درهم برهم است . وقتـی درخـت خطـا رسـم می‌شود، میانبرهای گیت به گیت ، منجر به سـردرگمی شـده و نشـان دهنـده ایـن اسـت کـه

[1] Not being methodical
[2] To shortcut

تحلیل گر درک ناقصی از سیستم دارد. درخت خطا وقتی به طور موفق آمیز رسم می‌شود کـه تحلیل گر شناخت و درک کامل و روشنی از سیستم مدل شده داشته باشد.




تصویر ۴-۱۸ : برشی از یک درخت خطا

### ۴-۶ ) خطاهای قطعه و خطاهای سیستمی

همانگونه که قبلاً بیان شد، جواب به این سوال که خطا مربوط به قطعه یا سیستم است، بسـیار سودمند می‌باشد. یک وضعیت خطای قطعه، منحصراً مربوط به یک قطعه خاص است. در طرف مقابل ، یک وضعیت خطای سیستمی فقط مرتبط با یک قطعه نیست و علت بلافصل وقـوع آن ممکن است مربوط به چند قطعه باشد .

مثالی از وضعیت خطای قطعه، باز نشدن یک شیر به علت خرابی است. ممکن است باز نشـدن شیر به دلیل وجود یک نقص یا عیب داخلی در سیستم شیر و یا عدم دریافت فرمان باز شدن ، باشد. هر دو این خطاها منحصراً مرتبط با شیر هستند.

مثالی از وضعیت خطای سیستمی، نداشتن جریان سیال در خروجی دو پمپ موازی مـی‌باشـد. در این حالت نمی توان گفت یکی از پمپ ها و یا هردو آنها حتمـاً ایـراد دارنـد و تحلیـل گـر ، نهایتاً به این نتیجه برسد که علت اولیه نداشتن جریان سیال، عدم تأمین آن از طـرف مخـزن باشد.

مثال دیگری از وضعیت خطای سیستمی، روشن شدن ناخواسته یک پمپ است. پمپ سـهمی در این خطا ندارد. بلکه اعمال ناخواسته تغذیه برق، علت اصلی خطا است. بنابراین می‌توان آن را یک وضعیت خطای سیستمی به حساب آورد.

وضعیت خطای قطعه را اغلب با استفاده از گیت **یا** منطقی (OR) و یا یک رویـداد اولیـه مـدل می‌کنند. در مورد مثال بالا در مورد باز نشدن شیر، می‌توان آن را با گیت یا منطقی بـا رویـداد اولیه خرابی شیر به عنوان ورودی اول و عدم دریافت سیگنال بـه شـیر بـه عنـوان ورودی دوم، مدل نمود. در مورد خطای بسته نشدن شیر نیز به همین شکل رفتار می شود .

وضعیت خطای سیستمی را می‌شود با هر نوع گیتی که کارائی داشته باشد، مـدل کـرد. بـرای مثال در مورد دو پمپ بالا، اگر هر دو پمپ مورد نیاز باشند از گیت **یـا** منطقـی و اگـر یکـی از پمپ‌ها کافی باشد از گیت **و** منطقی استفاده نمود .

### ۴-۷) رسم درخت خطا تا چه سطحی ادامه می‌یابد؟

اگر چه این عنوان در بحث های قبلی بوده اما بـه دلیـل اهمیـت آن بـه شـرح بیشـتر موضـوع می‌پردازیم:

اینکه تحلیل درخت خطا را تا چه سطح و عمقی جلو ببریم به پایان کار و نتایج حاصـله معنـی می‌بخشد. اگر درخت خطا بیش از حد بسط یافته و تا سطوح بسیار پایین‌تر ادامه پیدا کنـد نـه تنها تلاش بیهوده‌ای محسوب می‌شود بلکه عدم قطعیت[۱] و عدم اطمینان بیشـتری را در نتـایج حاصله ایجاد می‌کند.

به عنوان یک قاعده کلّی، **درخت خطا را باید تا سطحی که ارتباط بین اجزاء را مشخص کـرده و بـا میزان دسترسی به داده همخوانی داشته باشد، ادامه داد.** پیشـروی بیشـتر باعـث از دسـت رفـتن انسجام و ساختار می‌شود. به عنوان مثال، یک شیر کنترل[۲] را ممکن است تا ریزترین قطعـاتش تجزیه کرد اما آیا در چنین سطحی و تا این حد و اندازه، داده و اطلاعات موجود است و با فرض وجود ، عدم اطمینان در نتایج کمّی شده به شدت افزایش می یابد.

**معمولاً درخت خطای مربوط به یک شکست و خرابی سیستمی، تا قطعات عمده سیستم بسط یافتـه و تا سطحی که به نقش ها و اجزاء اصلی مربوط می‌شود، ادامه پیدا می‌کند.** مثال‌هـایی از قطعـات و نقش‌های اصلی، شیرهای کنترل، پمپ‌ها و خطاهای انسانی قابل تشخیص می‌باشـد. همچنـین نشان دادن سرویس‌های جانبی[۳] پشتیبان از قبیل تغذیه برق و منابع آب خنک کننده[۴] ، حـائز

[1] Uncertainty
[2] Control valve
[3] Utility
[4] Cooling Water

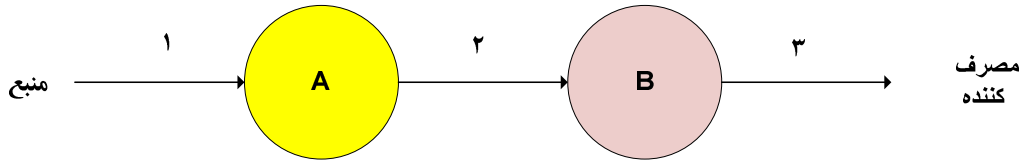
اهمیت است. به هر حال بسط درخت خطا تا نمایان شـدن (آشـکار شـدن) وابسـتگی اجـزاء و رویدادهای اصلی ضروری است .

## فصل ۵ : توسعه تحلیل درخت خطا

در بخش‌هایی که خواهد آمد به موارد کاربردی تحلیل و پیاده سازی تحلیل درخت خطا می پردازیم. اولین مورد ، بحثی است در رابطه با کاربرد قواعد رسم درخت خطا در سیستمی که حاوی جریان سیال یا جریان تغذیه است دو حالت قطع و نشتی جریان را بررسی می‌کنیم. از جمله مباحث دیگر این بخش ، مدلسازی شکست‌های علت مشترک، خطاهای انسانی، حلقه‌ها و بازخورد، نامگذاری رویدادها و روش‌های آزمون صحّت درخت خطا است .

### ۵-۱) مدلسازی قطع جریان و نشتی جریان

قانون اصلی در مدلسازی درخت خطا در هر قدم و مرحله، تشخیص علل لازم، کافی و بلافصل وقوع خطاهاست. برای درک این موضوع و بهره گیری ضمنی از آن، دو وضعیت قطع جریان و نشتی جریان را به عنوان رویداد رأس در نظر گرفته، مدلسازی می‌کنیم. منظور ما از جریان، جریان مایع، گاز و یا هر جریان دیگری است که از یک منبع تأمین شده و در جایی مصرف می شود . این مثال نه تنها کاربرد قواعد رسم را نشان می‌دهد بلکه می‌تواند به عنوان الگو در بسیاری از تحلیل‌ها مورد استفاده قرار بگیرد. خط سیگنال زیر را در نظر بگیرید:



عناصر A و B ممکن است شیر آب باشند. در این صورت منبع، مثلاً یک مخـزن آب اسـت . در کاربردهای الکتریکی، A و B رله یا هر المان الکتریکی دیگـر و منبـع بـاتری و مصـرف کننـده لامپ است.

فرض کنید این عناصر توسط ۳ قطعه سیم یا لوله به هم وصـل شـده باشـند در تصـویر ۵-۱ و ۵-۲ مدل‌های درخت خطای قطع جریان و نشتی جریـان نمـایش داده شـده‌انـد. خواننـده بـه راحتی می‌تواند منطق به کار رفته در هر درخت را دنبال کند. همانطور که دیده می‌شـود ایـن منطق جزء گرا بوده و با شروع از مصرف کننده و تعریف رویداد رأس (قطع و یا نشتی جریـان) با گام‌هایی رو به عقب، به طرف منبع می‌رود و در هر گام ، تحلیل گر این سئوال اساسـی را از خود می پرسد : دلیل یا علل لازم، کافی و بلافصل وقوع رویداد در این گام چیست؟

در پایان ملاحظه می‌کنید که با تبدیل رویداد رأس از قطع جریان به نشتی جریان، گیـت‌هـای OR با گیت‌های AND تعویض می‌شوند.

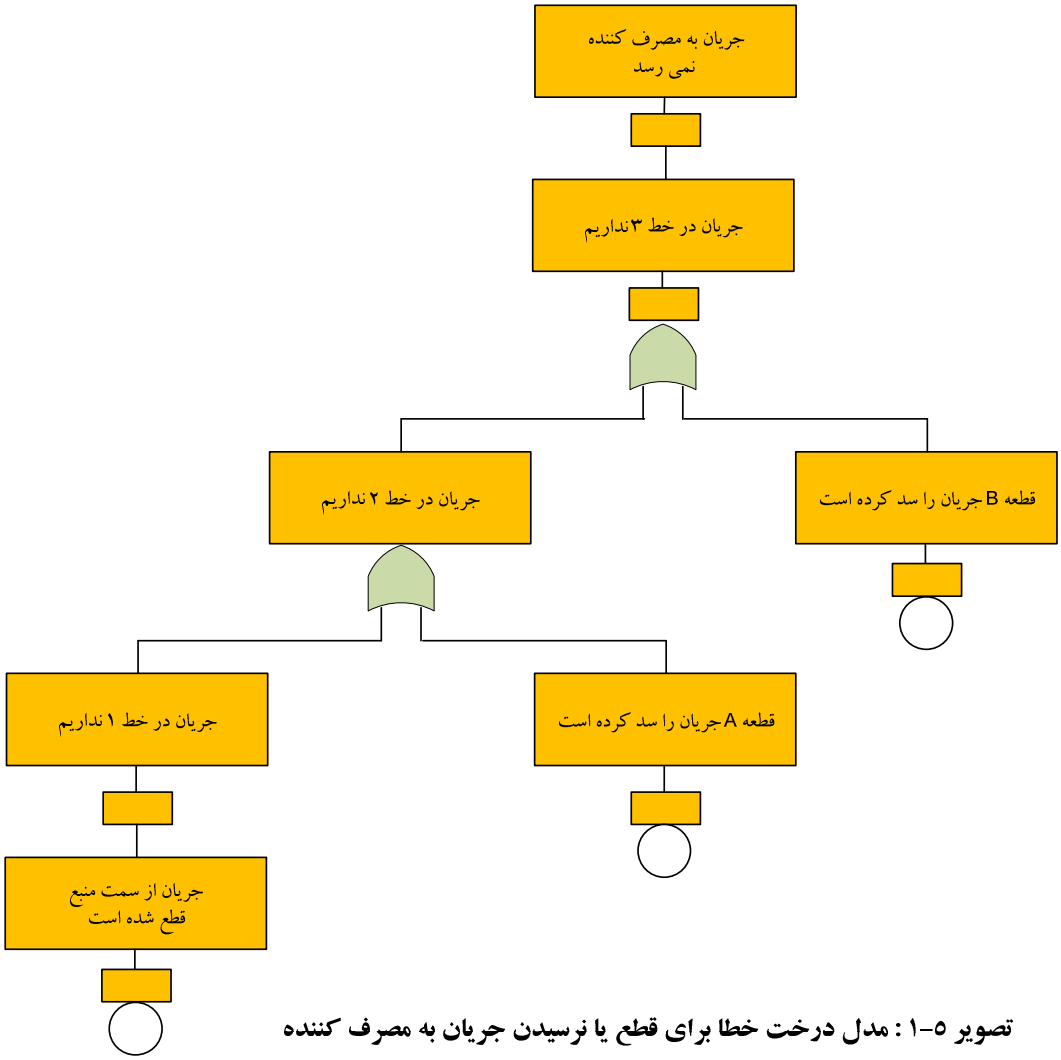
*** تصویر ۵-۱) منطق نرسیدن جریان به مصرف کننده**

۱- نرسیدن جریان به مصرف کننده = عدم جریان در خط ۳.

۲- عدم جریان در خط ۳= عنصر B جریان را مسدود کرده یا جریان در خط ۲ نداریم.

۳- عدم جریان در خط ۲= عنصر A جریان را مسدود کرده یا جریان در خط ۱ نداریم.

۴- عدم جریان در خط ۱= جریان از طرف منبع نداریم.




**تصویر ۵-۱ : مدل درخت خطا برای قطع یا نرسیدن جریان به مصرف کننده**

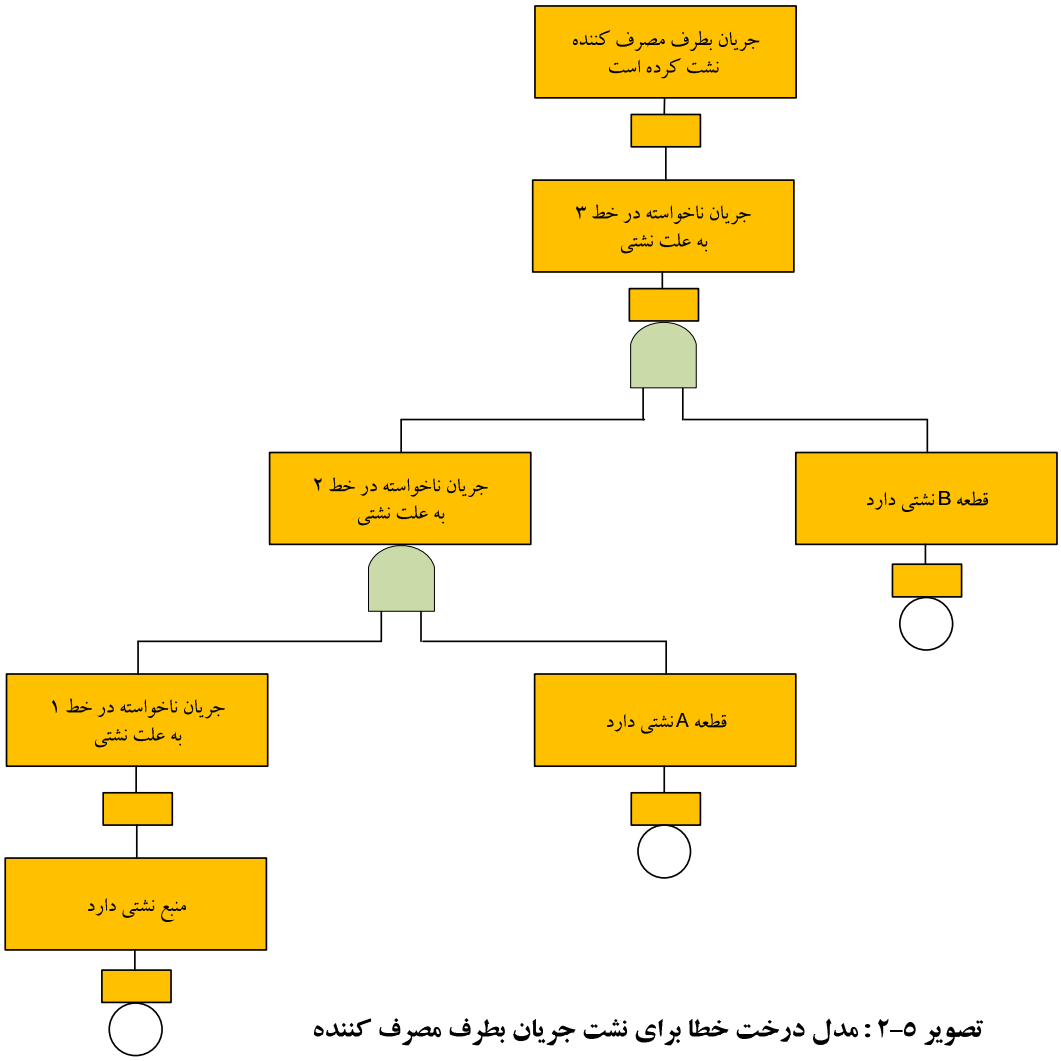
*** تصویر ۵-۲) منطق نشت جریان به طرف مصرف کننده**

۱- رسیدن جریان نشتی به مصرف کننده = وجود جریان نشتی در خط ۳

۲- وجود جریان نشتی در خط ۳= نشتی جریان از عنصر B و همزمان وجود جریـان نشـتی در خط ۲

۳- وجود جریان نشتی در خط ۲= نشتی جریان از عنصر A و همزمان وجود جریـان نشـتی در خط ۱

۴- وجود جریان نشتی در خط ۱= وجود جریان نشتی از طرف منبع




**تصویر ۵-۲ : مدل درخت خطا برای نشت جریان بطرف مصرف کننده**

مقایسه درخت‌ها در تصاویر ۵-۱ و ۵-۲ ، اهمیت تعریف رویداد رأس در رسم و ردیابی منطـق درخت خطا را نشان می‌دهد. همانطور که در تصویر ۵-۲ دیده  می‌شود ، در مدل نشت جریان

چند شکست باید به طور همزمان اتفاق بیفتد ولی در مورد قطع جریان (تصویر ۵-۱) شکست یکی از عناصر برای وقوع رویداد رأس، کافی می‌باشد. حالت‌های شکست عناصر هم متفاوت است و در صورت انجام محاسبات کمّی بایستی از داده‌های متفاوتی استفاده نمود.

## ۵-۲) مدل سازی شکست‌های علت مشترک[1]

منظور از شکست‌های علت مشترک (CCF ) ، شکست (خرابی) دو یا چند قطعه به طور همزمان یا در فاصله‌ای نسبتاً کوتاه است که به خاطر یک علت مشترک باشد. قطعه ، ممکن است هر عنصری از یک سیستم (مانند شیر کنترل، پمپ یا زیر سیستم‌هایی نظیر منبع تغذیه برق در صنایع نفت ) باشد . شکست‌های علت مشترک در تحلیل درخت خطا ، مانند دیگر شکست‌ها، به طور صریح دیده نمی‌شوند و در لفافه هستند بنابراین وابستگی یک قطعه را از نظر وظیفه و کارکرد به بخش تامین کننده سیستم (به عنوان مثال تغذیه برق یا سیم خنک-ساز) نشان نمی‌دهند که مثلاً اگر جریان از طرف این بخش قطع شد، چه شکست‌های چندگانه ای ممکن است بوجود آید . بنابراین منظور ما از شکست‌های علت مشترک، **یک وابستگی ضمنی است که می‌تواند باعث ایجاد شکست‌های یکسان در قطعات شبیه به هم شود.**

اهمیت، این نوع از شکست ها به حدی است که حذف آنها ممکن است منجر به اشتباه قابل توجه‌ای در تخمین احتمال وقوع رویداد رأس شود و بایستی در تحلیل درخت خطا مدل شوند. برای اطمینان از لحاظ نمودن شکست های علت مشترک ، بایستی عناصر و اجزای یکسان که

[1] Common Cause Failures = CCF

مستعد شکست هستند را شناسایی و مـدل نمـود. مثـال‌هـایی از CCF کـه ممکـن اسـت در سیستم رخ دهد، عبارتند از:

۱- یک عیب طراحی یا نقص مشترک در مواد سازنده قطعات مشابه یک کارخانـه کـه ممکن است منجر به شکست در کارکرد یا عدم تحمل شرایط محیطی طراحی شده بـرای آنهـا شود. مثال‌هایی از این دست ، ترک‌های آشکار نشـده در بدنـه موتورهـا و یـا اسـتفاده از مـواد ضعیف در پمپ‌ها ، می‌باشد.

۲- از تنظیم خارج شدن چند قطعه بدلیل یک خطای نصب مشترک ، مانند شـیرهای یکطرفه ای که ، بر عکس نصب شده‌اند و بعد از نصب ، بازرسی و بازبینی نشده‌اند.

۳- یک خطای تعمیر و نگهداری مشترک که منجر به عدم تنظیم چند قطعـه و عـدم کارائی آنها، شود. مانند شیرهای کنترلی که بعد از تعمیر به طور دقیق و در وضعیت مناسب در محل خود قرار نگرفته یا خوب کالیبره نشده باشند.

۴- شرایط ناهنجارمحیطی مشترک مانند ارتعاش، تشعشع، رطوبت یا آلودگی که منجر به شکست و خرابی چندین قطعه شود.

اگر علت مشترک خاصی مانند خطای تعمیر و نگهداری به طور شـفاف در درخـت خطـا آورده شود، در این صورت این خطا دیگر به عنوان CCF مدل نخواهـد شـد. عمومـاً خطاهـای علـت مشترک، سهم بالقوه‌ای در شکست قطعات مشابه، نظیر دو شـیر کـه مشخصـه‌هـای یکسـانی دارند، دو پمپ یکسان با مشخصه‌های فنی مشابه و غیره، دارند. همچنین اینگونه خطاها با بـالا رفتن تعداد قطعات یکسان، نقش و سهم بارزتری در وقوع رویدادهای بالا دست، پیدا می‌کنند.

برای تشریح اهمیت خطاهای علت مشترک به ذکر یک مثال ساده می‌پردازیم که بی‌ارتباط با وضعیت واقعی نیست. فرض کنید سه قطعه یکسان داریم که با شکست و خرابی هر سه، سیستم دچار شکست شود. این قطعات ممکن است شیر اطمینان، پمپ‌های هیدرولیک، کنترلر یا هر قطعه دیگری با کارکرد یکسان باشند. اگر هر قطعه یک مقدار احتمال شکست P برابر با ۰/۰۰۱ داشته باشد، در این صورت احتمال شکست همزمان هر سه قطعه با هم عبارت است از:

$$P_{independent} = p^3$$

یعنی

$$P_{independentt} = 1\times10^{-3}\bullet1\times10^{-3}\bullet1\times10^{-3}$$

یا

$$P_{independent}=1\times10^{-9}$$

در نتیجه احتمال شکست سه قطعه به طور مستقل، یکبار در یک بیلیون بار می شود.

حال، فرض کنید که امکان شکست و خرابی قطعات با علت مشترک نیز وجود دارد و احتمال وقوع این شکست مشترک برابر با یک درصد (یعنی ۰/۰۱) باشد. تعبیر این عدد این است که بگوییم **یک درصد از خطاها به علت** CCF است. به عنوان مثال ممکن است یک ترک مشترک در چندین قطعه وجود داشته باشد که به هنگام ساخت از چشم بازرسان بدور مانده باشد. به هر حال اگر به خاطر این عیب، یکی از قطعات دچار خرابی شود، دیگر قطعات نیز مصون نخواهند ماند.

بنابراین احتمال شکست مشترک ۳ قطعه، برابر است با:

$$P_{CCF} = 1\times10^{-3}\bullet1\times10^{-2}$$

یا

$$P_{CCF} = 1\times10^{-5}$$

در نتیجه احتمال شکست مشترک برابر یک بار در صد هزار بار بوده و **ده هزار مرتبه بزرگتر از احتمال شکست مستقل می‌باشد.**

در واقع CCF ، یک احتمال شرطی بوده و به معنای شکست و خرابی دیگر قطعات به شرط خرابی یک قطعه مفروض می باشد . بنابراین احتمال شکست مشترک ، کسری از شکست‌های دربرگیرنده تمامی قطعات مشابه می‌باشد و این مطلب اساس تخمین آن از داده‌ها است.*

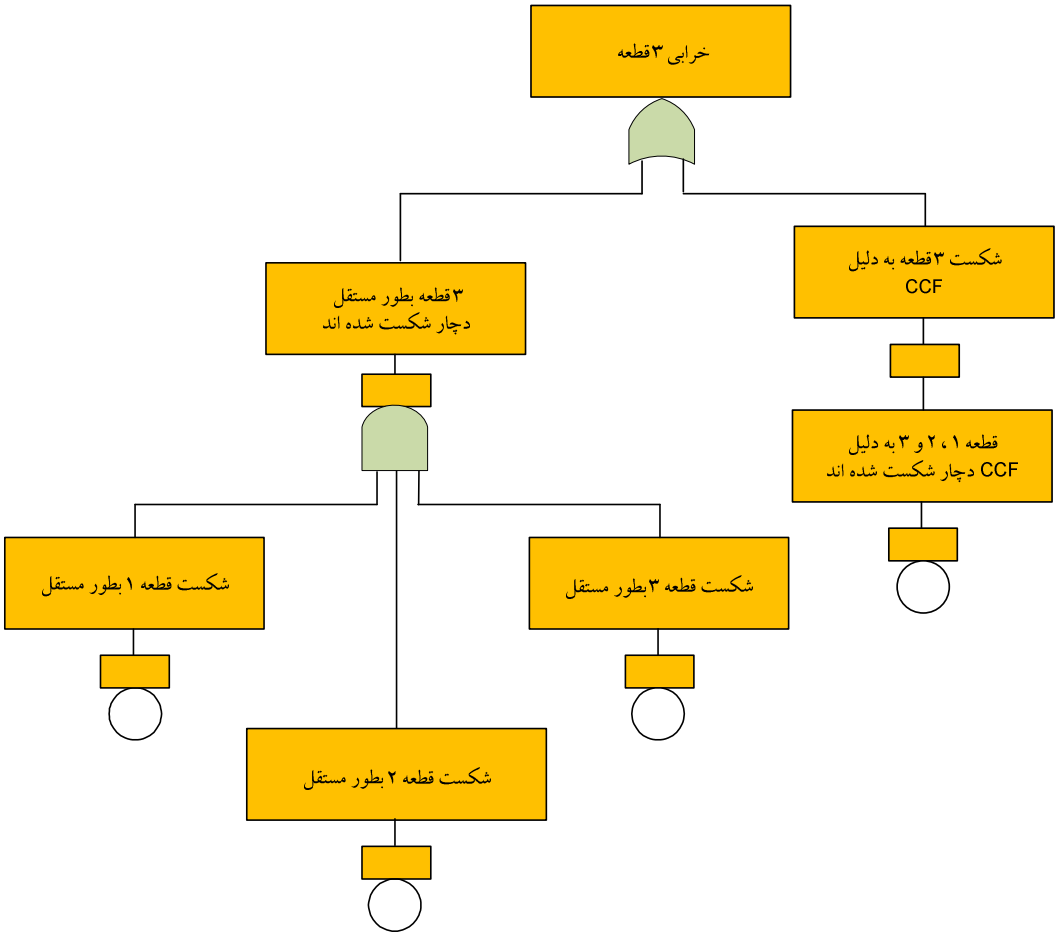
همانطور که مشاهده می‌شود ، CCF تمامی قطعات یک مجموعه مشابه را تحت تأثیر قرار می‌دهد و حتی اگر احتمال شکست آن ناچیز باشد ، می تواند احتمال شکست تمامی قطعات را بالا برده و باعث شکست سیستم شود. (در مثال بالا حتی اگر احتمال CCF یک در هزار بود ، احتمال شکست سیستم به خاطر CCF ، یک بار در یک میلیون بار می‌شد که هزار برابر احتمال شکست سیستم به علت شکست مستقل قطعات است).

شکست‌های علت مشترک در درخت خطا بایستی به طور مجزا مدل شوند. برای سه قطعه مثال بالا، ساختار درخت خطا را در تصویر ۵-۳ نشان داده‌ایم. همانطور که می‌بینید ، CCF به عنوان یک شاخه مستقل مستقیماً با یک گیت OR به رویداد رأس رسیده است . البته راه دیگری هم

* مدل‌های CCF متعددی وجود دارد. عمومی ترین مدل مورد استفاده ، مدل عامل بتا است که در آن حرف بتا نشان دهنده کسری از نرخ شکست است که مربوط به چندین قطعه یکسان می باشد. مدل های تفضیلی بسیاری که بین CCF ها با توجه به اندازه مختلف قطعات، تمایز قائل می شوند، توسعه یافته اند که از آن جمله می توان از مدل حروف یونانی چندگانه (Multiple Greek Letter) و مدل عامل آلفا نام برد.

وجود دارد ، بدین شکل که رویداد خطای CCF ، با هر رویداد پایه بطور مستقل OR شود که بیشتر در مدلسازی سیستم‌های پیچیده با وابستگی‌های تو در تو، مورد استفاده قرار می گیرد.

در تحلیل درخت خطا، نقش و سهم شکست‌های علت مشترک به عنوان رویدادهای مجزا بسیار مهم است. به هر حال برای فراموش نکردن و جا نگذاشتن شکست‌های علت مشترک ، یک قاعده ساده این است که هر کجا قطعات عامل یکسان داشتیم بایستی شکست‌های علت مشترک آنها را در نظر بگیریم.




**تصویر ۵-۳ : درخت خطای مربوط به شکست همزمان ۳ قطعه با در نظر گرفتن شکست های علت مشترک (CCF)**

در مورد قطعات یکسان غیر عامل یا ایستا ( مانند لوله ها و خطوط انتقال انرژی ) و در صورت اهمیت نقش آنها در بروز رویدادهای بالا دست، نیز می‌توان CCF را منظور نمود.

اگر در جایی برای آوردن CCF دچار تردید هستید ، بهترین تمرین این است که آن را در درخت خطا آورده و سپس از مطالعات و روش‌های تحقیقی دیگر مانند آزمون حساسیت برای یافتن اهمیت و نقش CCF در بروز رویداد رأس، استفاده کنید. اگر متوجه شدید که رویداد رأس به CCF مورد نظر، حساس است بایستی مطالعات دقیق تری در مورد خطاهای علت مشترک این قطعات انجام دهید.

### ۴-۵ مدلسازی خطاهای انسانی در درخت خطا

عملکرد نیروی انسانی محوریت مرکزی در ایمنی سیستم دارد. تعامل بین انسان و دستگاه در زمان عملیات، مقابله با حوادث، و تعمیر و نگهداری، همواره وجود دارد. این تعامل می تواند آثار و تبعات حوادث را به وسیله اقدامات کنترلی و بازیابی، کاهش دهد و از طرف دیگر آغازی برای رویدادهایی باشد که ناشی از خطاهای انسانی است.

عملکرد انسان نسبت به ماشین ازنظر انعطاف و پیچیدگی ، کاملاً متفاوت و غیر قابل پیش بینی است و انتظار می رود که در تعامل با سیستم های پیچیده، انسان، برتری های قابل توجه ای داشته باشد. اما خطاهایی که گاه از انسان در هنگام کنترل اوضاع و برقراری ارتباط با سیستم سر می زند، نه تنها وضعیت موجود را بهتر نمی کند بلکه بر وخامت آن می افزاید.

تحلیل قابلیت اطمینان انسانی[1] یا HRA ، روشی است که برای توصیف کیفی و کمی خطاهای انسانی اثرگذار بر ایمنی و قابلیت اطمینان سیستم، استفاده می شود . به خاطر اهمیت خطاهای انسانی، لحاظ کردن امکان رخداد این خطاها در تحلیل درخت خطا، تصویر واقعی تری را از شکست و ریسک در سرتاسر سیستم، ارائه می دهد. در اینجا به چگونگی مدلسازی خطاهای انسانی در درخت خطا و نحوه شناسایی و کمی کردن آنها در سیستم، می پردازیم . برای کسب اطلاعات بیشتر به منابع انتهای فصل مراجعه کنید.

**انواع خطاهای انسانی**

مثال هایی از خطاهای انسانی که قابلیت مدل کردن دارند عبارتند از:

- ✓ خطاهایی که مرتبط با تعمیر و نگهداری و آزمایش[2] هستند
- ✓ خطاهایی که باعث بروز رویدادهای آغازین[3] می شوند
- ✓ خطاهای اجرائی در زمان حادثه یا یک واقعه
- ✓ خطاهای ناشی از اقدام نامناسب
- ✓ خطاهای کشف و بازیابی[4]

اینک به شرح مختصری از هر یک از خطاهای فوق الذکر می پردازیم :

[1] Human Reliability Analysis =HRA
[2] Test
[3] Initial Event
[4] Detection and Recovery errors

**خطاهای مرتبط با تعمیر و نگهداری و آزمایش**

خطاهایی هستند که همراه با تعمیرات و آزمایش تجهیزات بوده و می توانند آنها را از کار انداخته یا در وضعیت نا مناسبی قرار دهند. مانند :

- عدم تنظیم مناسب یک قطعه یا سیستم بعد از انجام آزمایش
- کالیبراسیون اشتباه تجهیز
- اتصال اشتباه قطعات یک موتور الکتریکی
- سوار کردن دوباره[1] اجزاء یک شیر، پمپ، یا هر قطعه دیگر بطور غیر صحیح

این نوع خطاها را بایستی به طور صریح در یک درخت خطا، مدل نمود البته یک روش دیگر برای لحاظ نمودن خطاهای انسانی، عجین نمودن آنها به طور ذاتی با خطای در نظر گرفته شده با تجهیز می باشد. اما گاهی مثلاً خطای اپراتور در بسته نگه داشتن یک شیر را نمی توان در خطای ذاتی شیر یا خرابی آن ادغام کرد در اینگونه موارد بایستی این خطا را بطور جداگانه در هنگام رسم درخت خطا، بیاوریم. به هر حال در صورت آوردن خطای انسانی، بایستی آن را مانند دیگر شکست های اولیه ، به شکل یک رویداد پایه رسم کرد.

**خطاهایی که سبب بروز رویدادهای آغازین می شوند:**

خطاهایی که مربوط به عملکرد نامناسب انسان است و سبب شروع رویدادهایی نظیر آتش سوزی ، انفجار ، ترکیدگی لوله یا هر رویداد آغازین[2] دیگری می شود . البته این نوع خطاها

[1] Re-assembly

[2] منظور از رویداد آغازین (initial event) ، رویدادی است که منشأ و ریشه بسیاری از رویدادهای زنجیره ای دیگر می می گردد . به عنوان مثال بالا رفتن بیش از حد درجه حرارت بدنه یک موتور الکتریکی ، ممکن است باعث آتش سوزی در یک محیط قابل اشتعال گردد و این آتش سوزی در صورت عدم کارکرد مناسب سیستم اطفاء حریق ، مخزن حاوی بوتن را که

بیشتر در هنگام تحلیل کمی ریسک و در عدد فرکانس وقوع رویدادهای آغازین ، مورد استفاده قرار می گیرد و در تحلیل درخت خطا ، بطور ضمنی به آن توجه می شود . مگر آنکه آنها را در فرکانس وقوع رویدادهایی از این دست ، لحاظ نکرده باشیم یا اثرات چندگانه ای بر روی اجـزاء دیگر سیستم داشته باشند . منظور از اثرات چند گانه این است که مثلاً اپراتور علاوه بر ارتکاب خطای منجر به آتش سوزی ، بطور همزمان یکی از سیستم های اطفاء حریق را از کار بیاندازد .

**خطاهای اجرائی در زمان حادثه یا یک واقعه:**

این نوع خطاها به هنگام مقابله با تبعات یک حادثه یا واقعه در شرایط غیر عادی ، رخ می دهد. در هنگام ارتکاب این نوع خطا ، اپراتور اطلاعات دریافتی را بخوبی درک نکـرده و دسـتورالعمل های اجرایی (مثلاً نحوه مقابله بـا شـرایط اضـطراری ) را بـه شـکل اشـتباه انجـام مـی دهـد . خطاهایی از این دست در تحلیل درخت خطا به هنگام ارزیابی عکس العمل و نحوه پاسـخگویی انسان در وضعیت های اضطراری ، مدل می شوند . یعنی از نظر منطقی ، احتمال خطا در انجام دستورالعمل های اجرایی ، بررسی می گردد .

مثال هایی از خطاهای دستورالعملی ، غفلت در فعال کردن یا از کـار انـداختن یـک سیسـتم ، غفلت در تغییر وضعیت مثلاً یک شیر کنترل یا اشتباه در تشخیص مراحل یـک روش مقابلـه ، می باشد . در تحلیل درخت خطا ، خطاهای دستورالعملی با توجه به سیستم هایی که به خاطر

---

در مجاورت موتور قرار دارد ، گرم کند . حال اگر سیستم هشدار دهنده مخزن عمل نکند ، احتمال انفجار مخزن بسیار بالا می رود که این مسئله به نوبه خود حوادث پی در پی بعدی را بدنبال خواهد داشت . تمامی این زنجیره حوادث ، بخاطر گرم شدن بیش از حد بدنه موتور بود که از آن با عنوان رویداد آغازین (شروع یک اختلال در سیستم) ، یاد می کنیم .(مترجم)

ارتکاب خطاهایی از این نوع ، دچار شکست می شوند ، مورد تحلیل قرار گرفته و به عنوان دلیل بروز این شکست ها بطور صریح در درخت ، آورده می شوند .

**خطاهای ناشی از اقدام نامناسب :**

این خطاها گاهی خطاهای ارتکاب (اقدام)[1] نامیده می شوند و مشمول خطاهایی هستند که عاقبت مشکل ساز می شوند و اغلب همراه با خطاهای اجرایی بخش قبل هستند به عنوان مثال اپراتور بجای انجام دستوالعمل مناسب، دست به اقدامات دیگری بزند که به مشکل دامن بزند (در دسرساز شود)

به دلیل اینکه تمایز این نوع خطاها از دیگر خطاها مشکل است، و اختصاص یک عدد احتمال به آنها به هنگام کمی سازی سخت است اغلب به صورت صریح در درخت خطا آورده نمی شوند و به طور ضمنی در دیگر خطاها دیده می شوند.

**خطاهای کشف و بازیابی :**

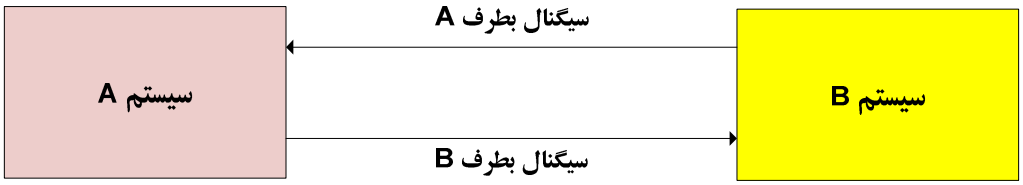
این خطاها مربوط به زمانی است که انسان در کشف و بازیابی یک شکست سیستمی ، اشتباه کند. برای مثال اگر قطعه ای خراب شود وبه موقع تعمیر گردد ممکن است به کاهش آثار یک حادثه کمک کند. اما خطا در کشف خرابی این قطعه و تعمیر آن در زمان مقتضی یک خطا از نوع کشف و بازیابی است. این نوع خطاها را بایستی یا به طور ضمنی در خرابی تجهیز دید یا به طور صریح تحت عنوان خطا در کشف و بازیابی در رفت خطا، لحاظ نمود.

[1] Errors of commission

به هر حال در مرحله تعیین حیطه زمانی و مکانی درخت خطا، بایستی نوع خطاهای انسانی که در درخت خطا دیده می شود را، مشخص نمود.

## ۴-۵ مدلسازی حلقه ها و باز خورد[1]

حلقه بازخورد شکل زیر را در نظر بگیرید. در این تصویر سیستم A سیگنالی را بـه سیسـتم B ارسال می کند. سیستم B نیز به نوبه خود سیگنالی را به سیسـتم A بازگشـت مـی دهـد. بـه عنوان مثال سیستم A ممکن است یک راکتور تولید کننده پلیمر باشد که پودر پلیمر همراه با گاز خود را به سیستم B که یک جداکننـده نیتـروژن اسـت ، مـی فرسـتد و سیسـتم B نیـز نیتروژن را به راکتور A بر می گرداند.

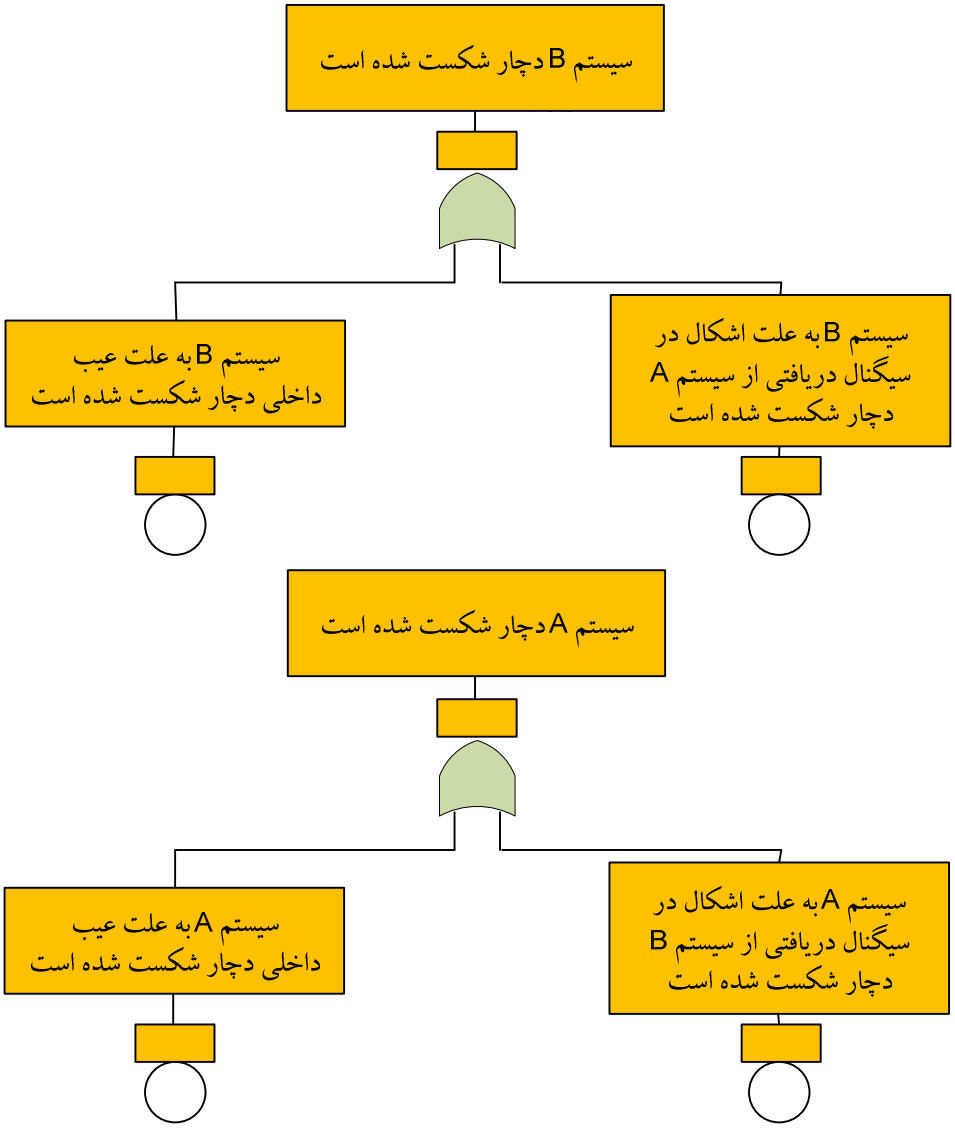



در درخت خطا ، مدل کردن سیستم های بازخورد نظیر تصویر بالا، مستلزم این است که مـدل درخت ، خطاهای سیستمی حاصل از سیگنال اشتباه سیستم دیگر را نیز مورد تحلیل قرار دهد. به هر حال بهتر است در مدلسازی درخت خطا از حلقه های بازخورد، اجتناب نمود. این حلقـه ها زمانی بروز می کنند که شکست سیستم B باعث اشکال در سیستم A و اشکال در سـیگنال

[1] Loops and Feedback

ارسالی از سیستم A (یا سیگنال دریافتی توسط سیستم B) سهمی در شکست سیستم B داشته باشد. در این صورت مدل بایستی نشان بدهد که چگونه سیستم A سبب بروز اشکال در سیستم B (و بالعکس) می شود. در تصویر ۵-۴ مدل درخت خطایی را مشاهده می کنید که شامل شکست های متقابل سیستم A و سیستم B بوده و حلقه ها را حذف کرده است .

در این تصویر ، تنها علل مربوط به شکست درونی و نه شکست های حاصل از باز خورد آورده شده است. برای مثال علت هایی که باعث بروز اشکال در سیستم A و به خاطر اشکال در سیگنال خروجی از این سیستم باشد ، در این مدل آورده نشده است . بنابراین حلقه ها در درخت خطا بریده یا حذف می شوند.




**تصویر ٥-٤ : درخت خطای مربوط به دو سیستم که بازخورد متقابل دارند**

مثلاً در مدل بالا در سمت راست گیت OR مربوط به شکست سیستم A ، تنها برای شکست های داخلی سیستم B ، بسط داده خواهد شد و به سیگنال مشکل ساز ارسالی از سیستم A به عنوان یکی از علل در شکست سیستم B ، پرداخته نمی شود . این قاعده کلّی یعنی لحاظ نمودن تنها شکست های درونی سیستم مبدأ سیگنال، در مورد تمامی سیستم هایی که با هم

تعامل دارند، بکار می رود و با استفاده از این قاعده دیگر حلقه ای در درخت خطای رسم شده نخواهیم داشت.

**نامگذاری نمادهای درخت خطا**

عامل اصلی برای نامگذاری گیت ها و رویدادهای پایه، اطمینان از این مسئله است که مقادیر احتمال صحیحی برای برش ها محاسبه شود. اگر رویداد پایه ای در چند جای درخت تکرار شود و نام های متفاوتی داشته باشد، در هنگام محاسبه برش های حداقل، به اشتباه افتاده و مقادیر نا معقولی برای رویداد رأس، بدست خواهد آمد .

با نامگذاری گیت ها و رویدادهای پایه می توان از آنها به عنوان شناسه یا کد کامپیوتری این رویداد ها استفاده نمود . در محاسبات کامپیوتری گیت ها و رویدادها با یک شناسه (identifier) مشخص می شوند. شناسه ها بایستی مرتبط و محدود باشند. معمولاً شناسه نوع قطعه و حالت شکست آن را نشان می دهد. برای مثال MOV[1] علامت شیرهایی است که با موتور کار می کنند، PMP[2] علامت پمپ و TNK[3] نشانه تانک می باشد.

این علائم بایستی قبل از رسم درخت خطا به شکل انحصاری معلوم شوند. برای بیان حالت شکست در یک شناسه می توان از عباراتی نظیر FTO[4] به معنی خطا در باز شدن، FTC[5] به معنی خطا در بسته شدن و INOP[6] به معنی غیر قابل استفاده، بهره گرفت.

[1] **M**otor **O**perated **V**alve
[2] **P**u**MP**
[3] **Ta**a**NK**
[4] **F**ailure **T**o **O**pen
[5] **F**ailure **T**o **C**lose
[6] **INOP**erable

بنابراین MOV-1233-FTO بدین معنی است که شیر شماره 1233 که راه انداز آن موتور است خطا در باز شدن دارد. اگر تعدد سیستم داشته باشیم می توان هر سیستم را با کد مربوط به خود در اول شناسه ذکر کرد. جدول ۵-۱ جدولی نمونه از این شناسه ها است. در این جدول HX علامت مبدل حرارتی[۱] ، IN نماد مبدل یا معکوس ساز[۲] ، IR نشانه یکسوساز قابل تنظیم[۳] ، IV علامت تنظیم کننده الکتریسیته ساکن[۴] ، LC نماد مدار منطقی[۵] و LS نشانه کلید سطح سطح مایع است . همچنین در ستون حالت شکست (ستون دوم) ، حرف F علامت شکست[۶] یا خرابی ، J پاره شدن تیوب ، P مسدود شدن یا گرفتگی ، D نقص یا عیب و L نشان دهنده (سطح) پایین است . بنابراین مثلاً HXP بیانگر مسدود شدن مبدل حرارتی است .

**جدول ۵-۱ : یک نمونه از نامگذاری قطعات و حالت شکست آنها در فرآیند**

| Component Type | Component Failure Mode | Description |
|---|---|---|
| HX | F | Heat Exchanger Cooling Capability Fails |
| HX | J | Heat Exchanger Tube Rupture |
| HX | P | Heat Exchanger Plugs |
| IN | F | Inverter No Output |
| IR | F | Regulating Rectifier No Output |
| IV | F | Static Voltage Regulator No Output |
| LC | D | Logic Circuit Fails to Generate Signal |
| LS | D | Level Switch Fails to Respond |
| LS | H | Level Switch Fails High |
| LS | L | Level Switch Fails Low |

[1] Heat Exchanger
[2] Inverter
[3] Regulating Rectifier
[4] Static Voltage Regulator
[5] Logic Circuit
[6] Failure

### ۵-۷ قوانین رسم درخت خطا

این قوانین به منظور محدود کردن حیطه زمانی، مکانی و یا تعیین سطح جزئیات درخت خطا، بکار می‌روند و تأثیری در نتایج کلی حاصل از درخت نخواهد داشت و بایستی قبل از استفاده از نظر قابلیت و کاربرد، بررسی شوند.

۱- مدلسازی را تا بالاترین سطحی که داده (اطلاعات) موجود بوده و تداخل سخت افزاری مشترکی با دیگر رویداد های سهیم ، وجود نداشته باشد، ادامه دهید. در واقع معنی این جمله، مدلسازی در سطح قطعات عمده و اصلی مانند شیر، پمپ و غیره است. مدلسازی در سطحی پایین‌تر از این، تنها تلف کردن وقت و همچنین اغلب همراه با خطا در اعداد احتمال بدست آمده است .

۲- خطاهای مربوط به سیم کشی بین قطعات الکترونیکی را مدل نکنید. خطای سیم‌بندی (مانند اتصال کوتاه به زمین یا سیم فاز) در مقایسه با قطعات اصلی و عمده، احتمال شکست خیلی پایین‌تری دارند. فقط در صورتیکه خطاهای شاخص مهمی نباشد یا سیم‌کشی تحت الشعاع شکست‌های دیگر (مثلا آتش سوزی) قرار بگیرد ، بایستی خطاهای مربوط به آن را در درخت خطا آورد . همچنین اگر قرار باشد خطاهای مربوط به خود سیم‌ها مورد بررسی قرار گیرد (برای مثال در مورد فرسودگی کابل‌هایی که مرتباً توسط تعمیر کاران مورد استفاده قرار می‌گیرند)، این نوع خطا در تحلیل درخت خطا، لحاظ می‌شود.

۳- خطاهای مربوط به لوله‌های رابط بین قطعات فرآیندی را، مدل نکنید. دلیل این مطلب، مشابه همان است که در دومین قاعده آورده‌ایم. خطاهای مرتبط با لوله‌های رابط ، عموماً

مقادیر احتمال ناچیزی دارند. البته مانند حالت قبل اگر هدف، مدل کـردن خطاهـای سیسـتم لوله کشی باشد یا در صورت عدم وجود خطاهای شاخص دیگر ، این نوع خطا در تحلیـل آورده می‌شود.

۴- شرایط خارج از طراحی را مدل نکنید. عموماً، انتظـار نمـی‌رود کـه قطعـات در محـدوده‌ای خارج از شرایط طراحی خود، کار کنند. بنابراین خطاهای بیرون از محـدوده طراحـی قطعـه در تحلیل آورده نمی‌شود. در شرایط خاص و در صورت لزوم برای لحاظ کـردن ایـن نـوع خطاهـا بایستی دلایل توجیه کننده آورده شود.

۵- علل شکست مشترک (CCF) را برای تمام قطعات یکسان و دارای یدک، مدل کنید. قطعات عامل (Active) عموماً مکانیکی یا الکترومکانیکی بـوده و تغییـری در وضـعیت سـیگنال‌هـا یـا جریان بوجود می‌آورند (به طور مثال پمپ‌ها، شیرهای موتوردار، موتورهـا و قطـع کننـده‌هـای مدار[1]) و خطاهای مشترک زیادی به علت تعامل این قطعات با محیط و عملیات، وجود دارد. در گذشته، خطاهای علت مشترک تمامی قطعات یکسان در درخت خطا آورده می‌شد و در پایـان یک تحلیل حساسیت بر روی آنها صورت می‌گرفت و خطاهای مشترکی که حساس‌تر بودند، بـا دقت بیشتری مورد بررسی قرار می‌گرفت.

۶- خطاهای انسانی ارتکابی را مدل نکنید . این خطاها مربوط به اموری است که قابل مشـاهده و اثبات نیست . دلیل مدل نکردن این نوع خطاها این است که تعداد آنها در هر اقـدام انسـانی قابل شمارش نیست .

[1] Circuit Breaker

۷- گیت های AND که بیش از چهار ورودی دارند را در صورتیکه گیت های مشابه با سه ورودی یا کمتر در جای دیگری از درخت وجود داشته باشد را مدل نکنید . به عنوان مثال اگر یک گیت AND دارای ورودی های A ، B ، C و D باشد و در جای دیگری از درخت خطا ، گیت AND دیگری با ورودی های مثلاً B و C موجود باشد . گیت اول را بایستی حذف نمود. این قانون بدین معنا است که **در صورت وجود گیت های AND با ترکیب ورودی های مرتبه پایین ، گیت های AND با ترکیب ورودی های مرتبه بالا حذف می گردند .**

۸- اگر به این اطمینان رسیده‌اید که عدد احتمال یکی از ورودی های یک گیت OR از دیگر ورودی‌ها بسیار کمتر است ، آنرا در درخت نیاورید. البته در این حالت می‌توانید این نوع ورودی‌ها را (که ممکن است شامل رویدادهای فرعی زیادی باشند) به صورت رویداد توسعه نیافته بیاورید تا در صورت لزوم و پس از رسم کامل درخت، مورد بررسی بیشتری قرار بگیرند.

### ۵-۸ ) اطمینان از صحت درخت خطای رسم شده

پس از رسم درخت خطا، بایستی اطمینان پیدا کنیم که دقت کافی در رسم آن و رعایت قواعد اصلی رسم شده است. این اطمینان به روش‌های زیر امکان پذیر است:

۱- برش‌های حداقل درخت را به دست آورید. کم رتبه‌ترین برش را شناسایی کرده و بررسی کنید آیا به درستی همان مسیر شکستی است که به رویداد رأس می‌رسد. برای این کار می‌توانید از طرح، نقشه یا نمودار سیستم استفاده کنید. اگر فقط یک یا دو قطعه در این برش

با پایین‌ترین رتبه وجود داشته باشد، می‌توان از روش **تحلیل حالات شکست و آثار آن**[1] نیز بهره برد.

۲- رویدادهای پایه و شکست‌هایی را که در پایگاه داده سیستم شما ثبت شده است را شناسایی کنید. ببینید این خطاها در درخت خطای رسم شده هم وجود دارند یا خیر. این بررسی، کامل و شامل بودن درخت خطا را تأیید می‌کند.

۳- مسیرهای موفقت[۲] درخت خطا را به دست آورید. کوچکترین مسیر موفقت رویداد رأس را مشخص کرده، بررسی کنید آیا واقعاً این مسیر جواب می‌دهد. این روش شبیه به روش شمارهٔ اول است به جزء آنکه به جای شکست از موفقیت استفاده می‌کند تا درخت خطا را از نظر عرضی نیز تأیید نماید.

۴- اگر روش‌های ۱ و ۳ شامل قطعات زیادی می‌شود که بررسی اینکه آنها واقعاً به شکست یا موفقیت می‌رسند ، مشکل باشد. می‌توانید این روش ها را برای رویدادهای فرعی یا میانی که برشهای کم رتبه و قطعات کمتری دارند، انجام دهید.

۵- احتمال برش‌ها و عناصر آنها را بررسی کنید و ببینید این اعداد و نتایج منطقی و معقول هستند . معمولاً کم رتبه‌ترین برش‌ها که شامل شکست قطعات عامل هم باشند، اعداد احتمال بالاتری دارند. همچنین اگر شکست‌های علت مشترک (CCF) یا خطاهای انسانی در درخت، مدل شده باشند، به نسبت نقش بالاتری را خواهند داشت.

[1] FMEA

[۲] برای کسب اطلاعات بیشتر در مورد مسیرهای موفقیت به ضمیمه **د** مراجعه کنید .

۶- روش قبل را در مورد خطاهای سیستم‌های فرعی یا ماژول‌ها تکرار کنید. و مقـادیر احتمـال آن‌ها را با آنچه که قبلاً تجربه شده است، مقایسه کنید . عموماً اعداد احتمال رویدادهای فرعی در مقایسه با احتمال رویداد رأس، بزرگتر هستند.

۷- بررسی کنید که آیا احتمال محاسبه شده برای رویداد رأس معقولانه است. این احتمال را با نوع مشابه‌ای که قبلاً انجام شده، مقایسه کنید. عدد احتمال خیلـی پـایین بـرای رویـداد رأس نظیر $1\times10^{-9}$ و یا پایین تر ، غیرمنطقی بوده و عموماً نشان دهنده این است که راه‌هـای بسـیار محتمل‌تری که منجر به وقوع رویداد رأس می‌شود ، شناسایی نشده‌اند. (به خاطر داشته باشـید احتمال نابودی کامل کره زمین، $1\times10^{-9}$ می‌باشد)

**مراجع :**

1. A. Mosleh, *Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis*, NUREG/CR-5801, US Nuclear Regulatory Commission , 1993.
2. D. Gertman and H. Blackman, Human Reliability and Safety Analysis Data Handbook, John Wiley and Sons , 1994.
3. E. Dougherty and J. Fragola, *Human Reliability Analysis: A Systems Approach with Nuclear Power Plant Applications*, Wiley, New York, 1988.

# فصل ۶ : ارزیابی کیفی درخت خطا و فرمول های اساسی احتمال

در این فصل به ارزیابی کیفی درخت خطا می‌پردازیم. این ارزیابی کاربرد جبر بـولی را در نحوه نوشتن معادلات مربوط به هر گیت نشان داده و به شرح فرمول‌هـای اساسـی احتمـال برای هر نوع گیت می‌پردازد. همچنین روشی برای به دست آوردن مجموعه برش‌هـای حـداقل درخت خطا و مجموعه مسیرهای حداقل آن در درخت موفقیت، ارائه داده و دیدگاه دیگـری را برای حل درخت خطا با استفاده از نمودارهای تصمیم دودوئی[۱]، تشریح می‌کند.

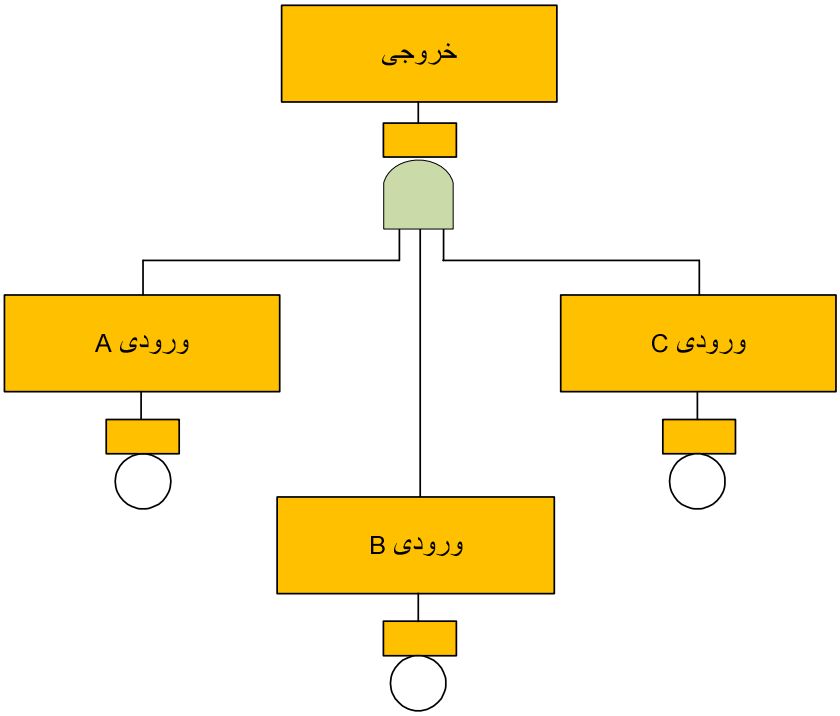
## ۶-۱) کاربرد جبر بولی درتحلیل درخت خطا

اکنون که درخت خطا به عنوان یک نمودار منطقی از زنجیره رویدادهای منتهی به وقوع یـک رویداد خاص ، درک شد. تعریف دقیق‌تری از رویدادهای درخت خطا ارائه می‌دهیم:

اگر رویدادی توسط رویدادهای دیگر، برانگیخته و شروع شود به آن **خطا**[۲] و اگر خود به تنهـایی یک آغازگر اصلی باشد، **شکست**[۳] نامیده می‌شود.

در درخت خطا ، رویدادهای خطا به رویدادهای شکسـت (و بـالعکس) بـا اسـتفاده از نمادهـای خاصی به هم وصل می‌شوند. همانطور که در فصل چهارم شرح داده شد، نماد اساسـی[۴] گیـت[۵] می‌باشد و هر گیت خروجی و ورودی‌هایی نظیر شکل ۶-۱ دارد.

[1] **B**inary **D**ecision **D**iagram =BDD
[2] Fault
[3] Failure
[4] Basic symbol
[5] Gate




**تصویر ٦-١ : نقش گیت در درخت خطا**

خروجی گیت، رویداد خطـایی بـا سـطح بـالاتر و ورودی‌هـای آن نسـبت بـه خروجـی، سـطح پایین‌تری دارند. رسم درخت خطا از رویدادهای خطای با سطح بالا شروع شده و به رویداد های شکست (پایه) سطح پایین ختم می گردد . در این فرآیند و به هنگام شـرح و بسـط رویـدادها دائماً در مورد گیت های مورد استفاده و مناسب برای ارتباط بـین رویـدادها ، بحـث و تصـمیم گیری می شود . دو طبقه[1] گیت پایه ، گیت AND و گیت OR می‌باشد. چـون ایـن گیـت‌هـا، رویدادها را با روشی مشابه عملگرهای بولی به هم ربط می‌دهند ، **تناظر یک به یکی بین نمـایش جبر بولی و درخت خطا وجود دارد.** قوانین جبر بول به طور خلاصه در ضمیمه الف آمده است.

[1] Category

**گیت OR**

همانطور که در فصل چهارم گفته شد، نماد گیت OR ،  است که اجتماع رویدادهای وصل شده به آن را ارائه می‌دهد.

یعنی یکی یا همهٔ رویدادهای ورودی بایستی رخ بدهند تا رویداد خروجی به وقوع بپیوندد. گیت OR معادل نماد + درجبر بولی است و به علت شباهت عملکرد این گیت با این نماد ، گاهی اوقات در داخل نماد گیت OR ، علامت + گذاشته می شود (تصویر صفحه بعد را ببینید). به عنوان مثال برای گیت OR با دو ورودی که در تصویر ۶-۲ رسم شده، عبارت معادل آن در جبر بولی به شکل Q=A+B آمده است. در این تصویر ، یکی از رویدادهای A یا B یا هر دو آنها برای وقوع رویداد Q بایستی رخ دهند. تعمیم این قضیه برای n رویداد ورودی معادله بولی زیر است:

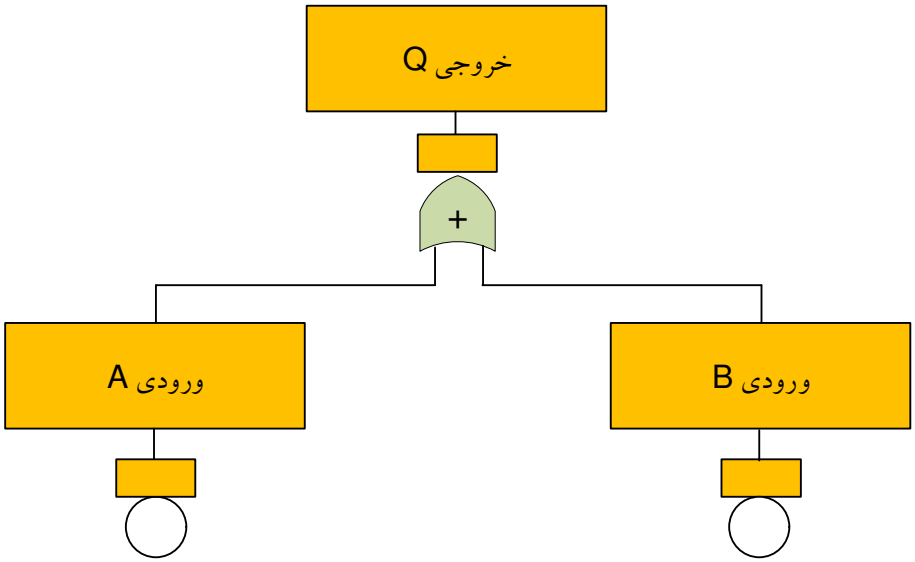
$$Q = A_1 + A_2 + A_3 + \ldots + A_n$$

معادلات مربوط به تصویر ۶-۲ بر حسب احتمال، عبارت است از:

$$P(Q) = P(A) + P(B) - P(A \cap B)$$ **معادله ۶-۱**

و یا

$$P(Q) = P(A) + P(B) - P(A)P(B|A)$$




**تصویر ٦-٢: یک گیت OR با دو ورودی**

مشاهده می‌شود که:

- اگر A و B رویدادهایی نامتداخل[1] باشند در این صورت $P(A \cap B) = 0$ است و داریم :

$$P(Q) = P(A) + P(B)$$

- اگر A و B رویدادهایی مستقل[2] باشند، داریم : $P(B|A) = P(B)$ و

$$P(Q) = P(A) + P(B) - P(A)\,P(B)$$

- اگر رویداد B کاملاً به رویداد A وابسته باشد (یعنی با وقوع A ، رویداد B نیز اتفاق بیفتد) ، در این صورت: $P(B|A) = 1$ و

از معادله $P(Q) = P(A) + P(B) - P(A)$ نتیجه می شود : $P(Q) = P(B)$

[1] Mutually exclusive
[2] Independent

- تقریب $P(Q) \approx P(A) + P(B)$ ، همواره تخمین محافظه کارانه‌ای از رویداد خروجی Q است یعنی برای هر رویداد A و B داریم :

$$P(A) + P(B) \geq P(A) + P(B) - P(A \cap B)$$

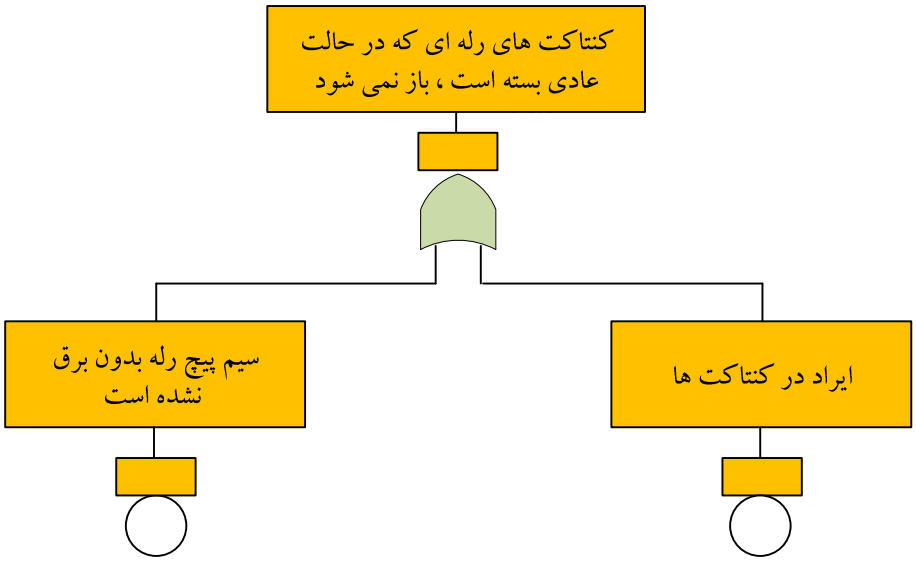
- اگر A و B ، رویدادهایی مستقل و کم احتمال (مثلاً با احتمال کمتر از ۰/۱)، باشند در این صورت، $P(A \cap B)$ درمقایسه با $P(A) + P(B)$ ، کوچک بوده و $P(A) + P(B)$ تقریب دقیقی برای $P(Q)$ خواهد بود.
- در یک گیت OR انحصاری با دو ورودی A و B ، رویداد خروجی Q وقتی اتفاق می‌افتد که A یا B و نه هر دو رخ بدهند. عبارت احتمالی رویداد خروجی Q در یک گیت OR انحصاری عبارت است از:

$$P(Q)_{\text{EXCLUSIVE OR}} = P(A) + P(B) - 2P(A \cap B) \qquad \textbf{معادله ۶-۲}$$

با مقایسه معادلات (۶-۱) و (۶-۲) مشاهده می‌کنیم که اگر A و B مربوط به شکست قطعات کم احتمال باشند، تفاوت بین عدد احتمال بین دو عبارت ، ناچیز است. به همین دلیل است که تمایز بین گیت OR انحصاری و معمولی، در صورت پایین بودن عدد احتمال شکست‌ها و استقلال آن‌ها، ضرورتی ندارد.

البته در صورت وجود یک وابستگی قوی بین رویدادهای ورودی یا بزرگ بودن احتمال وقوع شکست‌ها ، بایستی گیت OR انحصاری را متمایز نمود. چرا که دراین حالت عبارت اشتراک به حد کافی بزرگ و معنی‌دار بوده و در نتیجه به دست آمده، تأثیر گذار خواهد بود.

تصویر ۶-۳ مثالی واقعی از یک گیت OR برای مجموعه‌ای از کنتاکت‌ها است که در حالت عادی بسته می‌باشند.




**تصویر۶-۳ : مثالی از گیت OR با دو ورودی**

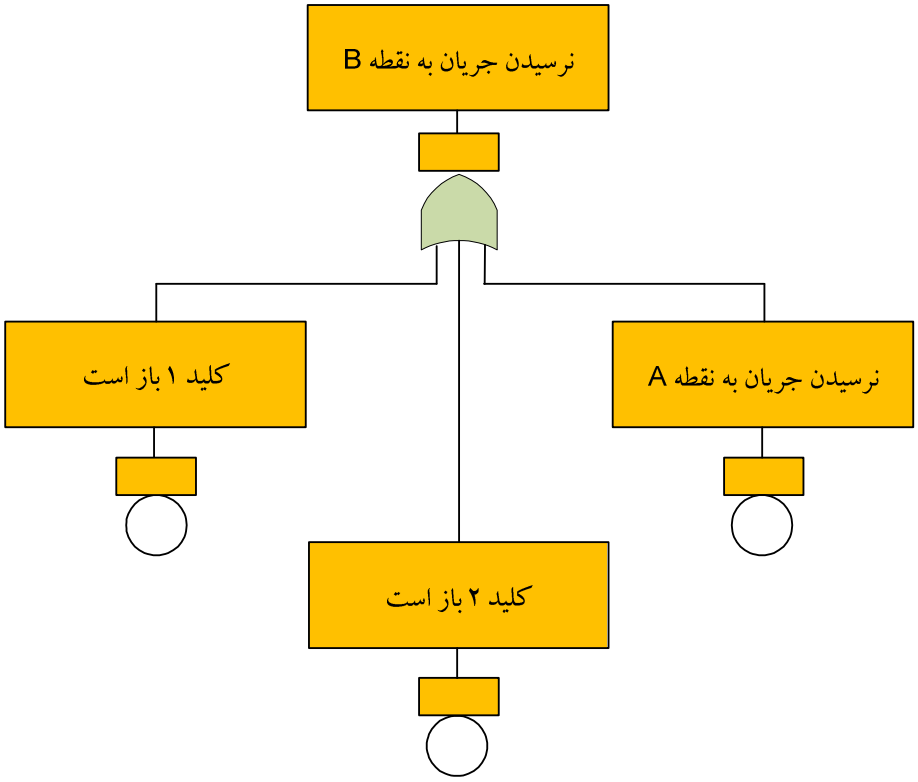
این گیت OR معادل عبارت بولی زیر است:


اگر رویداد باز نشدن کنتاکت های رله بر حسب Q و رویدادهای سیم پیچ رله بدون برق نشده و کنتاکت‌ها ایراد دارند را به ترتیب با حروف A و B نشان دهیم ، در این صورت معادله بولی شکل ۶-۳ می‌شود: **Q= A+B**

به عنوان مثالی دیگر، کلیدهای سری شده تصویر ۶-۴ را در نظر بگیرید.

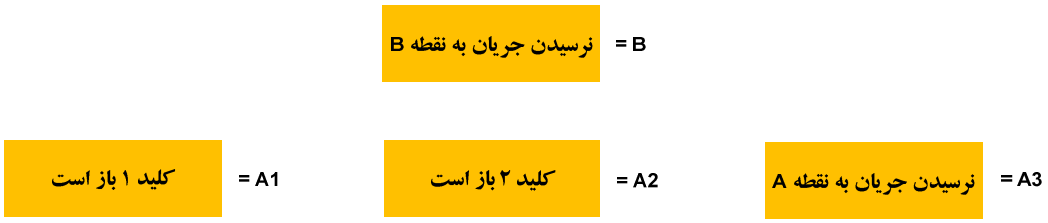

**تصویر ٦-٤ : دو کلید سری**

حروف A و B ، نقاطی از سیم می‌باشند ، با فرض ناچیز بودن خطای سیم ها ، نمایش درخت خطای رویداد **عدم جاری شدن جریان به سمت نقطه B** در شکل ۶-۵ رسم شده است:



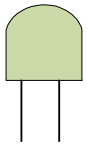

**تصویر ٦-٥ : مثالی از گیت OR با ۳ ورودی**

اگر رویدادها با نمادهای زیر نمایش داده شوند،




معادل بولی درخت فوق $B=A_1+A_2+A_3$ می‌شود. رویداد B به وقوع می‌پیوندد اگر رویدادهای $A_1$ یا $A_2$ یا $A_3$ رخ دهند.

**گیت AND**

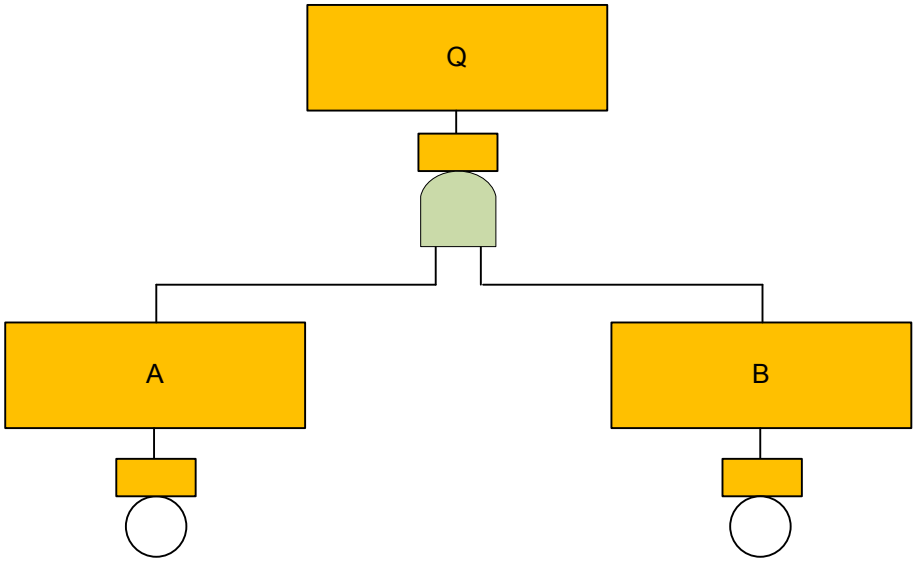
همانطور که در فصل چهارم ذکر شد نماد گیت AND  است کـه اشـتراک رویدادهای وصل شده به آن را نمایش می‌دهد.

گیت AND معادل نماد «۰» در جبر بول است. تمامی رویدادهای متصل شده به گیت AND بایستی رخ دهند تا رویداد خروجی گیت به وقوع بپیوندد. در تصویر ۶-۶ ، یک گیت AND بـا دو ورودی را مشاهده می کنید که معادله بولی آن Q=A.B است.

به علت شباهت عملکرد این گیت با نماد «۰» در جبر بولی، گاهی اوقات در داخل نمـاد گیـت AND ، علامت «۰» می گذارند . (تصویر ۶-۶ را ببینید) برای گیت AND با n رویداد ورودی عبارت بولی معادل زیر داریم:

$$Q = A1 \bullet A2 \bullet A3 \bullet \ldots \bullet An$$

در این حالت، رویداد Q تنها وقتی رخ می‌دهد که تمامی رویدادهای $A_i$ ، رخ دهند.




**تصویر ٦-٦ : گیت AND با ۲ ورودی**

از نظر احتمال برای دو رویداد A و B تصویر ۶-۶ داریم:

$$P(Q) = P(A)\,P(B|A) = P(B)\,P(A|B)$$

از معادله بالا نتایج زیر نتیجه می‌شود :

- اگر A و B رویدادهایی مستقل باشد داریم :

$P(B|A)=P(B),\ P(A|B)=P(A)$ و در نتیجه $P(Q)=P(A)\,P(B)$

- اگر A و B مستقل نباشند ، P(Q) ممکن است به طور معنی داری بزرگتر از P(A)P(B) باشد. برای مثال اگر در شرایط افراطی، B کاملاً وابسته به A باشد یعنی هر جا که A رخ دهد، B نیز رخ دهد، در این صورت $P(B|A)= 1$ است و در نتیجه $P(Q) = P(A)$ می باشد .

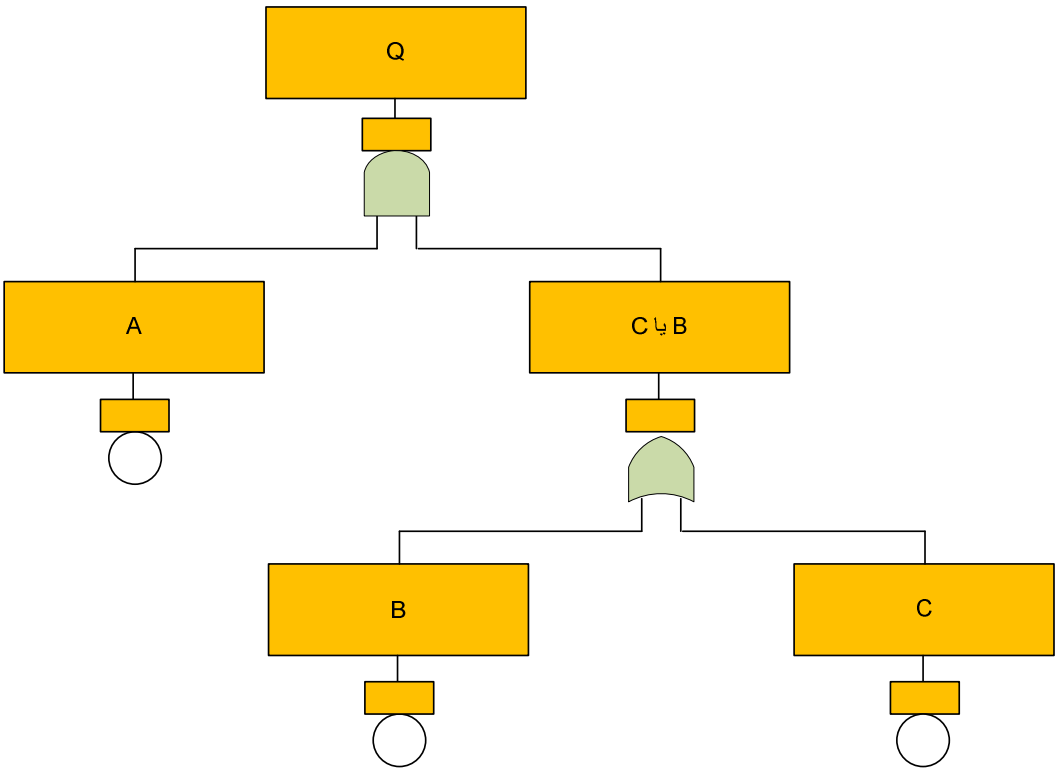
وقوع رویداد Q، مشروط به وقوع همه رویدادهای ورودی به آن است . این ارتباط علّی ، نقطه تمایز بین گیت AND و گیت OR است. در حالت کلی اگر برای وقوع یک رویداد ، رخداد

یکی از رویدادهای ورودی کافی باشد ، از گیت OR و اگر رخداد همزمان رویـدادهای ورودی ، شرط وقوع رویداد خروجی باشد ، از گیت AND استفاده می شود .

این بحث را با مثالی که نحوه بازسازی درخت خطا را توسط جبر بولی نشـان مـی‌دهـد، ادامـه می‌دهیم. معادلهٔ $D = A \cdot (B+C)$ را در نظر بگیرید. درخت خطای مربوط به آن در تصویر ۶-۷ آمده است. حال براساس قانون 3a از ضمیمه الف ، رویداد D را می‌توان به شکل زیر نشان داد.

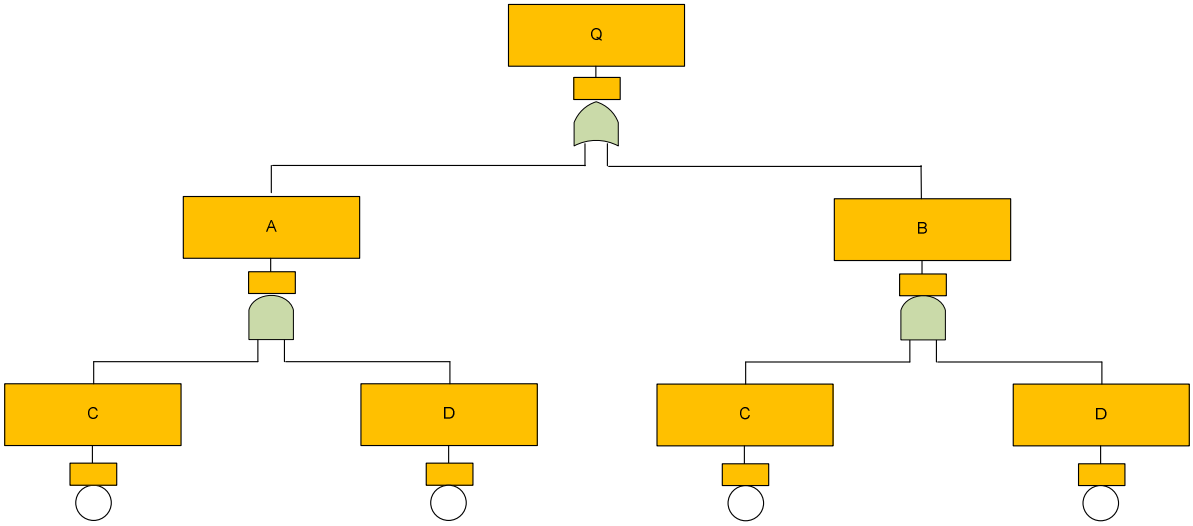
$$D = (A \cdot B) + (A \cdot C)$$

درخت خطای مربوط به معادله فوق، در تصویر ۶-۸ نشان داده شده است .




**تصویر ٦-٧ : ساختار درخت خطا برای $D = A \cdot (B+C)$**

ظاهراً ساختار دو درخت خطای رسم شده در تصاویر ۶-۷ و ۶-۸ متفاوت هستند، در صورتیکه معادل می‌باشند . **بنابراین تنها یک درخت خطای صحیح برای یک مسئله وجود نداشته، ممکن است اشکال متفاوت اما معادلی برای آن وجود داشته باشد**. در حقیقت از قوانین جبری بولی می‌توان برای دوباره سازی[1] درخت به شکلی ساده‌تر و قابل فهم تر، بهره برد . بعدها از قوانین جبر بولی برای به دست آوردن شکلی از درخت خطا که شکل **مجموعه برش حداقل** [2] نامیده می‌شود و اجازه کمی سازی معادلات کیفی را به روشی ساده به ما نشان می‌دهد، استفاده خواهد شد.




**تصویر ٦-٨: درخت خطای معادل تصویر ٦-٧**

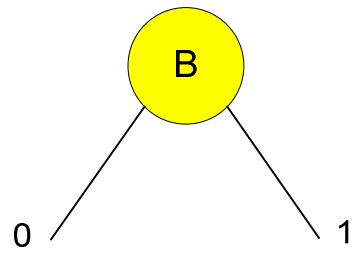
[1] Restructure
[2] Minimal Cut Set = MCS

### ۶-۲) دیاگرام‌های تصمیم دودوئی[1] (BDD)

پیشرفت‌های جدیدی که اخیراً در منطق دیجیتال، رخ داده است، دستورالعمل دیگری را برای تحلیل درخت خطا، معرفی کرده است. این روش که براساس دیاگرامهای تصمیم دودوئی (BDD) می‌باشد، مستقیماً با عبارات منطقی و نه مجموعه برش‌ها، سرو کار دارد. یک دیاگرام تصمیم دودوئی را می توان به عنوان نمایشی گرافیکی از ساختمان داده یک تابع منطقی، در نظر گرفت.

دیاگرامی که در درخت خطا مورد استفاده قرار می‌گیرد، معروف به BDD با رتبه‌بندی کاهش یافته[2]، است. کاهش یافته به این معنی که BDD به شکلی حداقل رسیده است و رتبه‌بندی به گونه‌ای است که متغییرها در رتبه‌ای یکسان در هر مسیر، ظاهر می‌شوند. برای کسب اطلاعات بیشتر در مورد روش BDD، مراجع [2] ,[1] پایان فصل را ببینید.

یک BDD از روی درخت خطا و با روشی برگشتی، یعنی از پایین به بالا[3] ساخته می‌شود. هر رویداد پایه، گره‌ای منفرد در BDD دارد. برای مثال BDD رویداد پایه B در تصویر ۶-۹ آمده است.



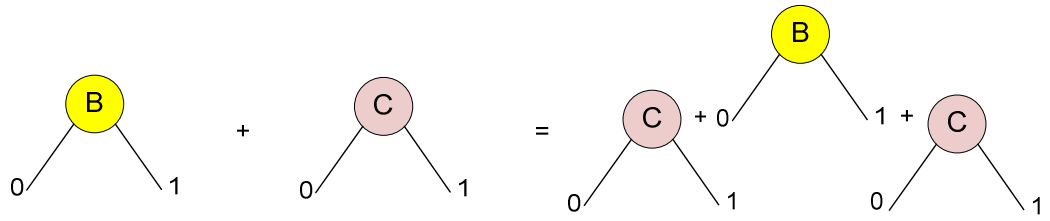

**تصویر ٦-۹ : BDD برای رویداد پایه B**

[1] Binary Decision Diagram = BDD
[2] Reduced Ordered BDD
[3] Bottom-up

با شروع از انتهای (کف[1]) درخت خطا[2] ، برای هر یک از رویدادهای پایه یک BDD ساخته شده و سپس براساس منطق تعریف شده توسط گیت‌های بالادست، این BDD ها ، ترکیب می‌شوند.

دیاگرام تصمیم دودوئی رابطهٔ OR دو رویداد B و C (یعنی B+C ) با اعمال تابع OR بر روی دیاگرام دو رویداد B و C ، شکل می‌یابد. چون B در ابتدای رابطه آمده، گره ریشه[3] محسوب شده و بنابراین BDD مربوط به رویداد C با هر گره فرزند[4] B ، OR می‌شود.

بنابراین مانند آنچه در شکل ۶-۱۰ آمده، B گره ریشه بوده وBDD رویداد C با فرزندان چپ و راست B ، OR می‌شود.




**تصویر ٦-١٠ : اجرای تابع OR با استفاده از روش BDD (مرحله ۱)**

ابتدا فرزند چپ B (شاخه صفر) ، را در نظر بگیرید. براساس قوانین جبربولی (8b و 8d از ضمیمه الف، جدول الف -۱) داریم:

$$1+X = 1 \quad و \quad 0+X = X$$

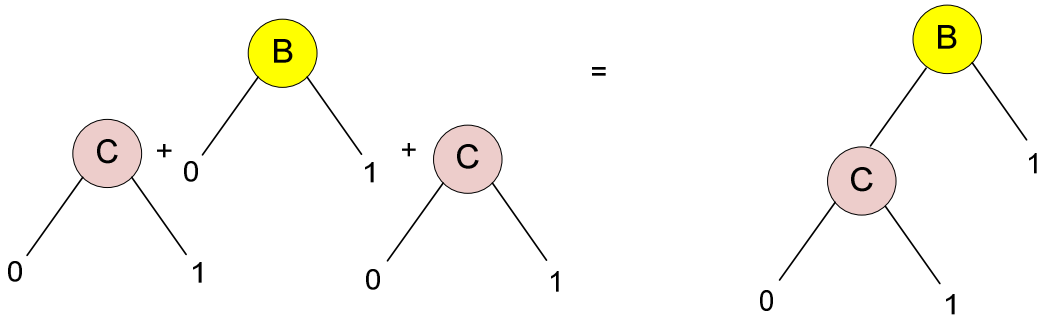
[1] Bottom

[2] اگر درخت خطا را درختی وارونه که تنه در بالا و شاخه‌ها و برگ‌ها در پایین باشند ، در نظر بگیریم، جایی که ریشه قرار دارد ، رویداد رأس و برگ‌ها رویدادهای پایه هستند و هر یک از شاخه‌ها از یک رویداد فرعی منشعب می‌شوند. با این توضیح، شروع از انتهای درخت به معنی شروع از رویدادهای پایه است. (مترجم)

[3] Root node

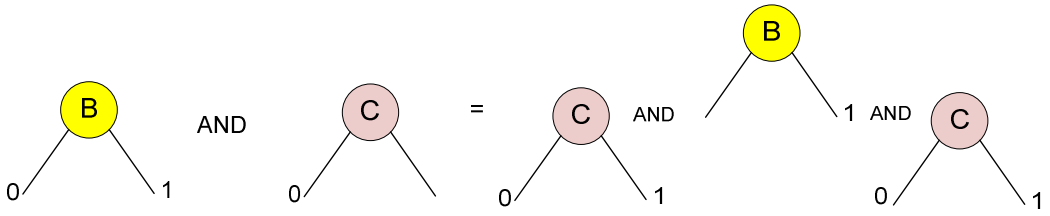
[4] Child node

بنابراین فرزند چپ (شاخه صفر رویداد B ) ، به C کاهش یافته و فرزند راست (شاخه یک رویداد B ) ، تولید 1 می‌کند (تصویر ۶-۱۱ را ببینید)



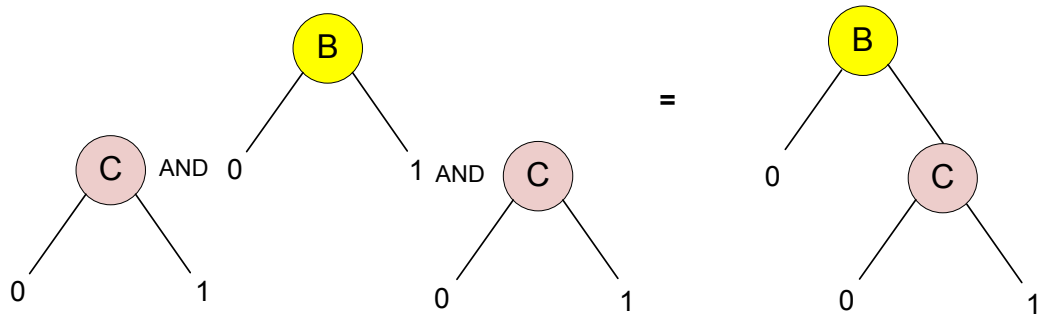

**تصویر ٦-١١ : اجرای تابع OR با استفاده از روش BDD (مرحله ۲)**

حال اعمال تابع AND را بر روی رویدادهای A و B در تصویر ۶-۱۲ ببینید. مجدداً با استفاده از قوانین جبر بولی داریم: $1.X = X$ و $0.X = 0$




**تصویر ٦-١٢ : اجرای تابع AND با استفاده از روش BDD (مرحله ۱)**

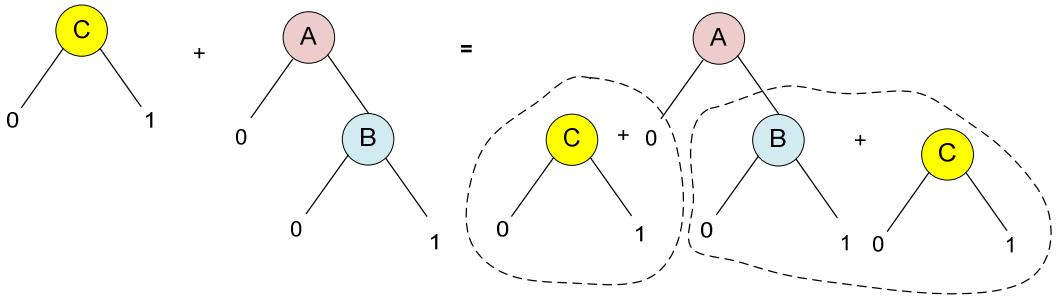
BDD کاهش یافته برای AND دو رویداد یعنی A.B در تصویر ۶-۱۳ دیده می‌شود.




**تصویر ٦-١٣ : اجرای تابع AND با استفاده از روش BDD (مرحله ٢)**

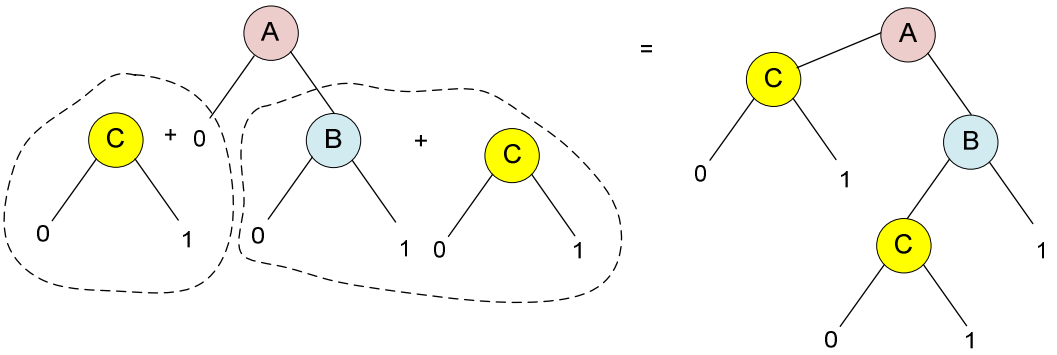
به عنوان یک مثال پیچیده تر ، رویداد C را در نظر بگیرید که با رویدادهای A و B ورودی به گیت AND ، OR می شود: (یعنی A•B+C )

چگونگی ساخت BDD این رابطه در تصویر ۶-۱۴ آمده است. چون A قبل از C و B مـی‌آیـد، گره ریشه محسوب شده وتابع OR بر روی فرزندان A ، اعمال می‌شود. فرزند چپ با اسـتفاده از جبر بولی کاهش می‌یابد و فرزند راست مانند تصویر ۶-۱۱ با تولید BDD شـبیه بـه تصـویر ۶-۱۵، ادامه می‌یابد.



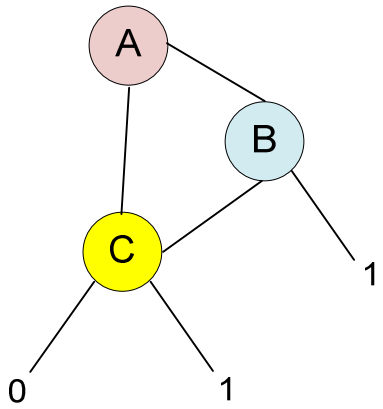

**تصویر ٦-١٤ : اجرای روش BDD برای تابع C+A.B ( مرحله ١)**

حتی می‌توان BDD سمت راست را ساده‌تر کرد (بیشتر کاهش داد)




تصویر ٦-١٥ : اجرای روش BDD برای تابع C+A.B ( مرحله ۲)

توجه کنید که گره C در دو بخش BDD تکرار شده است که یکی اضافی بوده و حذف می‌گردد وشما نتیجه کار را در تصویر ۶-۱۶ می بینید .




**تصویر ٦-١٦ : اجرای روش BDD برای تابع C+A.B ( مرحله۳)**

هر مسیری که از گره ریشه به گره پایانه 1 ختم می‌شود ، یک ترکیب گسسته از رویدادها بوده و باعث شکست سیستم می‌گردد. بنابراین، برای تصویر ۶-۱۶ ، که خلاصه شده رابطه A•B+C است ، مسیرهای شکست عبارت اند از : A'C+AB+AB'C

چون مسیرها، گسسته هستند، محاسبه احتمال شکست ساده است. این احتمال برابر با جمع احتمال مسیرها است. تبدیل درخت خطا به همین منوال ادامه می‌یابد تا تمامی گیت‌ها به BDD پیوند بخورند. و مسیرهای شکست منتهی به شاخه 1، با جمع مسیرهای شکست ، کمّی می‌شوند.

### ۳-۶ مقایسه روش BDD با روش مجموعه برش حداقل

روش BDD ، روش مکمل مجموعه برش حداقل( MCS ) می‌باشد. هر روش ویژگیها و مزایای مربوط به خود را دارد. در روش MCS ، مجموعه‌های حداقلی از رویدادهای پایه، باعث بروز رویداد رأس می‌شوند. بنابراین MCS ، ترکیبی از شکست‌های مهم را متمایز کرده و نشان می‌دهد که چگونه تغییرات در طراحی می‌تواند از تشکیل این ترکیب ناخواسته جلوگیری کند یا آثار آن را کاهش دهد. همچنین MCS برای بررسی صحت و اعتبار درخت خطا، سودمند می‌باشد چرا که با بازرسی مجموعه برش‌های حداقل خاصی می‌توان پی برد که مقدار احتمال به دست آمده برای رویداد رأس، به واقعیت نزدیک است یا خیر .در واقع MCS ها تقویت‌کننده اقدامات بازسازی هستند چرا که داشتن روشهای بازسازی مؤثر ، کاهش احتمال شکست مجموعه برشهای حداقل را بدنبال خواهد داشت . بنابراین MCS ها اطلاعات کیفی با ارزشی را به همراه اطلاعات کمی، یکجا در خود دارند.

روش BDD محاسبه دقیقی را از احتمال وقوع رویداد رأس، ارائه می‌دهد. این محاسبه دقیق مخصوصاً در زمانیکه رویدادهایی با احتمال بالا در درخت وجود دارند، مفید واقع می‌شود.

همچنین روش BDD ، روش بسیار کارآمدی برای محاسبات اعداد احتمال است. به علت آنکه مسیرهای حداقل تولید شده در این روش، گسسته هستند، محاسبات مربوط به اهمیت و حساسیت با راندمان خوبی انجام می‌گیرد. بنابراین روش BDD برای انجام محاسبات کمّی بسیار دقیق‌تر و کارآمدتر است .

در یک درخت خطا با تعداد بیشماری گیت OR و AND ، MCS های بسیاری تولید می‌شود و در روش MCS ، اغلب از مجموعه برش‌های حداقل با احتمال پایین، صرف نظر می‌شود تا محاسبه احتمال وقوع رویداد رأس در زمان کوتاه‌تری انجام پذیرد. در نرم افزارهای درخت خطای کنونی، الگوریتم‌هایی برای محدود کردن این حذف کردن‌ها، پیش بینی شده است که خطای ناشی از حذف و یا گرد کردن اعداد احتمال را کاهش می‌دهد. به هر حال استفاده از روش MCS، سالیان درازی به عنوان یک استاندارد، در محاسبات درخت خطا رواج داشته است و نرم‌افزارهای موجود از یکی و یا از هر دو این روش‌ها، بهره می‌برند.

**مراجع**

1. R. Sinnamon and J. Andreas, *Fault Tree Analysis and Binary Decision Diagrams*, Proceedings of the Reliability and Maintainability Symposium, January 1996, pp 215-222.
2. A. Rauzy, *New Algorithms for Fault Tree Analysis*, Reliability Engineering and System Safety, Vol. 40, 1993, pp 203-211.

# فصل ۷: ارزیابی کمّی درخت خطا

## ۷-۱) کمّی سازی درخت خطا و داده‌های مورد نیاز آن

برای محاسبه مقدار احتمال وقوع رویداد رأس در یک درخت خطا ، بایستی مقادیر احتمال رخداد هر یک از رویدادهای پایه را در دست داشته باشیم. سپس با جایگذاری این مقادیر در معادله بولی به دست آمده، که بر حسب مجموعه برشهای حداقل مرتب شده است ، می‌توان احتمال وقوع رویداد رأس را به دست آورد. همانطور که در فصل قبل شرح داده شد، یک روش ، استفاده از نمودار تصمیم دودوئی (BDD ) و معادلات آن است. البته بیشتر نرم‌افزارهای FT ، مجموعه برش های حداقل ( MCS ) را به دست می‌آورند که عمده مزیت آن، ارائه اطلاعات باارزش بیشتر نظیر شاخص اهمیت است.

با توجه به اینکه رویداد رأس، حاصلجمع برش های حداقل است، می‌توان احتمال آن را با جمع نمودن احتمال برش‌ها، تقریب زد. البته فرض این تقریب که به **تقریب رویداد نادر**[1] معروف است ، داشتن برش‌های حداقل با مقدار احتمال کمتر از 0.1 می‌باشد. واضح است که برقرار نبودن این شرط، مستلزم این است که احتمال اشتراک برش‌ها نیز محاسبه شود.

از طرفی یک مجموعه برش حداقل ، اشتراک رویدادهای پایه است و در جبر بولی بصورت حاصلضرب رویدادهای پایه (مثلاً A.C.D و یا خیلی ساده ACD ) نوشته می شود . بنابراین احتمال یک برش حداقل ، با ضرب احتمال BE[2] ها به دست می‌آید. بنابراین **احتمال رویداد رأس در واقع حاصل جمع حاصلضرب احتمال رویدادهای پایه منفرد است** که به تقریب جمع

[1] Rare event approximation
[2] Basic Event رویداد پایه

حاصل ضرب ها[1] معروف است. در صورتیکه اکثر اعداد احتمال رویدادهای پایه کمتر از ۰/۱ باشد ، این تقریب دقتی تا دو رقم اعشار دارد . برای بررسی میزان دقت این تقریب می توان از یک تقریب مرتبه دوم (که شامل محاسبه احتمال اشتراک هر جفت برش حداقل می‌شود) و مقایسه آن با نتیجه به دست آمده استفاده کرد.

معادل ریاضی گفته‌های بالا عبارت است از:

$$P(Top) = \Sigma\, P(M_i)$$

$$P(M_i) = P(BE_1)P(BE_2) \ldots P(BE_k)$$

که درآن عبارت $P(\ )$ ، احتمال رویدادی را نشان می‌دهد که در داخل پرانتز قرار دارد و منظور از Top ، رویداد رأس یا Top Event است . همچنین $M_i$ ، یک مجموعه برش حداقل خاص ، BE رویدادهای پایه $M_i$ ، K تعداد رویدادهای پایه و $\Sigma$ علامت جمع می باشد .

اگر FT کوچک و تعداد رویدادها کم باشد، به راحتی می‌توان تمامی برش‌های حداقل را نوشت. اما برای FT های بزرگ که تعداد رویدادهای آن مثلاً بیش از ۱۰۰عدد با تعداد زیادی گیت‌های AND و OR باشد، شمار برش های حداقل از یک میلیون بیشتر می‌شود و نیاز به استفاده از نرم‌افزار می‌باشد. اکثر نرم‌افزارهای FT ، تکنیک‌هایی را برای تخمین شمار کلی برش های حداقل براساس تعداد رویدادهای پایه، گیت‌ها و نوع آنها، دارند.

**انواع داده**

همانطور که در بخش قبل گفته شد ، کمّی کردن درخت خطا ، وقتی قابل انجام است که رویداد رأس بر حسب برش های حداقل ، نوشته شود . این برش ها خود شامل رویدادهای پایه

[1] Sum of products approximation

هستند که آنها نیز شکست قطعات عمده سیستم را در بر می گیرند . بنابراین ، کمّی کردن درخت خطا به این مسئله بر می گردد که آیا به اندازه کافی داده و اطلاعات در مورد نرخ شکست قطعات یا احتمال خرابی آنها داریم یا خیر . معمولاً داده های مربوط به رویدادهای پایه چهار نوع اصلی به شرح زیر دارند :

۱- **احتمال شکست قطعه**[۱] دریک بازهٔ زمانی

۲- **احتمال وقوع یک رویداد**[۲] در یک بازهٔ زمانی

۳- **دسترس ناپذیری قطعه**[۳]

۴- **احتمال صرف رویداد**[۴]

برای محاسبه احتمال شکست قطعه در یک بازهٔ زمانی خاص، نیاز به دانستن نرخ شکست قطعه[۵] ( بر حسب تعداد شکستها در وا حد زمان) و مدت زمان سپری شده مأموریت قطعه می‌باشد. این زمان، جمع کل زمان کاری و غیرکاری قطعه است.

در وضعیت عملیاتی یا کاری، قطعه در معرض تنش‌های حاصل از کارکرد خود ( انتقال یا تبدیل انرژی، سیگنال یا اطلاعات) است . در وضعیت غیرکاری، کارکرد قطعه متوقف شده (مثلاً پمپی که خاموش است) و قطعه تنها در معرض تنش‌های محیطی است که در آن قرار دارد. نرخ شکست اینگونه تعریف می‌شود:

$$\lambda = \lambda_O d + \lambda_N (1-d)$$

[1] Component failure probability
[2] Event occurrence probability
[3] Component unavailability
[4] Pure event probability
[5] Component failure rate

که در آن:

**d** = نسبت یا کسر دوره کاری (کل زمان کارکرد تقسیم بر کل زمان)

$\lambda_O$ = نرخ شکست قطعه در وضعیت کاری

$\lambda_N$ = سهم نرخ شکست قطعه در زمان توقف

در حالت استاندارد، نرخ شکست قطعه را ثابت فرض می کنند که براساس فرضیات دیگری نظیر عدم فرسودگی و راه اندازی موفقیت‌آمیز قطعه می باشد که از نظر آمار و احتمال، داشتن نرخ شکست کاملاً تصادفی است. البته بایستی سعی شود تا بهترین داده نرخ شکست قابل دسترس، استخراج شود. نکته قابل توجه این است که در هنگام استفاده و بکارگیری نرخ شکست، نباید شرایط محیطی که قطعه در آن قرار دارد را فراموش نمود .

**سلسله مراتب داده‌های نرخ شکست به ترتیب زیر است:**

۱) داده‌های واقعی مربوط به کارکرد قطعه

۲) داده‌های واقعی مربوط به طراحی‌هایی مشابه

۳) داده‌های آزمایش عمر یا شتاب قطعه

۴) داده‌های آزمایش عمر یا شتاب قطعه مشابه

۵) داده‌های آزمایش یا فیلد ارائه شده توسط تأمین کننده قطعه

۶) پایگاه داده خاص یا پایگاه های داده داخلی مربوط به قطعات مشابه

۷) کتابهای مرجع استاندارد مربوط به داده‌های قابلیت اطمینان[1]

[1] Reliability

احتمال شکست قطعه[1] که همچنین عدم قابلیت اطمینان[2] نامیده می‌شود توسط فرمول زیر تعیین می‌شود:

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

که در آن λ ، نرخ شکست قطعه و t بازه زمانی مورد نظر است . برای مقادیر کوچک λt ، ( یعنی $\lambda t < 0.1$ ) فرمول بالا به شکل زیر ساده می‌شود.

$$P \cong \lambda t$$

واحد λ ، احتمال شکست در واحد زمان (مثلاً در هر ساعت که قطعه درمعرض شرایط کاری و محیطی قرار دارد ) است. در بیشتر نرم‌افزارهای FT نرخ شکست و بازه زمانی به عنوان ورودی‌های مجزا، استفاده می‌شوند. جدول ۷-۱ ، یک نمونه داده‌های نرخ شکست را نشان می-دهد. نرخ شکست‌ها از داده‌های تاریخی و تجربی استخراج شده‌اند. در این جدول، همچنین اطلاعات عدم قطعیت[3] داده‌ها درسه ستون آخر آمده است.

[1] با علامت اختصاری P از اول کلمه Probability به معنای احتمال

[2] Unreliability
[3] Uncertainty

**جدول ۷-۱ : نمونه ای از داده های مربوط به نرخ شکست قطعات**

| NAME | DESC | EVENT LEVEL | PART NAME | PART NUMBER | SOURCE | RELATED CIL | LOCATE | SUBSYSTEM | NUMBER OF FAILURES | EXPOSURE | UNITS | RATE | DELTA T | PF MISSION | DIST | UNCERTAINTY PARM1 (MEDIAN) | PARM2 (EF) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 042BD0101 | APU 1 BURST DISK FAILS TO BURST | BE | BURST DISK - SEAL CAVITY DRAIN | 48-6806, ME251-0017-0001 | PEAPU1SCD | 04-2-BD01-01 | 1R/2 | 04-2 | 0 | 0 | X | 2.55E-05 | 1 | 0.0000255 | L | 6.58E-06 | 15 |
| 042BD0101 | APU 2 BURST DISK FAILS TO BURST | BE | BURST DISK - SEAL CAVITY DRAIN | 48-6806, ME251-0017-0001 | PEAPU2SCD | 04-2-BD01-01 | 1R/2 | 04-2 | 0 | 0 | X | 2.55E-05 | 1 | 0.0000255 | L | 6.58E-06 | 15 |
| 042BD0101 | APU 3 BURST DISK FAILS TO BURST | BE | BURST DISK - SEAL CAVITY DRAIN | 48-6806, ME251-0017-0001 | PEAPU3SCD | 04-2-BD01-01 | 1R/2 | 04-2 | 0 | 0 | X | 2.55E-05 | 1 | 0.0000255 | L | 6.58E-06 | 15 |
| 042BD0102 | APU 1 BURST DISK EXTERNAL LEAKAGE | BE | BURST DISK - SEAL CAVITY DRAIN | 48-6806, ME251-0017-0001 | PEAPU1FLK, PEAPU1SCD | 04-2-BD01-02 | 1/1 | 04-2 | 0 | 0 | H | 2.55E-05 | 217.5 | 0.0055463 | L | 6.58E-06 | 15 |
| 042BD0102 | APU 2 BURST DISK EXTERNAL LEAKAGE | BE | BURST DISK - SEAL CAVITY DRAIN | 48-6806, ME251-0017-0001 | PEAPU2FLK, PEAPU2SCD | 04-2-BD01-02 | 1/1 | 04-2 | 0 | 0 | H | 2.55E-05 | 217.5 | 0.0055463 | L | 6.58E-06 | 15 |
| 042BD0102 | APU 3 BURST DISK EXTERNAL LEAKAGE | BE | BURST DISK - SEAL CAVITY DRAIN | 48-6806, ME251-0017-0001 | PEAPU3FLK, PEAPU3SCD | 04-2-BD01-02 | 1/1 | 04-2 | 0 | 0 | H | 2.55E-05 | 217.5 | 0.0055463 | L | 6.58E-06 | 15 |
| 042BD0103 | APU 1 BURST DISK INTERNAL LEAKAGE OR PREMATURE RUPTURE | BE | BURST DISK - SEAL CAVITY DRAIN | 48-6806, ME251-0017-0001 | PEAPU1SCD | 04-2-BD01-03 | 1R/2 | 04-2 | 0 | 0 | H | 2.55E-05 | 217.5 | 0.0055463 | L | 6.58E-06 | 15 |
| 042BD0103 | APU 2 BURST DISK INTERNAL LEAKAGE OR PREMATURE RUPTURE | BE | BURST DISK - SEAL CAVITY DRAIN | 48-6806, ME251-0017-0001 | PEAPU2SCD | 04-2-BD01-03 | 1R/2 | 04-2 | 0 | 0 | H | 2.55E-05 | 217.5 | 0.0055463 | L | 6.58E-06 | 15 |

نوع دوم از داده های احتمال ، یعنی **احتمال وقوع رویداد** در یک بازهٔ زمانی ، شبیه بـه احتمـال شکست قطعه است و با این تفاوت که در این حالت بایستی **نرخ وقوع رویـداد**[1] در بـازه زمـانی مورد نظر ، تهیه شود. فرمول محاسبه‌ای این نوع احتمال نیز، مشابه بوده و تنها تفاوت در تعبیر $\lambda$ است. نرخ وقـوع رویـداد، در رویـدادهایی نظیـر آتـش سـوزی، از هـم گسـیختگی[2] و دیگـر رویدادهای آغازگر که اطلاعات مربوط به میزان وقوع آنها ( در سال یا در ساعت) موجود اسـت، کاربرد دارد.

[1] Event occurrence rate
[2] Rupture

نوع سوم داده احتمال، **دسترس ناپذیری قطعه**[1] است. این نوع داده برای قطعاتی که قابل تعمیر یا قابل تست هستند، تهیه می‌شود. همچنین رویدادهایی که مربوط به از سرویس خارج بودن قطعه در زمان فراخوانی آن است، نیاز به این نوع داده دارند. در مورد عدم دسترسی قطعه، نرخ شکست و مدت زمان تعمیر یا تست، تهیه می‌گردد. داده‌های خاص دیگر به نوع قطعه بستگی دارد. دو فرمول معمول درمورد عدم دسترسی قطعه ( q ) عبارتند از:

$q= \lambda_0\tau/ (1+\lambda_0\tau) \cong \lambda_0\tau$ برای حالت کار قطعه

$q = (1/2)\ \lambda sT/ (1+1/2\ \lambda sT) +1\text{-}e^{-\lambda 0\tau} \cong (1/2)\ \lambda sT + \lambda_0\tau$ برای حالت آماده باش قطعه

نمادهای بکار رفته در فرمول اول (حالت کار قطعه) ، عبارت اند از :

**λ0** نرخ شکست قطعه در حالت کار

**τ** زمان میانگین تعمیر قطعه

نمادهای بکار رفته در فرمول دوم (حالت آماده باش قطعه) ، عبارت اند از :

**λs** نرخ شکست قطعه در حالت آماده باش

**T** زمان تست یا بازرسی

**λ0** نرخ شکست قطعه در حالت کار

[1] منظور از دسترس ناپذیری قطعه ، عدم دسترسی به آن ، در زمانی است که فرآخوان می شود . به عنوان مثال پمپی که تنها در صورت افت فشار خط مورد استفاده قرار می گیرد ، ممکن است در شبانه روز فقط یکبار روشن شود . حال اگر در یک ماه (۳۰ بار فراخوانی) ، پمپ ۳ بار به دلیلی سرویس ندهد ، می گوییم نرخ عدم دسترسی به پمپ 0.1 است .(مترجم)

$\tau$ زمان کارکرد قطعه بعد از فراخوانی آن

مثالی از یک قطعه در حال آماده باش ، یک باتری است که در صورت از دست رفتن برق فراخوانی شود ویک نمونه از قطعه در حال کار، پمپی است که به طور دائم آب را در یک سیستم خنک کننده، به گردش در می‌آورد. دربیشتر نرم‌افزارهایFT ، پارامترهای بالا به عنوان ورودی تعریف شده‌اند.

چهارمین و آخرین نوع داده احتمال، **احتمال صرف رویداد** است که گاهی احتمال در هنگام تقاضا[1] یا کار نامیده می‌شود. این نوع احتمال، مستقیماً به عنوان ورودی تعریف شده و تجزیه نمی‌شود[2]. عموماً تنها ورودی است که در مورد یک رویداد، نیازی به ثبت نرخ شکست یا نرخ وقوع درواحد زمان ندارد. مثال‌هایی از این نوع داده ، خطاهای انسانی و رویدادهای محوری[3] ( که عموماً احتمالات شرطی هستند) می‌باشد. همچنین به عنوان مثال، احتمال شکست یک شیر اطمینان در زمان عمل کردن آن (یعنی وقتی فشار از حد مجاز بیشتر می‌شود) داده نوع چهارم است .

### ۷-۲) داده‌های مورد نیاز

همانطور که قبلاً گفته شد برای کمی سازی درخت خطا نیاز به داده‌های شکست رویدادهای پایه می‌باشد. بدین منظور پایگاه‌های داده براساس نوع رویدادهای پایه تقسیم بندی شده‌اند.

[1] Demand

[2] تفاوت این نوع داده با داده نوع اول این است که نیاز به دانستن توزیع نرخ شکست ندارد و عدد احتمال را می توان بطور مستقیم در محاسبات مربوط به برش ها و رویداد رأس ، بکار برد .(مترجم)

[3] یا Pivotal events به رویدادهایی گفته می شود که بعد از رویداد آغازین و قبل از رویداد پایانی ، قرار می گیرند . (مترجم)

داده‌های موجود در این پایگاه ها از فرمول های استاندارد احتمال وقابلیت اطمینان برای محاسبه احتمال رویدادها استفاده می‌کنند. انواع داده‌های اصلی مورد نیاز برای کمی سازی درخت خطا عبارت است از:

**الف) داده‌های نرخ شکست قطعات**

این داده‌ها برای محاسبه احتمال شکست و عدم دسترسی قطعه، مورد نیاز است. اگر از یک پایگاه داده نرخ شکست استفاده شود، حالت شکست قطعات نیز مشخص می‌گردد. البته اگر قطعه در شرایط محیطی خاصی قرار داشته باشد، بایستی در استخراج نرخ شکست از این نوع پایگاه ها، دقت کرده و اصلاحات لازم را انجام داد. مورد دیگر اینکه بایستی براساس وضعیت کاری یا آماده باش قطعه، نرخ شکست را تعیین کرد. نرخ شکست در حالت دوم مربوط به زمانی است که قطعه در حالت آماده باش قرار دارد و بایستی احتمال شکست آن را در صورت فراخوانی محاسبه نمود. نرخ شکست در حالت اول مربوط به زمانی است که قطعه با موفقیت فراخوانی شده و شروع به کار کرده است و می‌خواهیم احتمال خرابی قطعه را درهنگام کارکرد آن محاسبه کنیم. البته در این حالت بایستی بازه زمانی کار قطعه نیز مشخص گردد و درحالت آماده باش، مدت زمان متوسط خرابی قطعه قبل از اتمام تعمیرات ، به منظور محاسبه عدم دسترسی مورد نیاز است. نرخ‌های شکست گاهی به جای اینکه برحسب ساعت باشند براساس تقاضا آورده می‌شوند.

**ب) داده‌های مربوط به خطای انسانی**

داده‌های موجود در پایگاه‌های داده خطای انسانی براساس نرخ خطا در هنگام عمل است. کمی سازی یا بررسی قابلیت اطمینان خطای انسان، به غیراز تحلیل عوامل انسانی می‌باشد. تحلیل عوامل انسانی، جنبه‌های روانی عوامل تأثیرگذار بررفتار انسانی را بررسی می‌کند و کیفی است در صورتیکه تحلیل قابلیت اطمینان انسانی به کمی سازی و محاسبه احتمال انواع مختلف اعمال انسانی می‌پردازد و برای همین قابل استفاده در FTA است.

برای کمی کردن خطاهای انسانی در درخت خطا نیاز به یک پایگاه داده نرخ خطای انسانی می‌باشد و خطاهای انسانی ذکرشده در تحلیل درخت، بایستی با موارد موجود در این پایگاه داده، انطباق داده شود و در صورت عدم انطباق اغلب از تجربه کارشناسان برای تخمین نرخ خطای انسانی استفاده می‌گردد. اگر بخواهیم خیلی محافظه کارانه عمل کنیم ، می‌توانیم برای اینگونه خطاها، نرخ بالایی در نظر گرفته و با انجام آزمون حساسیت، حساسیت احتمال رویداد رأس به دست آمده را نسبت به این مقادیر تعیین کنیم. البته درهر حالت همواره یک عدم قطعیت در نرخ خطای انسانی وجود دارد که بایستی براساس تغییرات احتمالی در عملکرد انسان و شرایط موجود و همچنین خطای ناشی از تخمین‌های آماری، مدنظر قرار بگیرد.

**ج) داده‌های شکست‌های علت مشترک**

در صورتیکه شکستهای علت مشترک (CCF) در درخت خطا مدل شده باشد بایستی داده‌های مربوط به این نوع شکست‌ها تهیه شود. عموماً دراین حالت، احتمالات شرطی هستند و براساس

ضرایب بتا تعیین می‌شوند. البته مانند بخش قبل، به منظور تست حساسیت، بهتر است، مقادیر بزرگتری برای پارامترها در نظر گرفت و اگر رویداد رأس حساسیت زیادی نسبت به این مقادیر نشان داد، ارزیابی دقیقتری از آنها انجام دهیم.

**ه) داده‌های مربوط به پدیده‌های طبیعی**

این داده‌ها به عنوان رویداد آغازین و به عنوان رویداد پایه در درخت خطا مدل می شوند. رویدادهایی نظیرآتش‌سوزی، انفجار یا زلزله از این دسته‌اند و براساس تکرار یا تواتر آنها در واحد زمان یا در زمان مأموریت، آورده می‌شوند. اگر این تواترها کوچک باشند، اغلب جایگزین عدد احتمال رویداد می‌شوند (البته اگر بر حسب واحد زمان باشند و در بازهٔ زمانی مورد مطالعه ضرب شود). برای تواترهای خیلی بزرگ، رویداد رأس برحسب تواتر (تعداد مورد انتظار بروز رویداد رأس در بازه  زمانی داده شده) بیان می‌شود.

**۷-۳) احتمال رویداد رأس**

احتمال رویداد رأس براساس اعداد احتمال اختصاص داده شده به رویدادهای پایه محاسبه می-شود. نحوه محاسبه رویداد رأس در ضمیمه الف شرح داده شده است.

### ۷-۴) احتمال گیت

احتمال گیت که گاهی احتمال رویداد میانی نامیده می‌شود، احتمال رویدادهایی است که در پایین دست رویداد رأس قرار دارند. هر گیت مانند یک رویداد رأس مستقل برای رویدادهای پایین دست خود محسوب می‌شود و می‌توان معادلات جبر بولی را برای آنها نوشت. لازم به ذکر است محاسبه احتمال گیت‌ها، در هنگام رتبه بندی رویدادهای فرعی الزامی است.

### ۷-۵) سنجش اهمیت[1] در درخت خطا

یکی از مهمترین خروجی‌های تحلیل درخت خطا، اندازه‌گیری اهمیت نتایج حاصله است. البته میزان اهمیت رویدادها را می‌توان در تمامی سطوح درخت خطا و برای رویدادهای فرعی انجام داد تا سهم آنها در وقوع رویداد رأس مشخص شود و با توجه به نتایج آن، بتوان رویدادهای میانی (رویدادهای گیت) و حتی رویدادهای پایه را بر اساس اهمیتشان، الویت بندی کرد.

این سنجش‌ها، هم به صورت نسبی و هم مطلق محاسبه می‌شود آنچه اغلب به هنگام محاسبه این اهمیت‌ها نتیجه‌گیری و استنباط می‌شود این است که تنها تعداد اندکی از رویدادها، نقش برجسته‌تری در وقوع رویداد رأس دارند. در بسیاری موارد کمتر از ۲۰ درصد رویدادها در ۹۰ درصد وقوع رویداد رأس نقش دارند.

علاوه بر مشخص شدن میزان اهمیت رویدادها، از دیگر نتایج سودمند این اندازه‌گیری، روشن شدن وضعیت تخصیص منابع به منظور، تست، تعمیر و نگهداری[1]، بازرسی[2]، کنترل کیفیت[3] و

[1] Importance Measure

غیره می باشد . تا بدینوسیله، با بهینه سازی توزیع منابع، هزینه‌ها به حداقل برسد وسیستم به وضعیت بهتری سوق داده شود.

از طرفی اگر هزینه از قبل برای مثلاً بالا بردن سطح کیفی سیستم یا تعمیر و نگهداری اختصاص داده شده باشد، با تشکیل درخت خطا و تعیین میزان اهمیت رویدادها، می‌توان احتمال وقوع رویداد رأس را به حداقل رساند.

علاوه بر تخصیص منابع ، از سنجش اهمیت می‌توان برای تعیین زمان های تعمیر یا از سرویس خارج کردن قطعات، بهره برد. آنچه مسلم است قطعه‌ایی که سهم عمده‌ای در وقوع رویداد رأس دارد بایستی در زمان کمتری تعمیر شود یا از سرویس خارج گردد.

سنجش‌های اهمیتی که در تحلیل درخت خطا رایج است عبارتند از :

**الف) سنجش اهمیت Fussell-Vesely (F-V) Importance**

این سنجش، سهم رویدادها را در احتمال وقوع رویداد رأس مشخص می‌کند و به هر دوشکل نسبی و مطلق انجام می‌شود.

**ب) سنجش اهمیت Risk Reduction Worth (RRW)**

این سنجش میزان کاهش احتمال وقوع رویداد رأس در صورت اطمینان دادن از عدم وقوع یک رویداد مفروض، را مشخص می‌کند این سنجش نیز به هر دو شکل نسبی و مطلق انجام شده و

[1] maintenance
[2] inspection
[3] quality control

به سنجش RRW معروف است. روش انجام آن بدین صورت است که بایستی بـا صـفر نمـودن احتمال یک رویداد مفروض، احتمال وقوع رویداد رأس را مجدداً تعیین کرد.

**ج) سنجش اهمیت Risk Achievement Worth (RAW)**

این سنجش میزان افزایش احتمال وقوع رویداد رأس در صورت اطمینان از وقـوع یـک رویـداد مفروض را مشخص می‌کند. سنجشRAW ، مسیر فعالیت‌های پیشگیرانه[1] را برای اطمینـان از عدم وقوع یک شکست نشان می‌دهد چرا که شکست‌هایی با RAW بزرگ تأثیر منفی بیشتری بر روی سیستم داشته و بایستی از وقوع آنها پیشگیری شود. مجـدداً هـر دو سـنجش نسـبی و مطلق قابل انجام است و برای محاسبه آن بایستی احتمال وقوع رویداد رأس را مجدداً با فـرض یک بودن احتمال وقوع یک رویداد مفروض، محاسبه کرد.

**د) سنجش اهمیت Birnbaum (BM)**

این سنجش نرخ تغییر در احتمال وقوع رویداد رأس را براساس تغییر عدد احتمال یک رویـداد مفروض، تعیین می‌کند. سنجش BM ، همان **تحلیل حساسیت**[2] است و روش انجـام آن بـدین صورت است که برای یک رویداد داده شده، ابتدا مقدار احتمال یک درنظر گرفته شده و سپس احتمال وقوع رویداد رأس مشخص می‌شود و بعد مقدار احتمال رویـداد مزبـور ، بـا عـدد صـفر

[1] prevention activities
[2] Sensitivity analysis

جایگزین شده، مجدداً احتمال وقوع رویداد رأس محاسبه می‌گردد و دو مقدار فوق از هـم کـم می‌شوند. ارتباط BM با دو روش قبل عبارت است از:

$$\mathbf{BM = RAW + RRW}$$

**مراجع**

1. W. Vesely et al., *Measures of Risk Importance and their Applications,* NUREG/CR-3385, U.S. Nuclear Regulatory Commission, 1983.
2. T. Bedford and R. Cooke, Probabilistic Risk Analysis: Foundations and Methods, Cambridge University Press, 2001.

# فصل ۸ : کاربرد تحلیل درخت خطا

در این فصل به ذکر مثالی عملی در مورد کاربرد درخت خطا در شناسایی نقاط ضعف سیستم، می‌پردازیم و بعد از معرفی سیستم تحت مطالعه و تعیین رویداد رأس، درخت خطا را براساس قواعد مطرح شده در فصل چهارم رسم می‌کنیم. سپس با بکارگیری جبر بولی به محاسبات مجموعه برشهای حداقل و نوشتن احتمال رویداد رأس بر حسب احتمال این برشها می‌پردازیم. در ادامه با کمی سازی تحلیل خود، نتایجی را ارائه می‌دهیم که حتی توسط خبره ترین کارشناسان سیستم، قابل پیش بینی نیست.

## ۸-۱) مطالعه موردی[1]: مخزن ذخیره تحت فشار

تصویر ۸-۱ ، مخزن ذخیره تحت فشاری را نشان می‌دهد که شامل مخزن، سیستم کنترل فشار، ورودی سیال، بخش موتور و پمپ وشیر خروجی می‌باشد.

وظیفه سیستم کنترل، تنظیم کارکرد پمپ است، این پمپ، سیال* را از ورودی به طرف مخزن می‌فرستد. با ورود سیال، مخزن فشار می‌گیرد فرض کنید زمان لازم برای رسیدن به فشار مجاز سیال ، ۶۰ ثانیه باشد. کنتاکتهای[2] سوئیچ فشار[3] در زمان خالی بودن مخزن، بسته است. وقتی

[1] Case Study

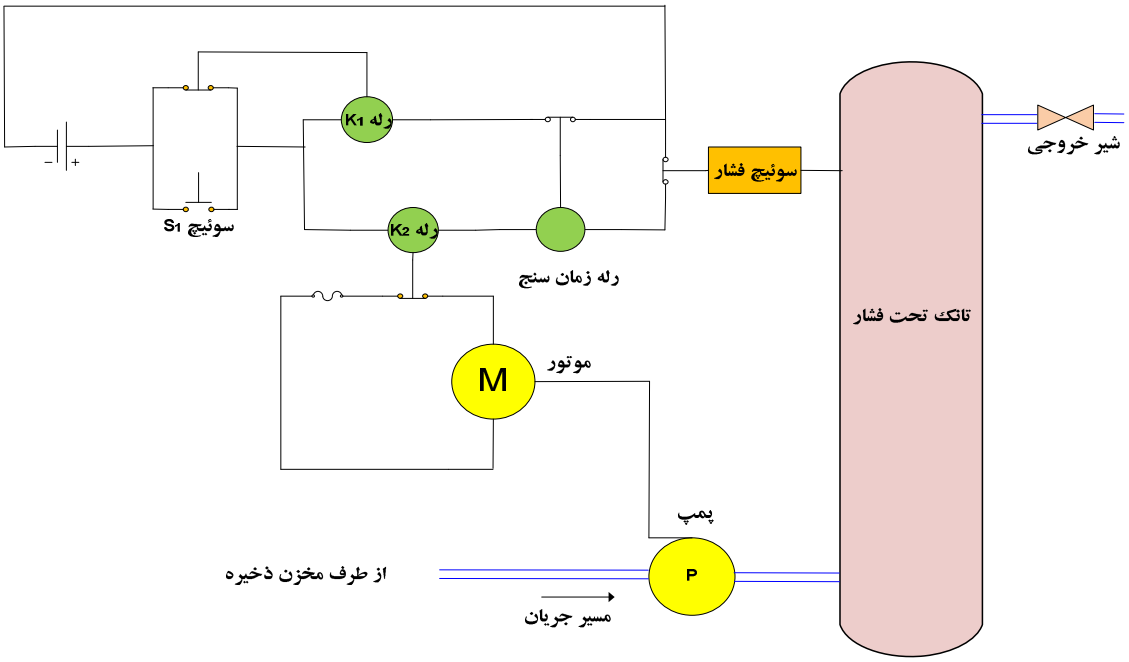
* در این مطالعه نوع سیال را مشخص نکرده ایم ، چرا که هدف ما بیشتر تشریح یک مثال کاربردی در صنایع ، در رابطه با انجام تحلیل درخت خطا می باشد . این سیال به عنوان مثال می تواند نفت و گاز ورودی به مخزن production یک کارخانه بهره برداری در صنایع نفت ، یک مخزن ذخیره آمونیاک در صنایع پتروشیمی یا هر مخزن ذخیره تحت فشار دیگری باشد . (مترجم)

[2] Contacts

[3] Pressure Switch

منظور از سوئیچ فشار در اصطلاح ابزاردقیق ، کلیدی است که با افزایش یا کاهش فشار از یک مقدار از پیش تعیین شده ، با توجه به حالت پیش فرض آن ، باز یا بسته می شود . (مترجم)

فشار مخزن به آستانه مجاز خود می‌رسد، کنتاکتهای سوئیچ باز مـی‌شـود و باعـث بـدون بـرق شدن[1] سیم‌پیچ رله K2 می‌گردد. در نتیجه کنتاکتهای رله K2 باز شده وبرق ورودی به پمپ را قطع می‌کند و پمپ از کار می‌افتد . ایـن مخـزن مجهـز بـه یـک شـیر خروجـی اسـت کـه در

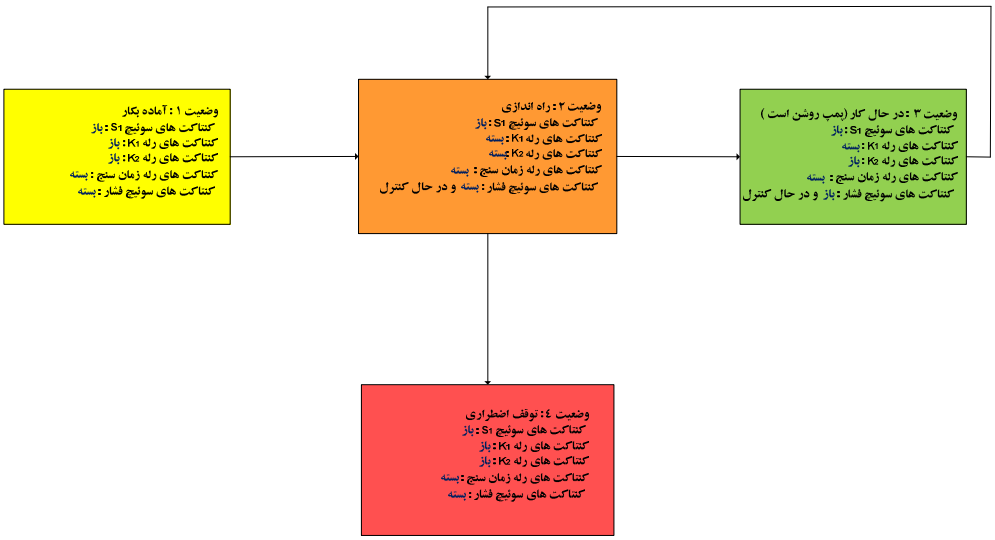



**تصویر ۸-۱ : مخزن ذخیره تحت فشار**

مدت زمان کوتاهی محتویات مخزن را تخلیه می‌کند. البته لازم به ذکر است که این شـیر، بـه غیراز شیر اطمینان[2] می‌باشد. با تخلیه کامل سیال ، کنتاکتهـای سـوئیچ فشـار، بسـته شـده و مجدداً مخزن توسط پمپ پر می‌شود. تصویر ۸-۲ حالتهای متفاوت کارکرد این سیستم را نشان می‌دهد. در آغاز فرض براین است که سیستم درحالت ساکن قرار دارد یعنی کنتاکتهای سوئیچ S1 و کنتاکتهای رله‌های K1 و K2 باز است و سیستم کنترل کاملاً بدون برق و انرژی است. در

[1] De-energized
[2] Relief Valve

این وضعیت ، کنتاکتهای رله زمان سنج[1] نیـز بسـته اسـت و مخـزن خـالی اسـت و در نتیجـه کنتاکتهای سوئیچ فشار در حالت عادی خود بوده و بسته می‌باشد.




تصویر ۸-۲: چرخه کاری مخزن ذخیره

با فشار دادن سوئیچ S1 برای شروع کار، رله K1 برقرار وکنتاکتهای آن بسته می‌شود و رله به علت داشتن مدار خود نگهدار حتی بعد از باز شدن سوئیچ S1 ، بسته می‌ماند و برق را همزمان به سیم‌پیچ‌های رله K2 و رله زمان سنج می‌رساند. کنتاکتهای رله K2 بسته شده و تغذیه بـرق به پمپ وصل می‌شود و تغذیه مخزن با سیال شروع می‌شود.

از طرف دیگر زمان سنج به کارمی‌افتد. پیش‌بینی رله زمـان سـنج درمـدار، تنهـا بـرای مواقـع اضطراری است که ممکن است سوئیچ فشار عمل نکرده و باعث توقف سیستم نشود.

[1] Timer relay

همانطور که در بالا گفته شد رله K1 ، بطور همزمان رله K2 و زمان سنج را به کار می‌اندازد، تنظیم زمان‌سنج برروی ۶۰ ثانیه است و بعد از گذشت این زمان، کنتاکتهای آن باز شده و به دلیل داشتن مدار خود نگهدار، باز می‌ماند. در نتیجه برق از روی K1 و بعد K2 و در نهایت پمپ برداشته می‌شود و پمپ از کار می‌افتد. در وضعیت عادی، وقتی کنتاکتهای سوئیچ فشار باز است ( و درنتیجه کنتاکتهای رلهK2 نیز باز می‌باشد) ، زمان سنج روی صفر ثانیه ری‌ست[1] می‌شود.

رویداد نامطلوب برای این مثال (رویداد رأس درخت خطا) عبارت است از:

**از هم گسیختگی مخزن**
**بعد از شروع پمپاژ**

فرض بر این است که خرابی سیم کشی و لوله‌های انتقال سیال و تمامی شکستهای ثانویه از احتمال ناچیزی برخودار است. ممکن است خواننده اظهارنماید که سیستمی با این فرضیات (شیر خروجی که در کوتاهترین زمان محتویات مخزن را تخلیه کند و داشتن دسترسی تمام وقت به سیال) واقعی نیست و علاوه براین فرض ناچیز شمردن احتمال خرابی سیم‌کشی ولوله-های انتقال، ممکن است صحیح نباشد. اما هدف از آوردن این مثال و ساده سازی آن با فرضیات ارائه شده، تنها نشان دادن مراحل انجام تحلیل درخت خطا به صورت قدم به قدم به خواننده و تمرین مفاهیم مطرح شده در کتاب است. مسلماً با درک و تجزیه و تحلیل یک مثال

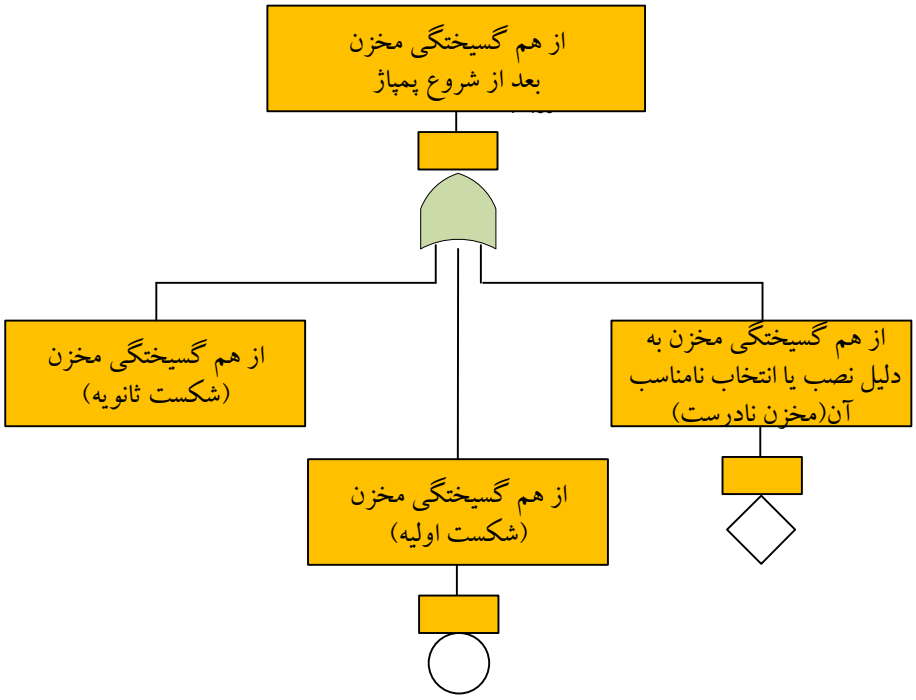
[1] Reset
به حالت اولیه برگرداندن یک دستگاه دیجیتال می باشد . منظور از ری ست شدن زمان سنج در این مثال ، صفر شدن دوباره زمان آن است .

کاربردی ساده، مسیر برای تحلیل سیستم‌های پیچیده‌تر و دارای جزئیات بیشتر، هموار می‌گردد. ابتدا مطمئن شوید که رویداد رأس به شکل عبارت خطا نوشته شده و چگونگی و زمان وقوع رویداد را در خود دارد. سپس این سؤال را مطرح کنید:

**آیا این خطا بیان کننده شکست یک قطعه است؟**

چون پاسخ مثبت است بلافاصله یک گیت OR در پایین رویداد رأس قرار دهید و به حالت‌های اولیه، ثانویه و فرمان[1] این شکست بپردازید (برای یادآوری به بخش ۴-۲ فصل دوم مراجعه کنید) . رسم درخت تا بدین مرحله، در تصویر ۸-۳ آمده است. در این مثال، پرداختن به جزئیات تا سطح شکست قطعات تعیین شده است. منظور از قطعه، مواردی است که در تصویر ۸-۱ (نقشه کلی سیستم)، نامگذاری شده‌اند. بنابراین شکست اولیه مخزن ( مثلاً فرسودگی دیوارهٔ مخزن) درمرز تحلیل قرار گرفته و بایک دایره در زیر جعبه رویداد آن ، متمایز می‌شود. البته فرض براین است که مخزن در شرایط طراحی خوبی قراردارد، در غیر این صورت بایستی به جای دایره از لوزی استفاده می‌شد که نشان‌دهنده رویدادهای بسط نیافته است. به هر حال و درهر صورت قرار نیست این رویداد بیش از این دنبال شود و به همین وضعیت باقی می‌ماند.

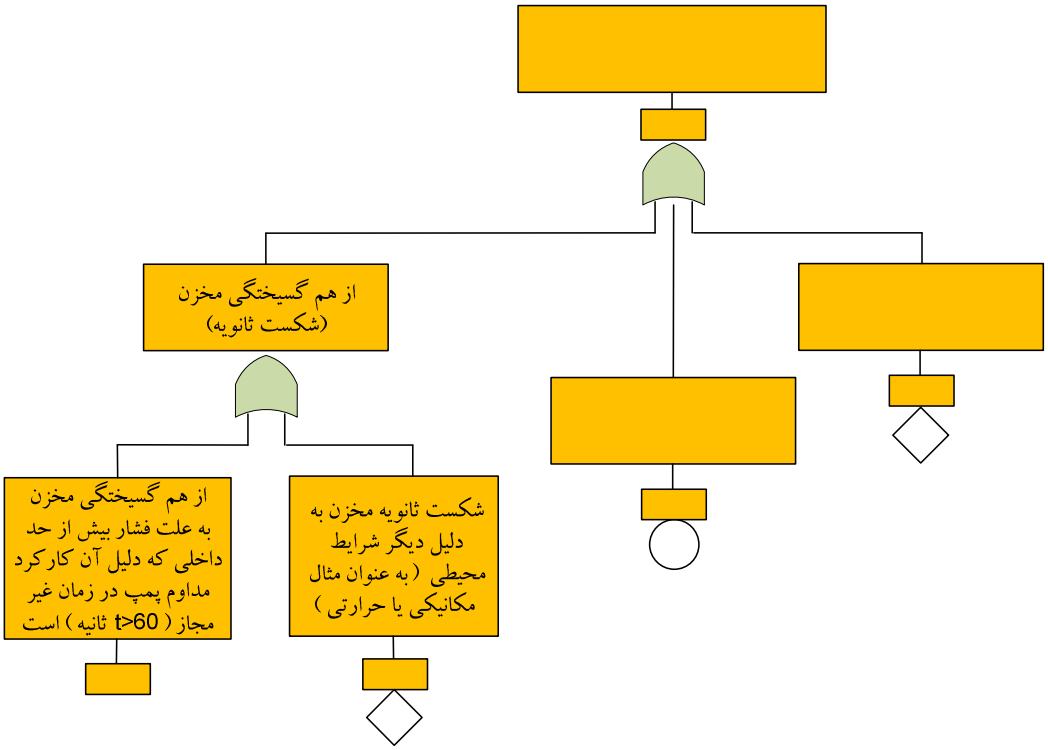
[1] در این موردخاص، حالت فرمان نداریم.




**تصویر ۸-۳ : رسم درخت خطا – گام اول**

حالا توجه خود را به شکست ثانویه مخزن، معطوف می‌کنیم. از فصل دوم به خاطر بیاورید که این نوع شکست نقطه مقابل شکستهای اولیه است که در محدوده طراحی قطعه اتفاق می‌افتد. چون این شکست ثانویه درردیف شکست قطعه قرار می‌گیرد، گیت OR دیگری را در این قسمت به درخت اضافه می‌کنیم که در تصویر ۸-۴ مشخص شده است.

ممکن است این تصویر دور از واقعیت به ذهن برسد که حتی بعد از گذشت زمان ۶۰ ثانیه، پمپاژ ادامه داشته و مخزن به طور معجزه آسایی، سالم باقی بماند. اما با یادآوری اولین قاعده رسم درخت خطا ( به فصل ۵ مراجعه کنید) قرار نیست هیچ اتفاقی معجزه آسایی در تحلیل ما بیفتد وفرض ما براین است که در صورت وقوع چنین اتفاقی، مخزن کاملاً از هم گسیخته و می ترکد.

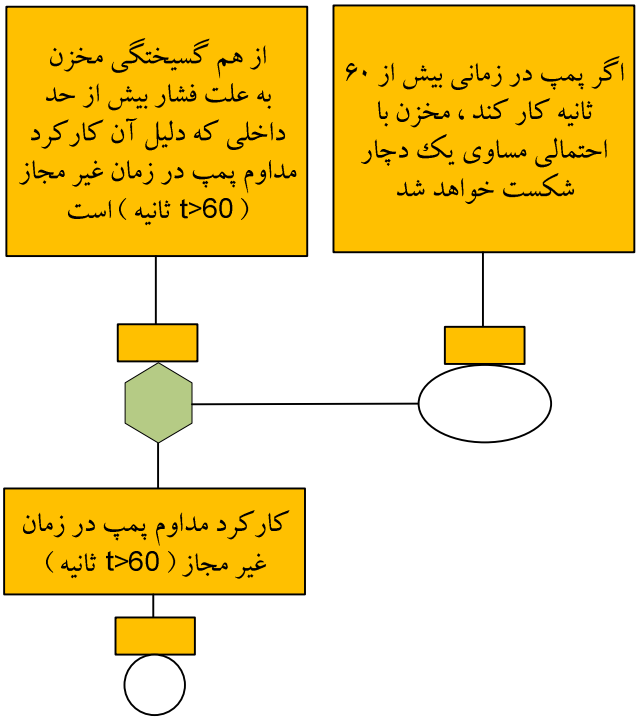



**تصویر۸-٤ : رسم درخت خطا – گام دوم**

این مسئله را می‌توان در درخت خطای رسم شده، با بهره‌گیری از یک گیت بازدارنده که ورودی آن «عدم توقف پمپ در زمان بیش از ۶۰ ثانیه» است، نمایش داد (تصویر ۸-۵)

آیا رویداد ورودی به یک گیت بازدارنده می‌تواند شامل یک شکست قطعه باشد؟ پاسخ منفی است. کارکرد پمپ درهر بازهٔ زمانی نمی‌تواند در برگیرنده یک شکست قطعه باشد. پس این رویداد خطا را بایستی مربوط به وضعیت سیستم دانست. حالا با توجه به قوانین مطرح شده درفصل ...، می توان در زیر این رویداد ، گیت OR یا AND قرارداد. علاوه بر این، بایستی دلیل

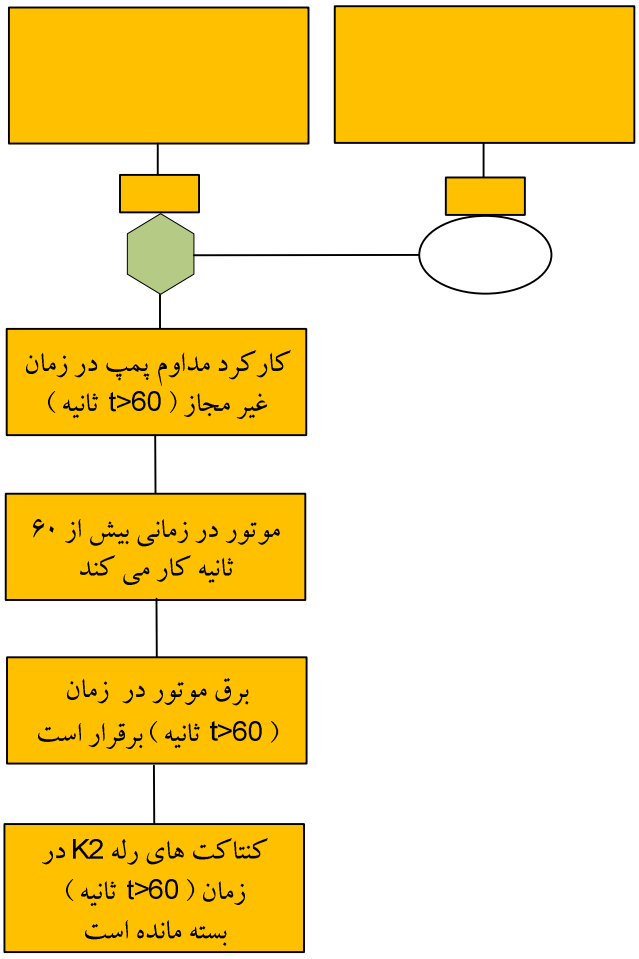
یا دلایل لازم، کافی و بلافصل وقوع این رویداد را شناسایی کرد . در این مورد، دلیـل بلافصـل، روشن بودن موتور در زمان $t > 60$ ثانیه است که یک خطای سیستمی است .




**تصویر ۸ -۵ : رسم درخت خطا – گام سوم**

و دلیل بلافصل این خطا نیز برقرار بودن تغذیه برق در زمان $t > 60$ اسـت کـه ایـن خطـا هـم مربوط به وضعیت سیستم است و دلیل فوری آن بسته باقی ماندن کنتاکتهای رله $K_2$ در زمان $t > 60$ می‌باشد. و بدین ترتیب رشته رویدادهای زیر به مدل درخت خطا اضافه می شود تا این اطلاعات اضافی را منعکس کند ( تصویر ۶-۸)

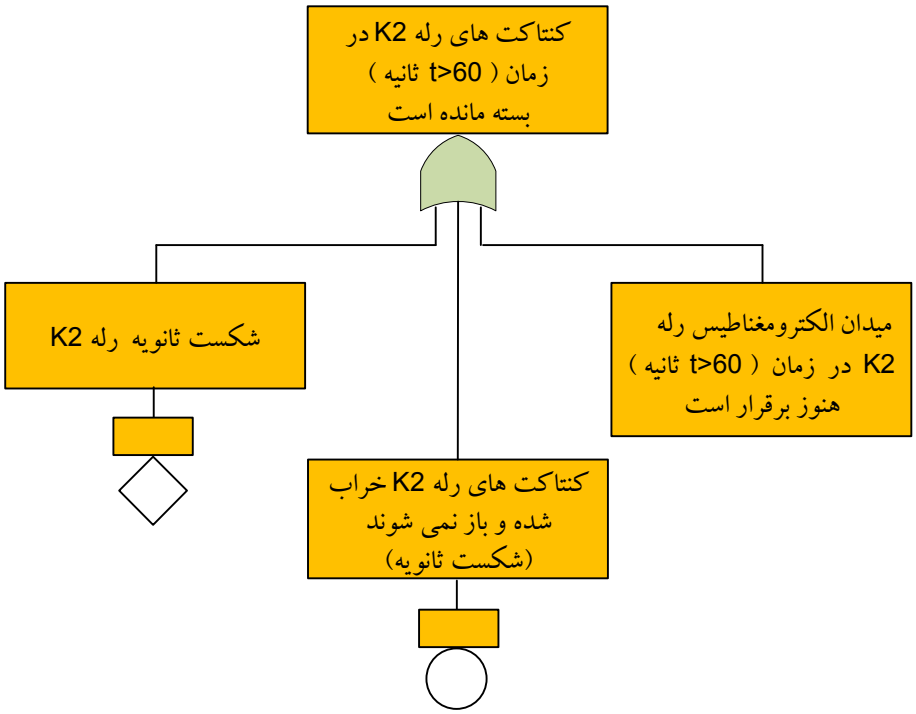
همانطور که ملاحظه می‌کنید در پیاده‌سازی مفهوم دلیل بلافصل، هیچ رویداد خطـایی حـذف نمی‌شود و تمامی دلایل بدون پرش و به طور منطقی آورده می‌شوند.



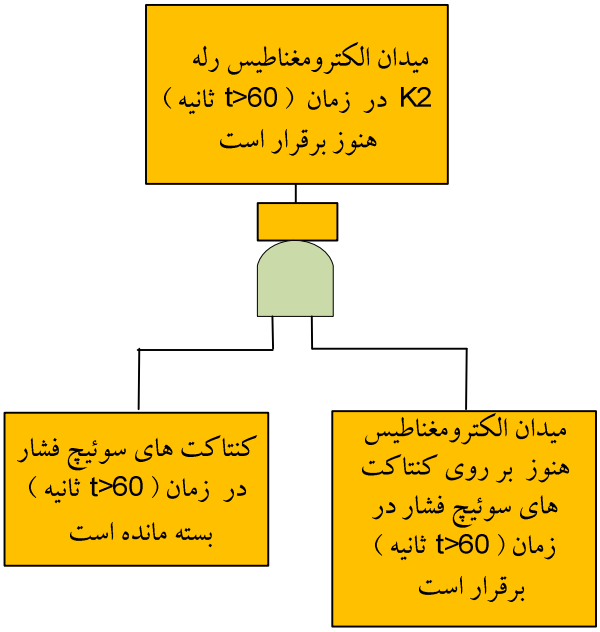

**تصویر۸-٦ : رسم درخت خطا – گام چهارم**

اینک، رویداد خطای «بسته باقی ماندن کنتاکتهای رله $K_2$ در زمان $t > 60$ » را در نظر بگیرید. با توجه به اینکه دلایل مختلفی از قبیل گیر کردن یا خرابی کنتاکت ها می تواند باعث وقوع این رویداد شوند ، بنابراین خطای آن از نوع قطعه است که در تصویر ۸-۷ با قرار دادن یک گیت OR ، نوع خطا را نمایش داده ایم . در مورد رویداد برقرار بودن میدان الکترومغناطیس در

زمان $t > 60$ بر روی رله $K_2$ ، بیاد بیاورید که خطای فرمان وقتی اتفاق می‌افتد کـه قطعـه بـه علت فرمان یا سیگنال خطایی که از جای دیگر دریافت می‌کند، کارکرد صحیح اما در زمان یـا مکان اشتباه دارد. در این مورد خاص، سیگنال خطا، برقرار بودن جریان برق در سیم‌پـیچ‌هـای رله در زمان $t > 60$ می باشد. این خطای فرمان را در تصویر ۸-۸ مورد تحلیل قرارداده‌ایم.




**تصویر۸-۷ : رسم درخت خطا – گام پنجم**

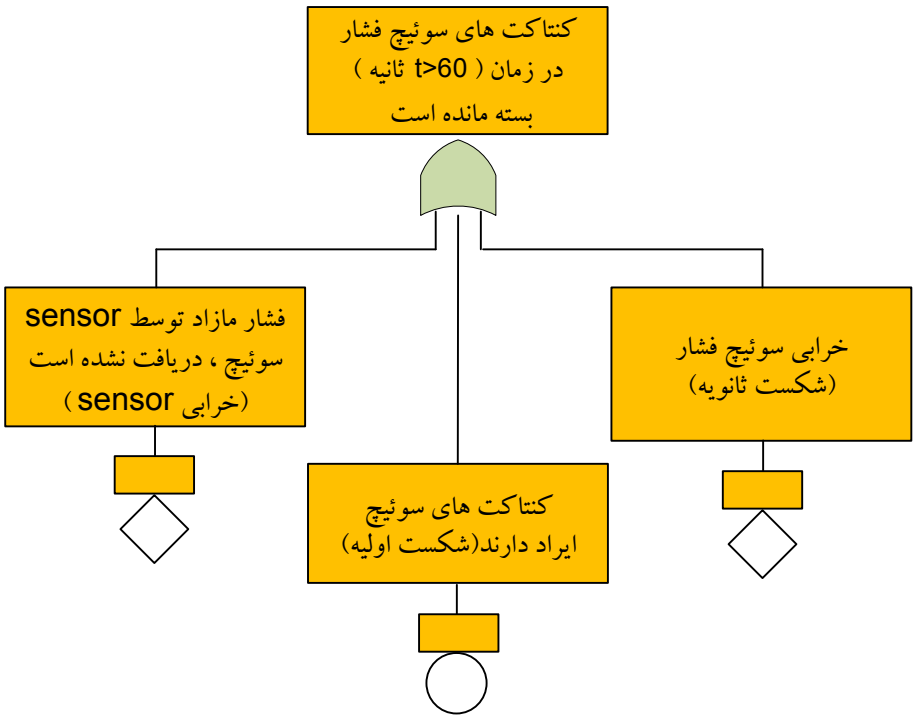



**تصویر۸-۸ : رسم درخت خطا – گام ششم**

توجه کنید که هردو رویداد ورودی به گیت AND در تصویر ۸-۸، تحت عنوان خطا آورده شده‌اند. درواقع همانطور که بحث شد تمامی عبارتهایی که در داخل جعبه‌ها نوشته می‌شود بایستی بیانگر یک خطا باشند مگر آنکه به عنوان توضیح آورده شوند ( که در این صورت این عبارات بایستی در یک کادر بیضی شکل قرار داده شوند) .

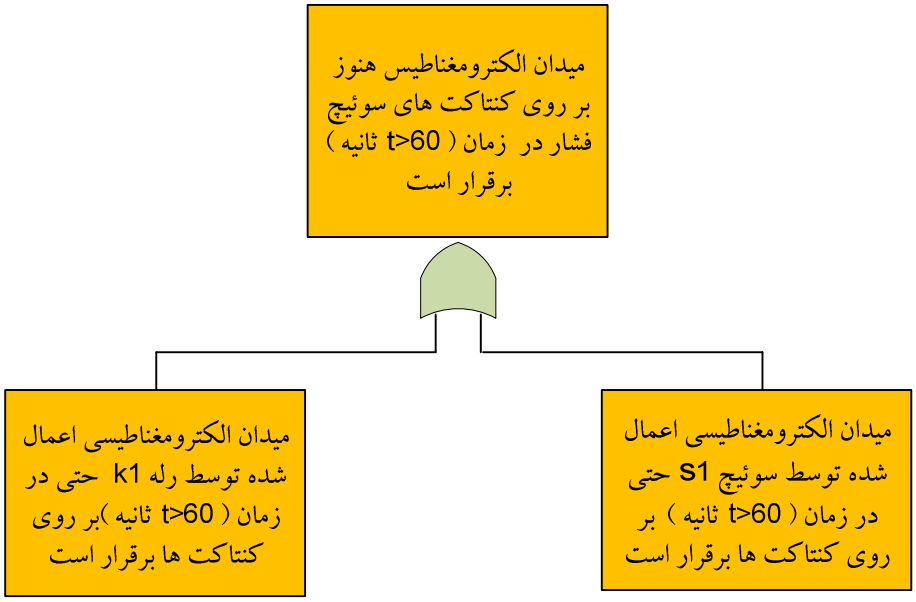
بسته باقی ماندن کنتاکتهای سوئیچ به خودی خودی خطا نیست، اما اگر این کنتاکت‌ها بیش از ۶۰ ثانیه بسته بماند، این خطا است. با همین تعبیر برقرار بودن جریان برق در سوئیچ فشار خطا نیست به شرط اینکه در زمان اشتباه نباشد. رویداد خطای بسته باقی ماندن کنتاکتهای سوئیچ در زمان $t > 60$ دربردارنده یک شکست قطعه است برای همین رویدادهای ورودی به

آن بایستی از یک گیت OR عبور کنند . این رویدادها به طور مجزا مـورد بحـث قـرار خواهنـد گرفت. ابتدا به رویداد سمت چپ تصویر ۸-۸ می پردازیم :



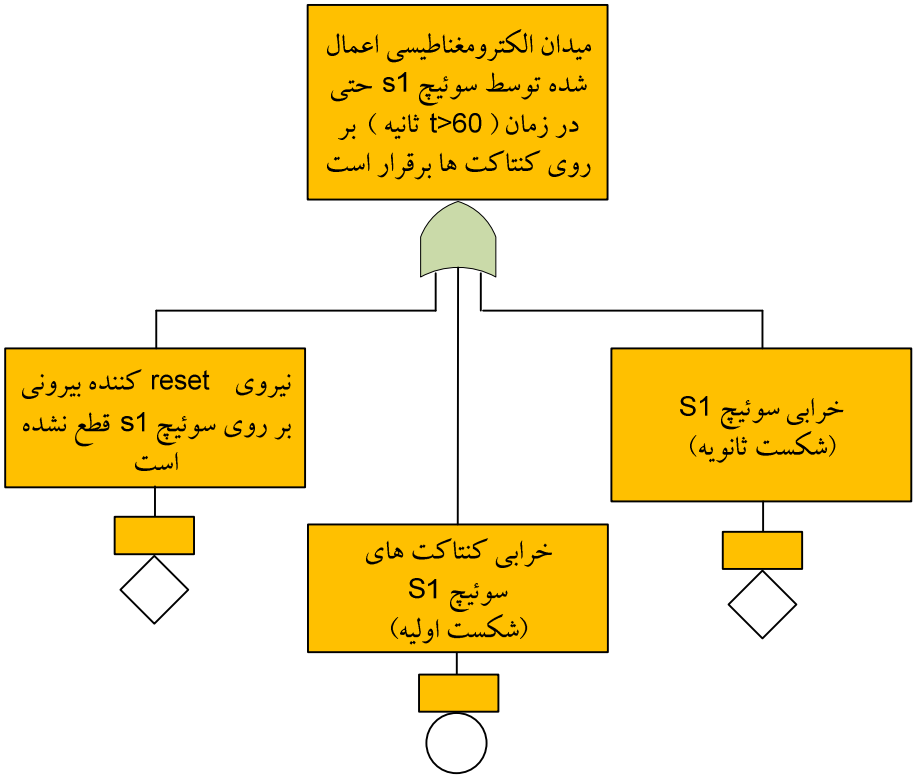

**تصویر ۸-۹ : رسم درخت خطا – گام هفتم**

بسط شاخه چپ درخت را در تصویر ۸-۹ آورده شده است .این شاخه از درخت به انتهای خـود رسیده است (تمامی رویدادهای ورودی به آن به دایـره یـا لـوزی خـتم شـده انـد) مگـر آنکـه بخواهیم، رویداد بسط نیافته (دارای شکل لوزی) سمت چپ را به دلایلـی، بـاز کنـیم و دلایـل وقوع آن را بیشتر دنبال کنیم. ( به عنوان مثال یکـی از دلایـل آن مـی‌توانـد پـارگی دیـافراگم باشد.)



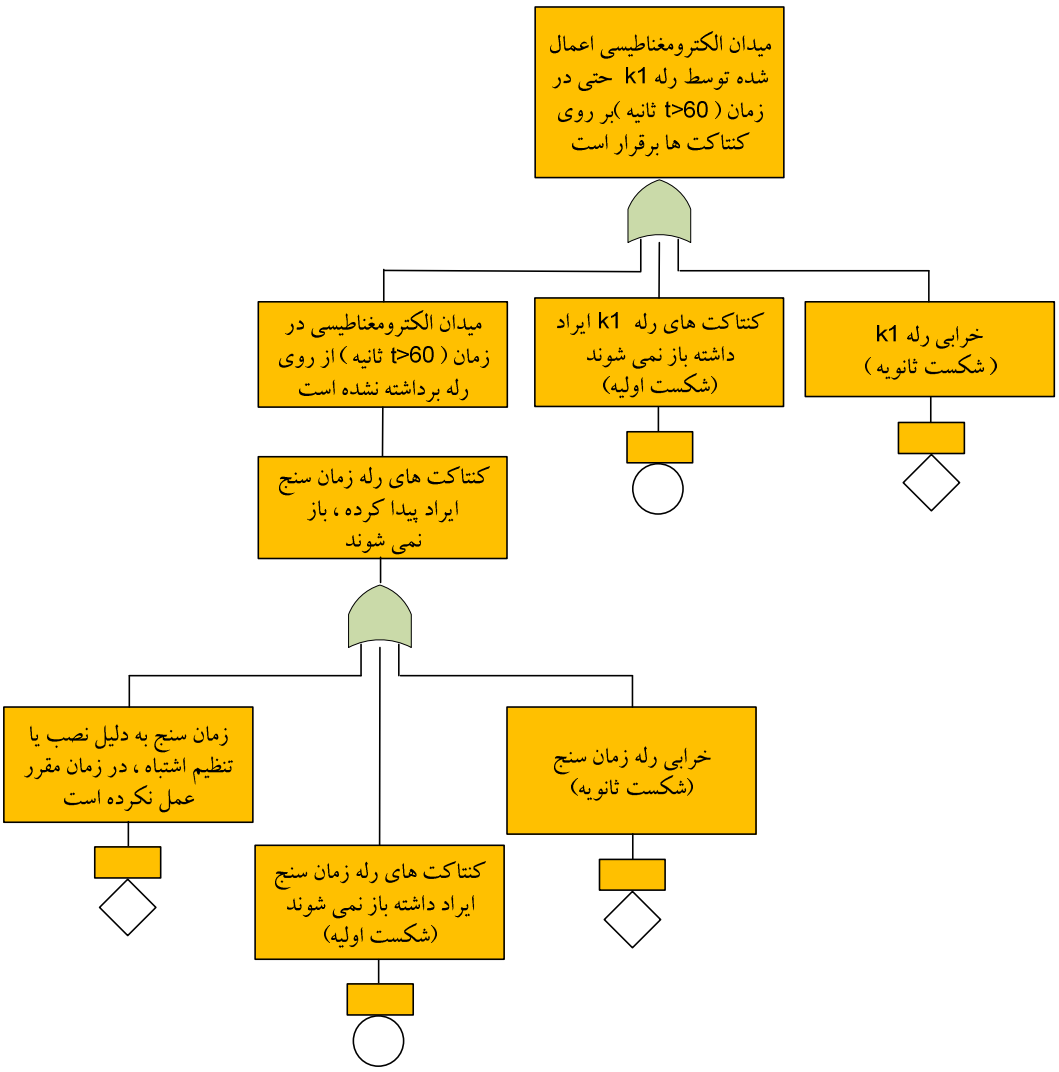

**تصویر۸-۱۰ : رسم درخت خطا – گام هشتم**

حال به سراغ رویداد شاخه راست تصویر ۸-۸ می رویم . بسط این شاخه از درخت در تصویر ۸-۱۰ مورد تحلیل قرار گرفته است هردو ورودی‌ها در این تصویر خطای قطعه بوده و تحلیل بیشتر آنها در تصویر ۸-۱۱ آمده است. همانطور که ملاحظه می‌کنید به انتهای شاخه دیگری از درخت رسیده‌ایم. تحلیل رویداد باقیمانده تصویر ۸-۱۰ در تصویر ۸-۱۲ نشان داده شده است. خواننده، متوجه این مطلب شده است که بسط درخت خطا به همین منوال، قدم به قدم ادامه می‌یابد تا به خطاهای رله زمان سنج برسیم. درخت خطای تکمیل شده مثال مخزن ذخیره تحت فشار در تصویر ۸-۱۳ نمایش داده شده است.

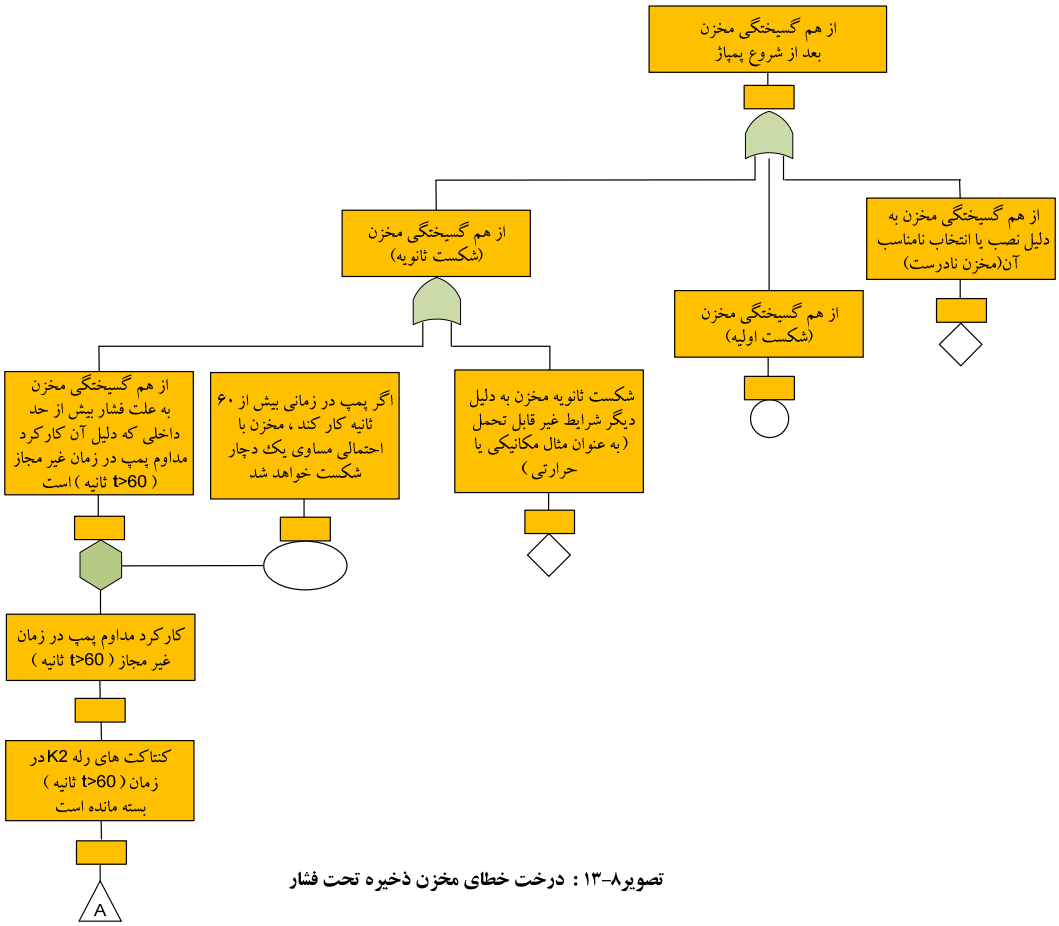



**تصویر۸-۱۱ : رسم درخت خطا – گام نهم**

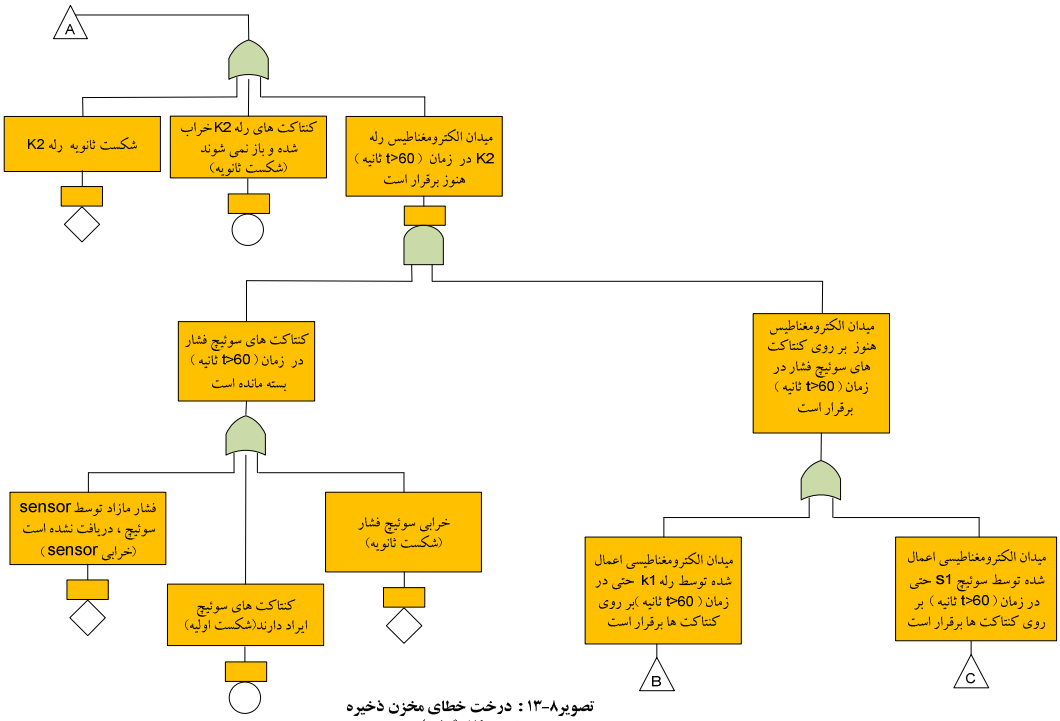
با ساده سازی بیشتر ، درخت خطای اصلی در تصویر ۸-۱۴ رسم شده است که در آن خطاهای اولیه با علائم اختصاری $E_1$ ، $E_2$ و ... نشان داده شده و در بخش ۸-۲ تعریف شده‌اند .



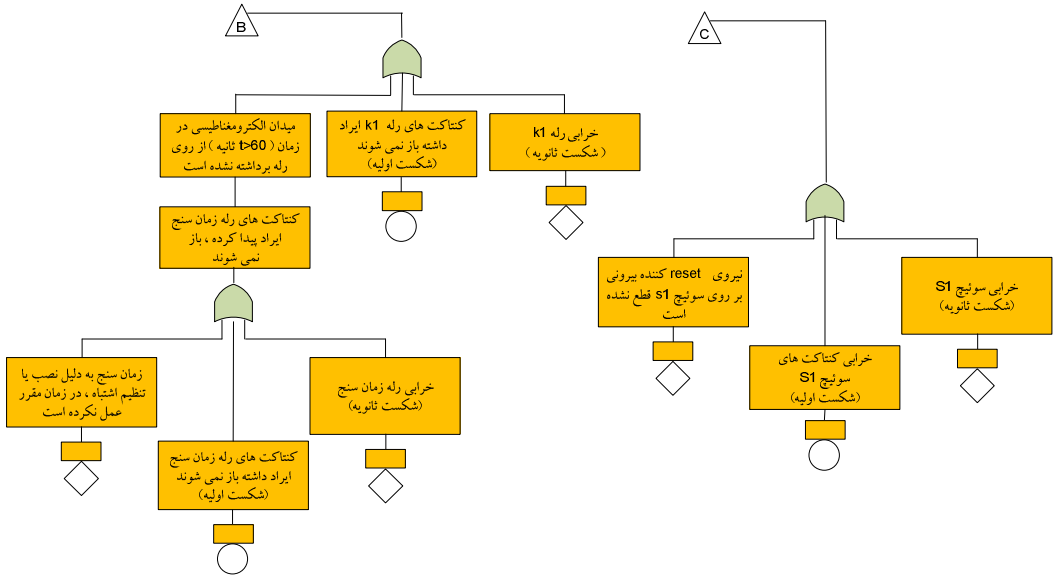

**تصویر۸-۱۲ : رسم درخت خطا – گام آخر**




**تصویر۸-۱۳ : درخت خطای مخزن ذخیره تحت فشار**




**تصویر۸-۱۳ : درخت خطای مخزن ذخیره تحت فشار(ادامه)**




**تصویر۸-۱۳ : درخت خطای مخزن ذخیره تحت فشار(ادامه)**

### ۸-۲) ارزیابی کمّی درخت خطای مربوط به مخزن ذخیره

رویداد رأس درخت خطای نشان داده شده در تصویر ۸-۱۴ را می‌توان با استفاده از جبر بـولی به صورت تابعی از رویدادهای ورودی اولیه، نوشت ( به ضمیمه الف بخش الف ۲ مراجعه کنید.) محاسبات عملی این تابع از رویـداد رأس ( کـه دربـالای درخـت مـی‌باشـد) شـروع شـده و تـا رویدادهای پایه (انتهای درخت) ادامه می‌یابد:

El = T+E2
= T+ (K2+E3)
= T+K2+(S•E4)
= T+K2+S• (S1+E5)
= T+K2+(S•S1) +(S•E5)
= T+K2+(S•S1) +S• (K1+R)
= T+K2+(S•S1) +(S•K1) +(S•R)

که در آن :

E1 = رویداد رأس

E2, E3, E4, E5 = رویدادهای خطای میانی

R = شکست اولیه رله زمان سنج

S = شکست اولیه سوئیچ فشار

S1 = شکست اولیه سوئیچ S1

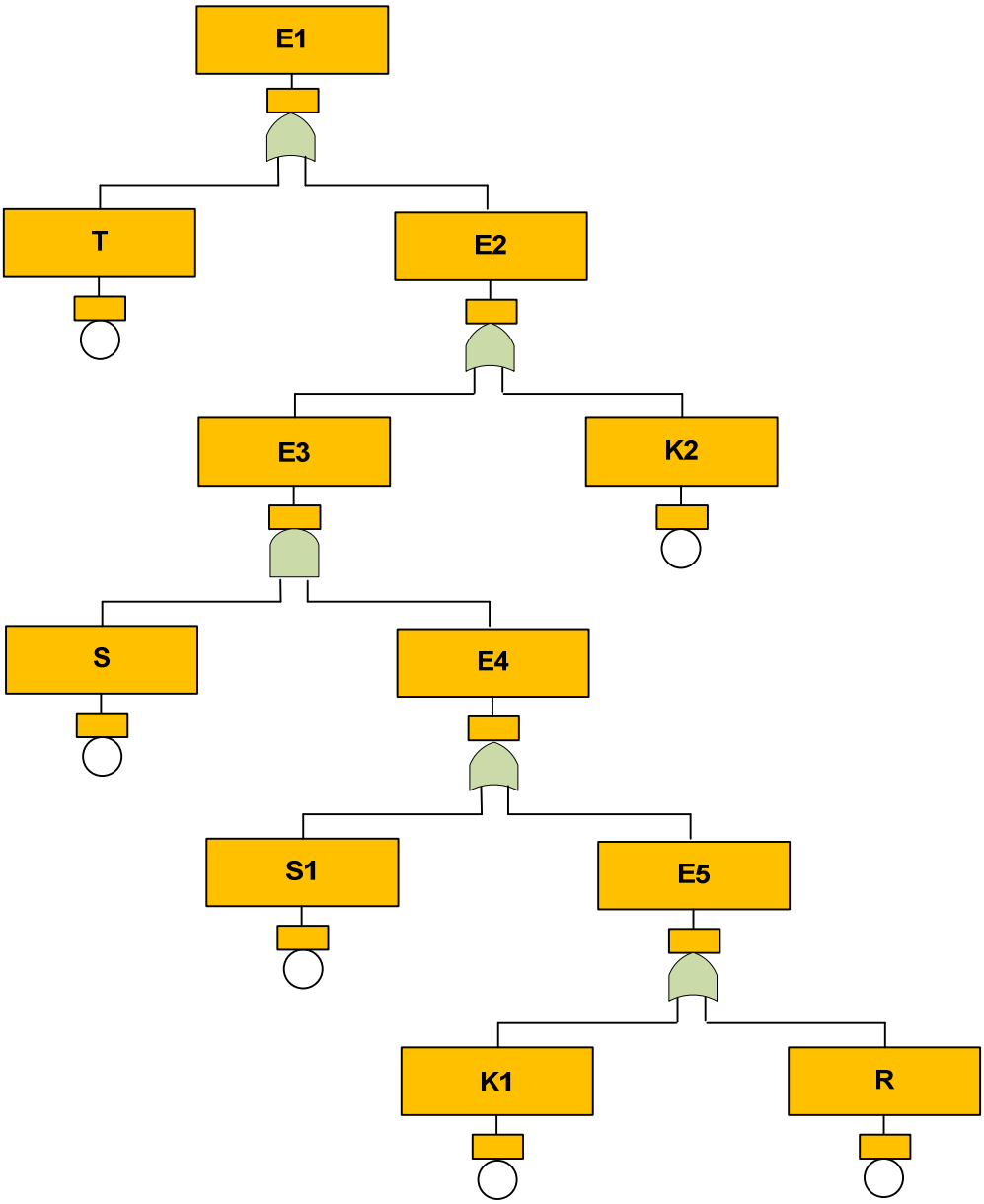
K1 = شکست اولیه رله K1

K2 = شکست اولیه رله K2

T = شکست اولیه مخزن ذخیره

می باشد . در این مثال پنج برش حداقل به شرح زیر از معادله بولی رویداد رأس به دست می‌آید که دو تا از آنها تک و سه تای دیگر دوتایی هستند:

**S•R , S•K1 , S•S1 , T , K2**




**تصویر۸-۱٤ : درخت خطای خلاصه شده مخزن ذخیره تحت فشار**

هر یک از این برشها حداقل مسیر رسیدن به رویداد رأس را مشخص می‌کنند به عنوان مثال درمورد برش S.R ، خرابی هم زمان سوئیچ فشار و رله زمان‌سنج ، احتمال وقوع رویداد راس (ترکیدن مخزن ذخیره ) را به دنبال دارد.

در این مرحله ابتدا یک ارزیابی کیفی و سپس براساس داده‌های موجود ارزیابی کمّی انجام می‌شود. **از نظر کیفی، قطعه عاملی که با خرابی خود به تنهایی منجر به بروز رویداد رأس می‌شود، رله K2 است.** بنابراین با اضافه کردن یک رله زمان سنج دیگر به موازات این رله حساس، می‌توان ایمنی سیستم را به طرز قابل توجه‌ای بالا برد. البته به نظر می‌رسد سیستم فوق از نظر طراحی هم مشکل دارد. قرار دادن تنها یک رله زمان‌سنج به عنوان مانع و پادمان در مقابل شرایط بحرانی فشار درمخزن منطقی به نظر نمی‌رسد. بهتر است در طراحی سخت افزار سیستم نیزاز یک قطعه با ضریب ایمنی بالا ( به عنوان مثال شیر اطمینان) استفاده کرد. اما اگر مخزن ذخیره در شرایط طراحی شده خود، دچار شکست شود (برش حداقل T ) نیز منجر به وقوع رویداد رأس می‌گردد. اما می‌دانیم که این تجهیز بر خلاف رله زمان‌سنج، غیرعامل بوده و احتمال شکست آن درمقابل با K2 بسیار کوچک تر است.

درمورد برشهای حداقل دیگر یعنی S•K1 ,S•S1 و S•R2 ، مشاهده می‌کنید که خرابی سوئیچ فشار (S) در هر ۳ مشترک است که بایستی مدنظر قرار بگیرد. البته به علت ضرب دوتایی اعداد احتمال در این برش‌ها به نظرمی‌رسد که احتمال وقوع بالایی داشته باشند.

به منظور انجام ارزیابی کمّی نتایج، نیاز به تخمین عدد احتمال شکست قطعات داریم درجدول ۸-۱ مقادیر فرضی احتمال شکست قطعات این سیستم، آورده شده است. هر برش حداقل،

اشتراک رویدادها را نشان می‌دهد، با فرض مستقل بودن شکست‌ها، احتمال وقـوع بـرش‌هـا بـا ضرب اعداد احتمال رویدادهای پایه آنها، به روش زیر به دست می‌آید:

**جدول ۸-۱ مقادیر فرضی احتمال شکست قطعات**

| قطعه | نماد | احتمال شکست |
|---|---|---|
| مخزن ذخیره | T | $5 \times 10^{-6}$ |
| رله K2 | K2 | $3 \times 10^{-5}$ |
| سوئیچ فشار | S | $1 \times 10^{-4}$ |
| رله K1 | K1 | $3 \times 10^{-5}$ |
| رله زمان سنج | R | $1 \times 10^{-4}$ |
| سوئیچ S1 | S1 | $3 \times 10^{-5}$ |

مشاهده می‌کنید که رویداد رأس، اجتماع برش‌های حداقل می‌باشد و احتمال آن با اسـتفاده از تقریب رویداد نادر[1] (فصل ۴) برابر با جمع احتمال این برش‌ها می‌شود. با استفاده از محاسـبات مربوط به احتمال وقوع برش‌ها داریم:

[1] Rare Event Approximation

$P[T] = 5\times10^{-6}$

$P[K2] = 3\times10^{-5}$

$P[S\bullet K1] = (1\times10^{-4})\ (3\times10^{-5}) = 3\times10^{-9}$

$P[S\bullet R] = (1\times10^{-4})\ (1\times10^{-4}) = 1\times10^{-8}$

$P[S\bullet S1] = (1\times10^{-4})\ (3\times10^{-5}) = 3\times10^{-9}$

محاسبه احتمال رویداد رأس یعنی E1 ، با توجه بـه محاسـبات بـالا ، دیگـر مشـکل نیسـت .

همانطور که قبلاً گفته شد ، رویداد رأس از نظر مجموعه ها برابر با اجتماع برش هـای حـداقل خود است (به فصل ۷ مراجعه کنید ) :

$$P(Top) = \Sigma\ P(M_i)$$

$$P(M_i) = P(BE_1)P(BE_2)\ \ldots\ P(BE_k)$$

با یک تقریب خوب و جمع احتمال برش های محاسبه شده بالا داریم :

$$P\ (E_1) \cong 3.4\times10^{-5}$$

اهمیت کمی نسبی برش‌های مختلف با تقسیم احتمال وقوع برش بر احتمال وقوع رویداد رأس و درصدگیری به دست می‌آید.

| مجموعه برش حداقل | میزان اهمیت |
|---|---|
| T | 14% |
| K2 | 86% |
| S•K1, S•R , S•S1 | کمتر از 0.1 درصد |

یکی از نتایج بسیار سودمند این مثال، متمایز کردن برش‌های حداقلی است که تنها یک قطعه را در بر می‌گیرند ( شکست اولیه رله K2 ) . اگر این قطعه عامل باشد به نظر می‌رسد در طراحی سیستم بایستی طوری تجدیدنظر کرد که به هنگام رسم درخت خطای شکست ماموریت سیستم، این رویدادهای منفرد از رویداد رأس فاصله داشته و ازطریق گیت‌های AND به آن برسند.

یکی از اشتباهات مکرری که در هنگام رسم درخت خطای این مثال در کارگاه های آموزشی اتفاق می افتد این است که اکثر دانشجویان ، بلافاصله بعد از نوشت رویداد از هم گسیختگی مخزن ذخیره به عنوان رویداد رأس ، متوجه سوئیچ فشار می شوند و تصور می کنند شکست این قطعه تنها شرط لازم و کافی برای وقوع رویداد رأس می باشد . که با آنچه به تفضیل در این فصل آمد ، یک اشتباه محض است .

## ضمیمه الف ) جبر بولی و کاربرد آن در تحلیل درخت خطا

### الف ۱) قوانین جبر بولی

قواعدی که در این بخش خواهد آمد ، کاربرد وسیعی در ارزیـابی کمـی درخـت خطـا دارد .در حقیقت درخت خطا ، تصویری از ارتباطات منطقی بین رویدادهایی است که به رویداد رأس می رسند و می توان این ارتباطات را به شکل معادلات جبری درآورد . بنابراین با تسلط بر قـوانین جبر بول می توان ارزیابی کیفی و کمی ریسک را به خوبی انجام داد و منطق حاکم بر درخت را تفسیر نمود . عمده ترین کاربرد جبر بولی در هنگام پیاده سازی کمی درخـت خطـا و نوشـتن معادلات مربوط به مجموعه برش ها و ساده سازی آنهـا اسـت . در واقـع بـا سـاده کـردن ایـن معادلات ، مجموعه برش های حداقل مشخص خواهند شد .

جدول الف -۱ ، شرح مختصری از قوانین حاکم بر جبر بولی می باشد . خواننده درستی هر از قوانین و روابط فوق را می تواند با استفاده از **نمودار ون**[1] ( توصیف شده در بخش اول ضمیمه ب ) بررسی کند . بر اساس قوانین 1a و 1b عملیات اجتماع و اشتراک ، در مورد دو یا چند رویداد ، خاصیت جابجایی دارد . قوانین 2a و 2b ، از روابط ساده جبری $a(bc) = (ab)c$ و $a+ (b+c) = (a+b) + c$ ، نتیجه گیری شده اند . قوانین توزیع پذیری، در روابط (3a) و (3b)، در جائیکه ترکیبی از عملیات AND و OR موجود باشد، اجازه توزیع عملگر را می‌دهد. یعنی با پیشروی از سمت چپ معادله به سمت راست آن، عبارت سمت چپ گسترده شده و از حالت فاکتورگیری خارج می‌شود. حال اگر از سمت راست معادله به سمت چپ آن برویم، عبارت خلاصه شده و پارامتر مشترک بیرون از پرانتز قرار می‌گیرد. اگر چه رابطه (3a) شبیه به

[1] Venn diagram

**جدول الف- ۱ ) قوانین جبر بولی**

| | نمایش ریاضی | نمایش مهندسی | شرح |
|---|---|---|---|
| (1a) | $X \cap Y = Y \cap X$ | $X \bullet Y = Y \bullet X$ | |
| (1b) | $X \cup Y = Y \cup X$ | $X+Y = Y+X$ | قانون جابجایی[1] |
| (2a) | $X \cap (Y \cap Z) = (X \cap Y) \cap Z$ | $X \bullet (Y \bullet Z) = (X \bullet Y) \bullet Z$ | |
| | | $X \bullet (Y \bullet Z) = (X \bullet Y) \bullet Z$ | قانون شرکت پذیری[2] |
| (2b) | $X \cup (Y \cup Z) = (X \cup Y) \cup Z$ | $X+(Y+Z) = (X+Y)+Z$ | |
| (3a) | $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$ | $X \bullet (Y+Z) = X \bullet Y + X \bullet Z$ | قانون توزیع پذیری[3] |
| | | $X \bullet (Y+Z) = X \bullet Y + X \bullet Z$ | |
| (3b) | $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$ | $X+Y \bullet Z = (X+Y) \bullet (X+Z$ | |
| (4a) | $X \cap X = X$ | $X \bullet X = X$ | |
| (4b) | $X \cup X = X$ | $X+X = X$ | قانون همانی[4] |
| (5a) | $X \cap (X \cup Y) = X$ | $X \bullet (X+Y) = X$ | |
| (5b) | $X \cup (X \cap Y) = X$ | $X+X \bullet Y = X$ | قانون جذب[5] |
| (6a) | $X \cap X' = \phi$ | $X \bullet X' = \phi$ | |
| (6b) | $X \cup X' = \Omega = I^*$ | $X+X' = \Omega = I$ | متمم گیری[6] |
| (6c) | $(X')' = X$ | $(X')' = X$ | |
| (7a) | $(X \cap Y)' = X' \cup Y'$ | $(X \bullet Y)' = X'+Y'$ | نظریه دمورگان[7] |
| (7b) | $(X \cup Y)' = X' \cap Y'$ | $(X+Y)' = X' \bullet Y'$ | |
| (8a) | $\phi \cap X = \phi$ | $\phi \bullet X = \phi$ | |
| (8b) | $\phi \cup X = X$ | $\phi + X = X$ | |
| (8c) | $\Omega \cap X = X$ | $\Omega \bullet X = X$ | عملیات با تهی و مرجع |
| (8d) | $\Omega \cup X = \Omega$ | $\Omega + X = \Omega$ | |
| (8e) | $\phi' = \Omega$ | $\phi' = \Omega$ | |
| (8f) | $\Omega' = \phi$ | $\Omega' = \phi$ | |
| (9a) | $X \cup (X' \cap Y) = X \cup Y$ | $X+X' \bullet Y = X+Y$ | برخی روابط پرکاربرد دیگر |
| (9b) | $X' \cap (X \cup Y') = X' \cap Y' = (X \cup Y)'$ | $X' \bullet (X+Y') = X' \bullet Y' = (X+Y)'$ | |

[1] Commutative Law
[2] Associative Law
[3] Distributive Law
[4] Idempotent Law
[5] Law of Absorption
[6] Complementation
[7] de Morgan's Theorem

قانون توزیع پذیری در جبر است اما رابطهٔ (3b) قانون مشابه‌ای در جبر ندارد. روابط (4a) و (4b) قانون همانی[1] را بیان می‌کند و عمل هر رویداد را بر روی خودش نشان می‌دهد. قانون جذب در روابط (5a) و (5b) براحتی با رسم نمودارهای ون مناسب، قابل اثبات هستند. رابطه (5a) را می‌شود به شکل دیگری نیز تعبیر کرد. اگر وقوع رویداد X به طور خودکار باعث وقوع رویداد Y شود. می‌گوییم رویداد X زیرمجموعه رویداد Y است. این وضعیت به صورت نمادین با رابطهٔ $X \subset Y$ یا $X \rightarrow Y$ نمایش داده می‌شود. در این صورت طبق قاعده جبر بول داریم :

$$X+Y = Y$$

$$X \cdot Y = X$$

در رابطه (5a) اگر رویداد X به وقوع بپیوندد رویداد $(X+Y)$ نیز رخ خواهد داد و از آنجا که $X \subset (X+Y)$ است ، داریم:

$$X \cdot (X+Y) = X$$

بحث مشابه‌ای را نیز می‌توان در مورد رابطه (5b) مطرح کرد. روابط (7a) و (7b) چگونگی حذف علامت متمم را از روی پرانتز نشان می‌دهد که همان قضیه معروف دمورگان است. فرض کنید X نشان دهنده شکست قطعه‌ای می‌باشد. در این صورت 'X کارکرد موفقیت‌آمیز آن را نشان می‌دهد. رابطه (7a) خیلی ساده بیان می‌کند شرط عدم شکست همزمان دو رویداد X و Y این است که یا رویداد X و یا رویداد Y دچار شکست نشوند. برای مشاهده کاربرد این رابطه عبارت زیر را ساده می کنیم .

$$(A+B) \cdot (A+C) \cdot (D+B) \cdot (D+C)$$

[1] Idempotent Law

با اعمال قانون (3b) به رابطه $(A+B)\cdot(A+C)$ ، نتیجه می شود :

$$(A+B)\cdot(A+C) = A+ (B\cdot C)$$

همچنین

$$(D+B)\cdot(D+C) = D+ (B\cdot C)$$

و نتیجه ای که حاصل می شود عبارت است از :

$$(A+B)\cdot(A+C)\cdot(D+B)\cdot(D+C) = (A+B\cdot C)\cdot(D+B\cdot C)$$

اگر رویداد E معادل $B\cdot C$ باشد ، داریم :

$$(A+B\cdot C)\cdot(D+B\cdot C) = (A+E)\cdot(D+E) = (E+A)\cdot(E+D)$$

با استفاده مجدد از رابطه (3b) ، داریم :

$$(E+A)\cdot(E+D) = E+A\cdot D = B\cdot C + A\cdot D$$

و نتیجه نهایی عبارت است از :

$$(A+B)\cdot(A+C)\cdot(D+B)\cdot(D+C) = B\cdot C + A\cdot D$$

مشاهده کنید که چگونه قوانین جبر بولی اجازه ساده سازی و یافتن برش های حداقل را به ما می دهد .

### الف-۲) تعیین مجموعه برش‌های حداقل یک درخت خطا

یکی از هدف‌های اصلی نمایش درخت خطا به شکل معادلات جبر بول این است که از این معادلات می‌توان برای تعیین مجموعه برش‌های حداقل بهره برد. با به دست آوردن برش‌های حداقل، کمی‌سازی درخت خطا کم یا بیش ساده می‌شود.

### برش‌های حداقل

طبق تعریف، یک مجموعه برش حداقل ترکیبی (اشتراکی) از رویدادهای اولیه است که برای وقوع رویداد رأس کفایت می‌کنند. به این ترکیب در صورتی حداقل می‌گویند که برای وقوع رویداد رأس به رخداد تمامی رویدادهای شکست موجود در برش، نیاز باشد. یعنی اگر تنها یکی از این رویدادها حذف شود، مسیر منتهی به وقوع رویداد رأس قطع گردد. هر درخت خطا شامل تعداد قابل شمارش از برش‌های حداقل است که تنها به رویداد رأس اختصاص دارند. برشی که تنها یک قطعه منفرد دارد، شکست‌های منفردی را نشان می‌دهد که به تنهایی باعث بروز رویداد رأس می‌شوند.

برش‌های حداقل با دو رویداد، نشان دهنده این هستند که شرط وقوع رویداد رأس، رخداد همزمان هر دو رویداد می‌باشد و به همین ترتیب برش‌های شامل n رویداد، به شرطی باعث وقوع رویداد رأس می‌شوند که هر n رویداد با هم رخ دهند. رویداد رأس بر حسب برش‌های حداقل خود به شکل زیر نوشته می‌شود:

$$T = M_1 + M_2 + \ldots + M_k$$

که در آن T رویداد رأس و $M_i$ برش حداقل i ام می‌باشد. هر برش حداقل در برگیرنده ترکیب خاصی از شکست‌های قطعه است، بنابراین برای برش حداقلی با n قطعه داریم:

$$M_i = X_1 \bullet X_2 \bullet \ldots \bullet X_n$$

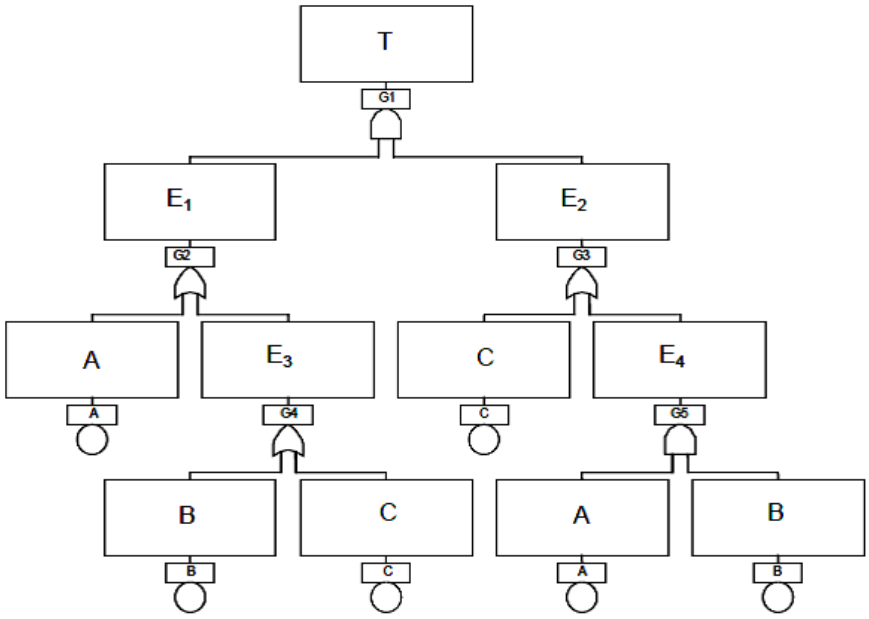
که در آن $X_1$ ، $X_2$ و . . . ، رویدادهای شکست قطعات پایه اند . یک مثال ساده از معادله رویداد رأس عبارت است از :

$$T = A + B \bullet C$$

در این مثال A ، B و C شکست‌های مربوط به قطعات می‌باشند . رویداد رأس فوق شامل یک برش یک قطعه‌ای A و یک برش دو قطعه‌ای (B•C) است. توجه داشته باشید برش‌های حداقل برای هر رویداد رأس منحصر به فرد می‌باشند.

برای تعیین مجموعه برش‌های حداقل یک درخت خطا، ابتدا درخت به صورت معادل بولی‌اش درمی‌آید. الگوریتم‌های متنوعی برای تبدیل درخت خطا به معادلات جبری وجود دارد. دو الگوریتم شایع، روش جایگذاری رو به پایین[1] و روش جایگذاری رو به بالا[2] می‌باشد. این روش‌ها بسیار ساده هستند و برای ساده‌سازی و حذف رویدادهای تکرار شونده، می‌توانیم از قوانین توزیع‌پذیری و جذب استفاده کنیم. درخت خطای ساده تصویر (الف-۱) را در نظر بگیرید. ابتدا جایگذاری رو به پایین را انجام می‌دهیم. با شروع از رویداد رأس و بسط و جایگذاری آن با رویدادهای $E_1$ و $E_2$ داریم.

[1] Bottom-up substitution
[2] Top-down substitution




**تصویر الف ۱ : مثالی از یک درخت خطای ساده**

T = El•E2
El = A+E3
E3 = B+C
E2 = C+E4
E4 = A•B

بنابراین :

$$T = (A+E_3) \cdot (C+E_4)$$
$$= (A•C) + (E3•C) + (E4•A) + (E3•E4)$$

با قرار دادن عبارت معادل $E_3$ داریم :

$$T = A•C + (B+C) •C + E_4•A + (B+C) •E_4$$
$$= A•C + B•C + C•C + E_4•A + E_4•B + E_4•C$$

طبق قانون همانی C•C = C است ، پس :

$$T = A•C + B•C + C + E_4•A + E_4•B + E_4•C$$

و بر اساس قانون جذب ، A•C + B•C + C + E4•C = C است ، یعنی :

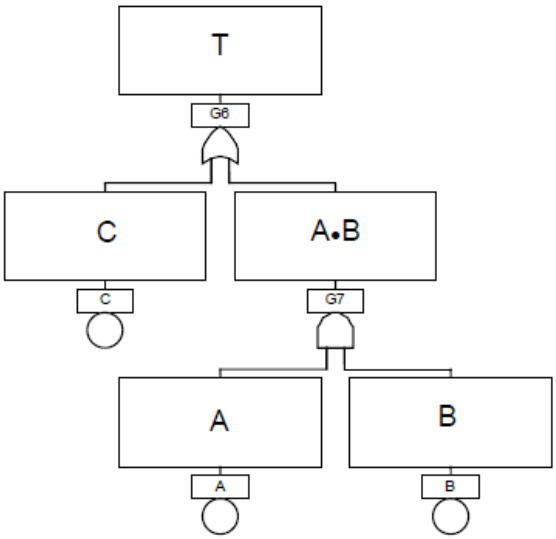
$T = C + E_4 \cdot A + E_4 \cdot B$

و نهایتاً با جایگذاری $E_4$ و استفاده دوباره از قانون جذب ، داریم :

$T = C + (A \cdot B) \cdot A + (A \cdot B) \cdot B$

$= C + A \cdot B$

بنابراین برش های حداقل عبارتند از : C و $A \cdot B$ ، که یکی از برش‌ها یک جزء ودیگری دو جزء دارد. حالا می‌توان درخت خطا را با این ساده سازی دوباره رسم کرد (تصویر الف -۲)




**تصویر الف- ۲ : درخت خطای معادل تصویر الف - ۱**

روش جایگذاری رو به بالا شبیه به همین روش می‌باشد با این تفاوت که این بار، جایگذاری از پایین درخت شروع شده و به سمت رویداد رأس، گسترش پیدا می‌کند. البته این روش مستلزم صرف وقت بیشتر و دشوارتر می‌باشد. مجدداً به مثال خود برمی‌گـردیم. (بـرای راحتـی و درک بهتر خواننده معادلات دوباره تکرار شده‌اند)

T = El•E2
El = A+E3
E3 = B+C
E2 = C+E4
E4 = A•B

چون $E_4$ تنها شکست‌های (رویدادهای) پایه را شامل می‌شود ، آن را در معادلهٔ بالا سری خود یعنی معادلهٔ $E_2$، قرار می‌دهیم. $E_3$را هم که بر حسب رویدادهای پایه است در معادله $E_1$ قرار می‌دهیم. و در گام آخر $E_1$ و $E_2$ را جایگزین حروف مشابه در معادلهٔ T (رویداد رأس ) می‌نماییم و سپس با بهره‌گیری از قانون جذب، معادلهٔ بولی رویداد رأس را ساده می‌کنیم از این روش هم نتیجه یکسانی برای مجموعه برش‌های حداقل به دست می‌آید. (تمرین این حالت را به عهده خواننده می گذاریم)

به عنوان مثال ساده دیگر، سیستم پمپاژ تصویر (الف-۳) را در نظر بگیرید. فرض کنید رویداد نامطلوب **عدم جریان یافتن آب به سمت نازل‌های دیلاژ** باشد. با صرف نظر کردن از سهم لوله‌های رابط (در بروز رویداد نامطلوب)، این سیستم را می‌توان مانند تصویر (الف-۲) با درخت خطا تحلیل کرد.

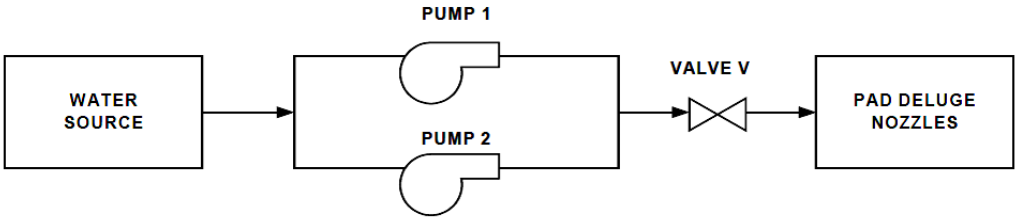
تعریف رویدادها چنین است:

T = عدم جریان یافتن آب به سمت نازل‌های دیلاژ

C = شیر V بسته نمی‌شود.

A = پمپ 1 روشن نمی‌شود.

B = پمپ 2 روشن نمی‌شود.




**تصویر الف- ۳ : سیستم پمپاژ آب**

در مثال قبل نشان داده شد که برش‌های حداقل درخت مربوط به این سیستم C و A.B است. بنابراین رویداد نامطلوب (T) زمانی اتفاق می‌افتد که یا شیر V بسته نشود و یا پمپ‌های 1 و2 به طورهم زمان از کار بیفتند. در این مثال ساده، برش‌ها تحلیل پیچیده‌ای از سیستم ارائه نمی‌دهند که نتوان با بررسی گذرای سیستم آن را به دست آورد. اما برای سیستم‌های پیچیده که حالت‌های شکست قطعات اینقدر واضح نباشد، برش‌های حداقل کمک شایانی به تحلیل‌گر در شناسایی عناصر و قطعات شاخصی که باعث بروز رویداد ناخواسته می‌شوند، می‌نماید. نکته دیگر اینکه برای درخت خطاهای کم حجم، به دست آوردن برش‌های حداقل به روش دستی قابل انجام است اما برای درخت خطاهای بزرگ‌های پیچیده می‌توان از نرم‌افزارهای کارآمد استفاده نمود.

## ضمیمه ب) نظریه احتمال: توصیف ریاضی رویدادها

این ضمیمه تکنیک ریاضی پایه مورد نیاز برای کمی سازی درخت خطا یعنی نظریه احتمال را شرح می‌دهد. نظریه احتمال در تحلیل درخت خطا ضروری می‌باشد چرا که بـه بررسـی رفتـار رویدادها می‌پردازد. رویدادهایی که عناصر اصلی درخت خطا هستند. عناوینی که در این بخش مورد بحث قرار می‌گیرند عبارتند از: نظریه مجموعه‌ها، جبر احتمال و قضیه بیز[1].

### ب-۱) نظریه مجموعه‌ها- بررسی ریاضی رفتار رویدادها

در نظریه مجموعه‌ها، رویدادهای نتیجه شده از یک تجربه، به منظـور تعیـین مقـادیر احتمـال سازماندهی می‌شوند. مجموعه ، گردآیه‌ای از اشیاء است که ویژگی متمایز و مشترکی دارند. بـه عنوان مثال اعداد اول ، رله‌ها ، روباه‌های خاکستری و غیره.

اما مجموعه مورد علاقه ما در درخت خطا، رویدادهای حاصل شده از تجربه‌های تصادفی است و به همین دلیل در مطالعه نظریه احتمال، نظر خود را بیشتر به رویـدادها، معطـوف مـی‌کنـیم . می‌توان تصور کرد که رویداد، گردآیه‌های از عناصراست. برای مثال رویـدادهای زیـر را حاصـل تجربه پرتاب تاس هستند، در نظر بگیرید.

A = عدد روی تاس،۲ است.

B= نتیجه یک عدد زوج است.

C= نتیجه عددی کمتر از ۴ است.

D = هرعددی که روشده باشد.

[1] Bayes theorem

E = نتیجه بر ۷ بخش‌پذیر است.

هر یک از این رویدادها، با مجموعه‌ای از فضای نمونـه ایـن تجربـه یعنـی {۶، ۵، ۴، ۳، ۲، ۱} ، مشخص می‌شوند :

A = {2}
B = {2, 4, 6}
C = {1, 2, 3}
D = {l, 2, 3, 4, 5, 6}
E = φ

که در آن آکلادها " {} " نشاندهنده یک مجموعه خاص و مقادیر داخل آن، عناصر ایـن مجموعه هستند. رویداد A تنها یک عنصر دارد (عدد ۲) و رویدادهای B و C مجموعه‌هایی با ۳ عنصر هستند. مجموعهٔ D شامل تمامی نتایج ممکن می‌باشد و بر فضای نمونه تجربه، منطبق شده است که مجموعه مرجع[1] نامیـده شـده و عمومـاً بـا نمـاد Ω یـا I نشـان داده می‌شود. رویدادE ناممکن بوده و مجموعه‌ای نمایش می‌دهد که هیچ عنصری نـدارد و بـه مجموعه تهی معروف است وبا نماد φ نمایش داده می شود .

با برگشت دوباره به مثال پرتاب تاس، مشاهده می‌کنید عدد ۱ به هر دو مجموعه C و D و نه A یا B تعلق دارد. این مطلب با علائم ریاضی زیر مشخص می‌شود.

$$1\in C,\ 1\in D,\ 1\notin A,\ 1\notin B$$

که در آن نماد ∈ به معنی « تعلق دارد به » و نماد ∉ به معنای «تعلـق نـدارد بـه» اسـت. همچنین به علت آنکه عناصر A ، B، C همگی در مجموعه D نیز هستند گفته می‌شود که آنها زیرمجموعه D می‌باشند و نمایش ریاضی این مطلب به صورت زیراست:

[1]Universal Set

$A \subset D, B \subset D, C \subset D$

در این مثال دو مجموعه مساوی نداریم. اما در حالت کل اگر X و Y دو مجموعه باشند با این شرط که X زیرمجموعه Y و همچنین Y زیرمجموعه X باشد، این دو مجموعه با هم معادل هستند. بیان ریاضی جملات بالا عبارت است از :

$X \subset Y$ و $Y \subset X$

به عنوان مثال دیگر، فرض کنید t (برحسب ساعت) زمان خرابی یک موتور دیزل باشد و مجموعه‌های زیر ار در نظر بگیرید:

A= شکست موتور دیزل در هنگام راه‌اندازی

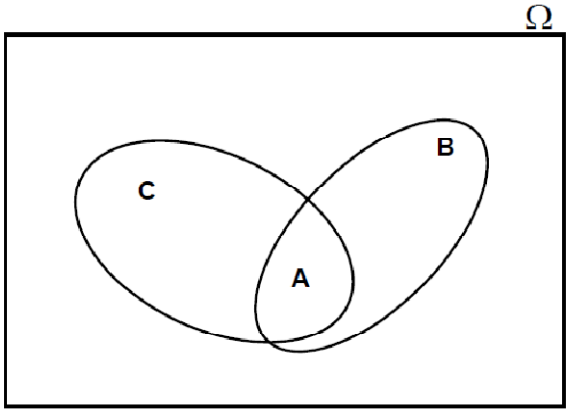
$A = \{t=0\}$
$B = \{t_i, 0 < t \leq 1\}$
$C = \{t_j, t > 1\}.$

B= شکست موتور دیزل در زمانی بین صفر تا یکساعت

C= شکست موتور دیزل در زمانی بیش از یکساعت

هر یک از این مجموعه‌ها (رویدادها) را می‌توان مرتبط با یک وضعیت غیرعادی سیستم (مثلاً قطع ناگهانی برق) دانست. برای درک بهتر مجموعه‌ها معمولاً از نمودارهای گرافیکی نظیر **نمودار ون** استفاده می شود. برای رسم نمودار، ابتدا مجموعه مرجع با یک شکل هندسی دلخواه (مثلاً مستطیل) رسم شده و سپس زیرمجموعه‌های آن (رویدادها) با اشکال دیگر در داخل آن رسم می‌شوند. تصویر (ب-۱)، نمودار ون مربوط به مثال پرتاب تاس را نشان می‌دهد. عملیات بر روی مجموعه‌ها (رویدادها) را می‌توان با کمک نمودار ون، تعریف کرد. به عنوان مثال، اجتماع دو مجموعه در تصویر (ب-۲) آمده است.

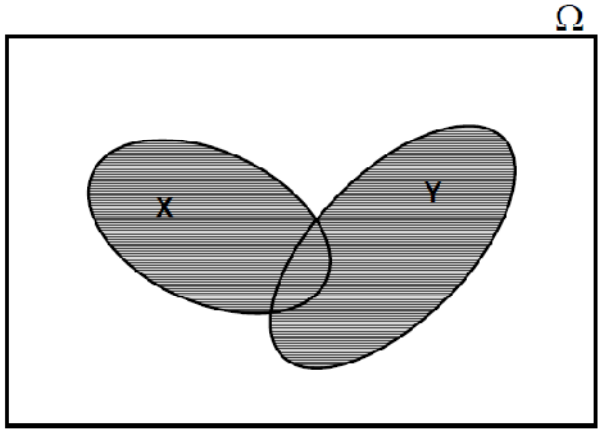
**تصویر ب-۱) نمودار ون**




اجتماع دو مجموعه X و Y، مجموعه ای است که تمامی عناصر X یا Y و یا هـر دو را در خـود دارد وبه شکل XUY نوشته می‌شود (ناحیه سایه‌خورده تصویر ب-۲) . به عنوان مثال اجتمـاع دو رویداد B و C در تجربه پرتاب تاس برابر است با :

$$B \cup C = \{1, 2, 3, 4, 6\}$$

**تصویر ب- ۲ : اجتماع مجموعه ها**

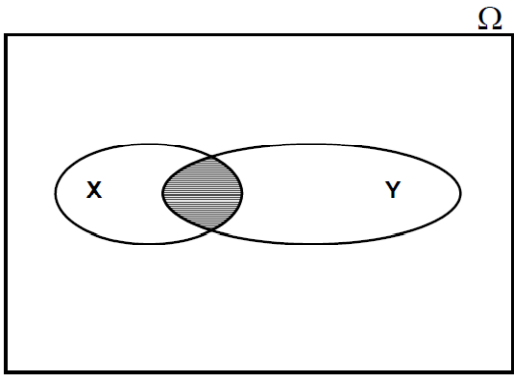



اشتراک دو مجموعه X و Y، مجموعه‌ای است که تمامی عناصر مشترک آنها را در خود دارد و به شکل X∩Y نوشته می‌شود (ناحیه سایه خورده تصویر ب-۳) . **مثلاً برای مثال پرتاب تاس داریم :**

$$B \cap C = \{2\} = A$$

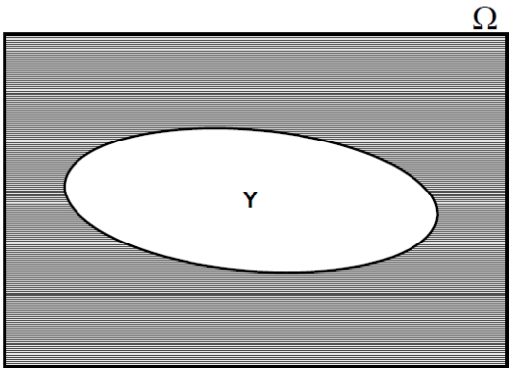
توجه کنید که کلمهٔ «و» به نماد ∩ تبدیل شده است.

**تصویر ب ۳ : اشتراک مجموعه ها**




عمل متمم‌گیری در تصویر ب-۴ آمده است. متمم مجموعه X ، شامل تمام عناصری است که در X نیست و به شکل □X ( یا X' )نوشته می‌شود و در تصویر ب -۴ به صورت سایه‌دار مشخص شده است.

**تصویر ب - ۴ : متمم یک مجموعه**




در مورد مثال پرتاب تاس، متمم مجموعه B∪C برابر است با:

$$(B \cup C)' = \{5\}$$

عمل تفریق در مجموعه‌ها نیز تعریف می‌شود که جدا از عملیات دیگر نیست. در تصـویر ب-۵ عمل تفریق مجموعه‌ها نمایش داده شده است شکل ریاضی این رابطه برای دو مجموعه‌ای است که اعضای آن در مجموعه Y هست، اما در مجموعه X نیست که در نظریه مجموعه ها با نمـاد (Y-X) یا $Y \cap X'$ نمایش داده می شود .به عنوان مثال سیستم ساده‌ای را در نظـر بگیریـد کـه شامل ۳ قطعه A ، B و C است. فرض کنید همین حروف نشان دهنده رویدادهایی باشـند کـه کارکرد موفقیت آمیز قطعات را تعریف می‌کند یعنی:

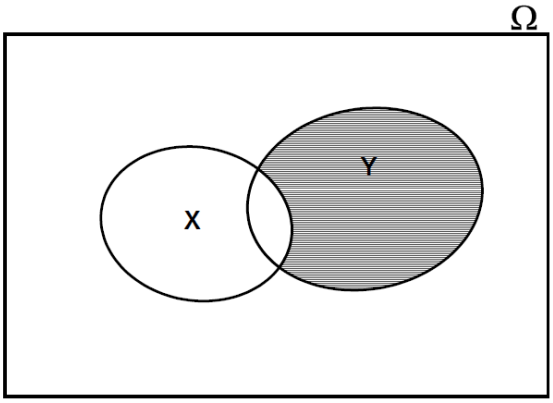
A = قطعه A به درستی کار می‌کند.

B= قطعه B به درستی کار می‌کند.

C = قطعه C به درستی کار می‌کند.

در این صورت $\overline{C}, \overline{B}, \overline{A}$ ، نشاندهنده متمم این رویدادها خواهند بود . در نتیجه عبارت $A\overline{B}C$ به معنی کارکرد درست قطعه A، خرابی قطعه B و کارکرد صحیح قطعه C خواهد شد.

**تصویر ب -۵ : رابطه (Y-X)**



چون ۳ قطعه و دوحالت کارکرد برای هر قطعه (درستی/ خرابی) داریـم، جمعـاً $2^3 = 8$ یـا ۸ ترکیب مختلف برای این سیستم به دست می‌آید . بنابراین مجموعه مرجع یا فضای نمونه نتایج به شکل زیر خواهد بود :

$$\Omega = \left\{ABC, AB\overline{C}, A\overline{B}C, A\overline{BC}, \overline{A}BC, \overline{A}B\overline{C}, \overline{AB}C, \overline{ABC}\right\}$$

فرض کنید سیستم در صورتی که دو قطعه یا سه قطعه آن از کار بیفتد، متوقف شود (شکسـت مأموریت سیستم) بنابراین رویدادهای زیر بیانگر وضعیت‌های شکست سیستم خواهند بود:

$$S_1 = A\overline{BC}$$
$$S_2 = \overline{A}B\overline{C}$$
$$S_3 = \overline{AB}C$$
$$S_4 = \overline{ABC}$$

و رویداد شکست سیستم (S) را می‌توان با عبارت

$$S = S_1 \cup S_2 \cup S_3 \cup S_4 = \left\{A\overline{BC}, \overline{A}B\overline{C}, \overline{AB}C, \overline{ABC}\right\}$$

نشان داد. بنابراین تمامی مسیرهای منتهی به شکست سیستم در این مجموعه آمده اسـت کـه اطلاعات مفیدی را در کاربردهای مختلف در بردارد. به عنوان مثال اگر احتمال شکست قطعات معلوم باشد، احتمال شکست سیستم قابل محاسبه می‌شود. با استفاده از نظریـه مجموعـه‌هـا و مفاهیم آن، احتمال معادلات اشتراک و اجتماع با روابط زیر مشخص می‌شوند.

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

$$P(A \cap B) = P(A|B)\,P(B) = P(B|A)\,P(A)$$

**ب-۲) نمادها و علائم**

جبر بولی یا جبر رویدادها، با استفاده از از نمادهای خاص ، روابط متفاوتی را بر روی رویدادها تعریف می‌کند . متاسفانه علائم مورد استفاده در نظریه مجموعه‌ها یک دست و یک شکل نیست و نماد ها در حوزه های مختلف احتمال، ریاضیات ، منطق و مهندسی متفاوت است . جدول زیر نمونه ای از کاربرد این علائم را نشان می‌دهد.

| Operation | Probability | Mathematics | Logic | Engineering |
|---|---|---|---|---|
| Union of A and B | A or B | $A \cup B$ | $A \vee B$ | A+B |
| Intersection of A and B | A and B | $A \cap B$ | $A \wedge B$ | A•B or AB |
| Complement of A | not A | A' or $\overline{A}$ | -A | A' or $\overline{A}$ |

نماد هایی که در ریاضیات و منطق استفاده می شوند ، بسیار شبیه به هم هستند . البته نماد های منطقی قدمت بیشتری دارند . در واقع نماد " V " ، علامت اختصاری کلمه لاتین" ver" به معنای OR است . متاسفانه استفاده از نمادهای + و – به جای ∪ و ∩ ، در کاربردهای مهندسی ، گاهی دردسر ایجاد می کند . به عنوان مثال در رابطه زیر:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

اگر به جای نماد ∪ از علامت + استفاده شود. رابطه سمت راست شکل کاملاً متفاوتی پیدا می کندکه ممکن است باعث سردرگمی شود. با این حال در تحلیل درخت خطا از نمادها وعلائم مهندسی که کاربرد گسترده‌ای دارد، استفاده می‌شود.

**ب- ۳) مباحث دیگری از مجموعه‌ها**

یکی از بحث‌های متداول در مجموعه‌ها، تفاوت بین رویداد ساده و رویداد ترکیبی می‌باشد. این جداسازی در مورد برخی مفاهیم درخت خطا قابل استفاده بوده و منجر به تعریف دقیق‌تری از احتمال می‌شود. دوباره به مثال پرتاب تاس برمی‌گردیم. رویداد A = {2} یک رویداد ساده است در واقع تنها یک عنصر از فضای نمونه را در خود دارد. از طرف دیگر رویدادهای B = {2, 4, 6} و C = {1, 2,3} رویدادهای ترکیبی هستند. آنها را به تنهایی نمی‌توان جایگزین عناصر فضای نمونه کرد گرچه خود عناصری از این فضا را شامل می‌شوند. البته این دو رویداد از هم جدا نبوده و مجموعه اشتراک آنها تهی نیست.

رویدادهای ترکیبی (مانند B و C) عموماً، در جهان حقیقی متمایز و مورد توجه هستند. رویدادهای ترکیبی را یک کلاس می‌نامند.کلاس، مجموعه‌ای است که عناصر آن خود مجموعه هستند و با نوشتن تمامی ترکیبات ممکن اعضای یک فضای نمونه، ساخته می‌شوند. به عنوان مثال ، فضای نمونه ۴ عنصری S = {1, 3, 5, 7} را در نظر بگیرید. اگر هر ترکیب ممکن این ۴ عنصر، فهرست شوند، کلاس $\underline{S}$ ساخته می‌شود.

S = {1}, {3}, {5}, {7}, {1, 3},{1, 5}, {1, 7}, {3, 5}, {3, 7}, {5, 7}, {1, 3, 5}

{1, 5, 7}, {1, 3, 7}, {3, 5, 7}, {1, 3, 5, 7}, {φ}

توجه داشته باشید که مجموعه تهی در کلاس فضای نمونه می‌باشد.همانطور که مشاهده می کنید ، تعداد عناصر کلاس $\underline{S}$ مثال بالا برابر ۱۶ یا $۲^۴$ است . این قاعده کلی است یعنی اگر

تعدا عناصر یک مجموعه مرجع یا فضای نمونه n باشد ، تعداد عناصر کلاس آن $2^n$ است . بنابراین یک کلاس در بردارنده تمامی نتایج متصور یک تجربه می‌باشد. به همین دلیل اگر چه عناصر فضای نمونه تجربه پرتاب تاس فقط ۶ تاست اما تعداد عناصر کلاس آن $2^6$ یا ۶۴ می‌باشد. در پرتاب ۲ تاس، S شامل ۳۶ عنصر و $\underline{S}$ حاوی $2^{36}$ عنصر (عددی نزدیک به $10^{10}$) است. یک رویداد نمونه در این تجربه آمدن مجموعه ۷ می‌باشد که در زیر آمده است.

$$E = \{(1, 6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1)\}$$

مجدداً سیستم ۳ قطعه‌ای A ، B و C را در نظر بگیرید که توقف سیستم منوط به شکست یا خرابی ۲ قطعه یا بیشتر باشد. در این مثال، مجموعه مرجع شامل ۸ عنصر و کلاس آن $2^8$=۲۵۶ عنصر دارد. مجموعه‌های زیر به عنوان رویداد از کلاس این تجربه استخراج شده‌اند:

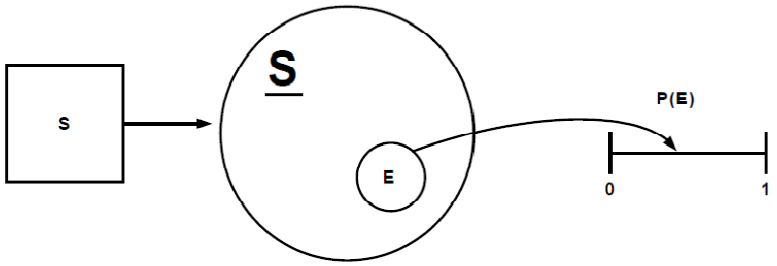
√ A درست کار می‌کند : $\{ABC, AB\overline{C}, A\overline{B}C, A\overline{B}\overline{C}\}$

√ B و C خراب شده‌اند : $\{A\overline{B}\overline{C}, \overline{A}\overline{B}\overline{C}\}$

√ هر ۵ عنصر خراب هستند : $\Phi$

√ سیستم متوقف شده است : $\{A\overline{B}\overline{C}, \overline{A}B\overline{C}, \overline{A}\overline{B}C, \overline{A}\overline{B}\overline{C}\}$

به هر حال همواره به خاطر داشته باشید عناصر یک کلاس، همگی مجموعه هستند. حال با داشتن اطلاعات راجع به تمامی نتایج ممکن ازیک تجربه که به صورت رویداد یا مجموعه کلاس آن، آمده‌اند می‌توانیم تعریف مناسبی از تابع احتمال ارائه دهیم تعریف تئوریک مجموعه‌ها از تابع احتمال در تصویر (ب- ۶) مشاهده می‌شود.




**تصویر ب ۶ : تعریف احتمال بر اساس نظریه مجموعه ها**

در تصویر (ب-۶) جعبه‌ای که با برچسب S مشخص شده، نتایج حاصل از یک آزمـون تصـادفی است. که به عنوان مثال می‌تواند مثال می‌تواند ۳۶ حالت حاصل از پرتاب دو تاس باشـد. دایـره مشخص شده با برچسب S ، کلاس به دست آمده از ترکیبات مختلف عناصرS است و همانطور که قبلاً ذکر شد تعداد عناصر آن بیش از $۱۰^{۱۰}$ است. عناصری که هر نتیجه متصور (سـاده یـا مرکب) این آزمون را نمایش می‌دهند. مثلاً رویداد E (جمع دو عدد نشان داده شـده ۷ اسـت) عضوی از S است. رویداد فوق در تصویر (ب-۶) به صورت شماتیک آمده است. حال محوری از اعداد حقیقی که بین صفر و یک هستند، رسم می‌کنیم. می‌توان تابعی بدین شکل تعریف کرد که رویداد E را بر روی نقطه‌ای از محور، نگاشت کند. این تابع همان تابع احتمال P(E) اسـت. شاید مفهوم نگاشت برای شما ناآشنا باشد. در این کتاب منظور از نگاشت ، خیلی سـاده برقـرار کردن یک تابع رابط است. به عنوان نمونه، رابطهٔ $Y = X^2$، تمـامی مقـادیر X را بـر روی یـک سهمی می‌نگارد (نقاطی مانند $Y = +1$ و $X = \pm 1$) . رابطه Y=X تمامی مقـادیر X را بـر روی یک خط با شیب ۴۵ درجه نسبت به محور Y، نگاشت می‌کند. در این مثـال‌هـا یـک بـازه از اعداد بر روی بازه دیگری از اعداد، قرار می‌گیرد که به توابع نقطه‌ای[1] معروف اند . در مورد تابع احتمال $P(E)$، قضیه کمی پیچیده است. این تابع نگاشت یک مجموعه برروی بازه‌ای از اعـداد

[1] Point Functions

است و به جای تابع نقطه‌ای، تابع مجموعه‌ای[1] نامیده شود اگر چه از نظر ماهیت تفاوتی بـا آن ندارد. در تعریفی ساده‌تر، تابع احتمال یک عدد منحصر به فرد را به هر رویداد، نسبت می‌دهد. در اینجا ذکر دو مطلب لازم است. اول اینکه تابع احتمـالی کـه تعریـف شـد بـدون اسـتفاده از محدودیت تناسب‌گیری (نسبت تعداد نتایج مورد نظر به کل نتایج) بود. دوم اینکه، این تعریـف روشی را برای محاسبه احتمال بیان نمی‌کند بلکه تنها ماهیت ریاضی تـابع احتمـال را تشـریح می‌کند. اگر E، رویداد آمدن جمع ۷ در آزمون پرتاب دو تاس باشـد ، روش محاسـبه احتمـال رخداد E چنین است:

$$P(E) = \frac{6}{36} = \frac{1}{6}$$

البته این تنها یک مثال ساده است. در دیگر موارد و گاهی با تفضیل بیشـتر، بایسـتی طبیعـت فیزیکی مسئله را بررسی کرد تا بتوان احتمال رویداد مورد نظر را به دست آورد.

### (ب-۴) اعمال جبری با احتمالات

یک تجربه تصادفی با دو نتیجه ممکن A و B را در نظر بگیرید. اگر این دو رویداد نامتداخل[2] ( مانع الجمع) باشند در این صورت وقوع همزمان A و B منتفی است . به عنوان مثال در آزمون پرتاب سکه، انتظار داریم تنها خط و یا شیر بیاید. رخداد همزمان ایـن دو رویـداد غیـر ممکـن است. با فرض مانع الجمع بودن دو رویداد A و B داریم:

$$P(A \text{ or } B) = P(A) + P(B)$$

[1] Set Function
[2] Mutually exclusive

این فرمول به فرمول **جمع احتمالات** معروف است و قابل تعمیم برای تعداد نامتناهی از رویدادهای مانع الجمع می باشد . فرمول کلی برای تعداد نامتناهی از رویدادهای نامتداخل A ، B ، C ، D ، E و . . . ، عبارت است از:

P (A or B or C or D or E or …) = P (A) + P (B) + P(C) + P (D) + P (E) + …

برای رویدادهایی که این ویژگی را ندارند ، باید از فرمول کلی تری استفاده کرد. به عنوان مثال پرتاب یک تاس را با دو رویداد داده شده زیر، در نظر بگیرید.

A = آمدن عدد ۲ بر روی تاس

B = آمدن عدد زوج بر روی تاس

واضح است که این دو رویداد مانع الجمع نیستند چرا که اگر عدد ۲ مشاهده شود در واقع هر دو رویداد اتفاق افتاده‌اند . اگر A و B دو رویداد به هم وابسته باشند . داریم:

P (A or B) = P (A) + P (B) - P (A and B)

اگر رویدادها مانع الجمع باشند ( یعنی اشتراک آنها عضوی نداشته باشد) ، عبارت آخر فرمول بالا صفر خواهد شد . یعنی :

P (A and B) = 0

حال به مسئله پرتاب یک تاس برمی‌گردیم. احتمال مشاهده کردن عدد ۲ یا عدد زوج بر روی تاس با توجه به اینکه اشتراک آنها تهی نیست ، اینگونه محاسبه می گردد :

P (A or B) = 1/6 + 1/2 - 1/6 = ½

تعمیم فرمول بالا برای ۳ رویداد وابسته A ، B و C ، عبارت است از :

P (A or B or C) = P (A) + P (B) + P(C) - P (A and B) - P (A and C) - P (B and C) + P (A and B and C).

و تعمیم آن برای n رویداد وابسته $E_n,...,E_2,E_1$ عبارت است از :

$$P(E_1 \text{ or } E_2 \ldots \text{or } E_n) = \sum_{i=1}^{n} P(E_i) - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} P(E_i \text{ and } E_j)$$
$$+ \sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=j+1}^{n} P(E_i \text{ and } E_j \text{ and } E_k) \ldots$$
$$+ (-1)^n P(E_1 \text{ and } E_2 \text{ and} \ldots \text{and } E_n),$$

کـه در آن Σ ، علامـت جمـع اسـت. اگـر از احتمـال وقـوع همزمـان دو یـا چنـد رویـداد Ei صرف‌نظرکنیم. معادله کلی فوق به شکل زیر خلاصه می‌شود:

$$P(E_1 \text{ or } E_2 \text{ or} \ldots \text{or } E_n) = \sum_{i=1}^{n} P(E_i)$$

که به **تقریب رویداد نادر**[1] معروف است و با شرط اینکه $P(E_i) < 0.1$ باشد، دقتـی تـا ده درصـد دارد. حال دو رویداد A و B که متقابلاً مستقل[2] هستند را در نظر بگیریـد منظـور از مسـتقل بودن رویدادها این است که اگر شما چندین بار تجربه را تکرار کنید وقوع (یا عدم وقوع) رویداد A هیچ تأثیری بر وقوع ( یا عدم وقوع) رویداد B و بالعکس نداشته باشـد. بـه عنـوان مثـال در پرتاب سکه، با شرط اینکه سکه کاملاً یکنواخت و متعادل باشد، آمدن خط در پرتاب اول، هـیچ تأثیری بر احتمال آمدن خط یا شیر در پرتاب دوم نخواهد داشت. اگـر A و B مسـتقل باشـند داریم:

$$P(A \text{ and } B) = P(A)\, P(B)$$

[1] Rare event approximation

رویداد نادر ، رویدادی است که به ندرت اتفاق می افتد (مترجم)

[2] Mutually independent

رابطه بالا قابل تعمیم به تعداد نامتناهی از رویدادها بوده و **به قانون ضرب احتمال**[1] مشهور است .به عنوان مثال احتمال مشترک ۴ رویداد مستقل عبارت است از :

P (A and B and C and D) = P (A) P (B) P(C) P (D)

اغلب با رویدادهایی مواجه می‌شویم که مستقل نبوده و یک نوع وابستگی به هم دارند. به عنوان مثال گرم شدن بیش از حد یک مقاومت در یک مدار الکتریکی، احتمال خرابی ترانزیستور نزدیک به این مقاومت را افزایش خواهد داد. یا احتمال آمدن باران در روز سه شنبه ممکن است به وضعیت آب و هوای روز دوشنبه وابسته باشد. در مورد این نوع رویدادها، مفهوم احتمال شرطی را با رابطه زیر تعریف می‌کنیم.

P (A and B) = P (A) P (B|A) = P (B) P (A|B)

که در آن P(B|A) به معنای احتمال وقوع رویداد B به شرط رخ دادن رویداد A است. اگر رویدادها مستقل باشند داریم:

P (A and B) = P (B) P (B)

و برای n رویداد $E_n,...,E_2,E_1$ ، این رابطه به شکل زیر بسط داده می شود :
P (E1 and E2 and ... En) = P (E1) P (E2|E1) P (E3|E1 and E2)… P (En|E1 and E2 ... and En-1).

برای درک بهتر این فرمول، تجربه تصادفی زیر را در نظر بگیرید:

فرض کنید ۴ جعبه کارت۹ تایی داریم که در هر جعبه بر روی کارت‌ها اعداد یک تا ۹ نوشته شده است. کارت‌های این ۴ جعبه را به خوبی مخلوط می‌کنیم و از بین ۳۶کارت یک کارت را انتخاب و بعد از مشاهده عدد روی آن، کنار می‌گذاریم.

[1] Multiplication rule for probabilities

(اگر کارت به دسته کارت‌ها برنگردد، اصطلاحاً نمونه‌گیری بدون جایگذاری انجام شده است) سپس کارت دیگری را انتخاب و عدد روی آن را یادداشت می‌کنیم حال می‌خواهیم احتمال دیدن حداقل یک عدد ۱ در دو کارت مشاهده شده را محاسبه‌کنیم. تعداد حالات مطلوب ما عبارت است از:

- اولین کارت یک است ولی دومی خیر
- اولین کارت یک نیست ولی دومی هست.
- اولین کارت یک و دومین کارت هم یک است.

پس داریم:

P (A) = (احتمال مشاهده حداقل یک کارت با شماره یک در دو بار انتخاب تصادفی)
P (A) = P (A1 and □2) + P (□1 and A2) + P (A1 and A2)
= P (A1) P (□2|A1) + P (□1) P (A2|□1) + P (A1) P (A2|A1)

که در آن زیرنویس‌ها اشاره به مرتبه مشاهده کارت دارد. محاسبه عددی عبارت بالا به شکل زیر است :

$$P(A)=\left(\frac{4}{36}\right)\left(\frac{32}{35}\right)+\left(\frac{32}{36}\right)\left(\frac{4}{35}\right)+\left(\frac{4}{36}\right)\left(\frac{3}{35}\right)=0.213$$

با این تعبیر، می‌توانیم مثلاً احتمال مشاهده عدد ۱۹ یا ۹۱ (بدون جایگذاری )را محاسبه کنیم:

P (A) = (احتمال مشاهده عدد ۱۹ یا ۹۱ در دو بار انتخاب تصادفی)

$$P(A) = P(A_1 \text{ and } A_9) = P(A_1)P(A_9|A_1) + P(A_9)P(A_1|A_9)$$

که در آن اندیس ها نشان دهنده عدد مشاهده شده می باشد . مانند مثال قبل داریم :

$$P(A)=\left(\frac{4}{36}\right)\left(\frac{4}{35}\right)+\left(\frac{4}{36}\right)\left(\frac{4}{35}\right)=0.025$$

نکته قابل ذکر این است که اگر رویدادهای مشاهده عدد ۱و ۹، مستقل بودند ، داشتیم:

$$P(A)=\left(\frac{4}{36}\right)^2=0.012\neq 0.025$$

بنابراین این رویدادها مستقل نیستند. البته خواننده می‌تواند در مورد استقلال رویدادها در صورتیکه بعد از انتخاب کارت اول و مشاهده آن، مجدداً کارت به دسته‌کارتها برگردانده شود، تحقیق کند. نتیجه‌ای که قابل استفاده برای درخت خطا هم هست، محاسبه احتمال وقوع حداقل یک رویداد از بین رویدادهای مستقل است.

فرض کنید

$$\{E_1,E_2,E_3,\ldots,E_n\}$$

مجموعه‌ای از رویدادهای مستقل متقابل باشند . همچنین منظور از رویداد $E_1$ عدم وقوع رویداد $E_1$ و منظور از رویداد $E_2$ ، عدم وقوع رویداد $E_2$ و به همین ترتیب تا آخر باشد . به دلیل اینکه برای یک رویداد خاص، دو حالت بیشتر نداریم (وقوع یا عدم وقوع )، روابط زیر همواره به قرار است:

$$P(E_i)+P(\overline{E}_i)=1$$
$$P(\overline{E}_i)=1-P(E_i).$$

در مورد این رویدادها یا حداقل یکی از $E_i$ ها اتفاق می‌افتد یا هیچکدام رخ نخواهند داد.

بنابراین :

(احتمال اینکه هیچکدام از $E_i$ ها رخ ندهد)-۱ = (احتمال اینکه حداقل یکی از $E_i$ ها رخ دهد)

(احتمال اینکه حداقل یکی از $E_i$ ها رخ دهد) = $1-P(\overline{E}_1 \text{ and } \overline{E}_2 \ldots \text{ and } \overline{E}_n)$

چون $E_i$ ها مستقل هستند ، $E_i$ ها نیز مستقل خواهند بود و در نتیجه :

$P(E\square_1 \text{ and } E\square_2 \ldots \text{ and } E\square_n) = P(E\square_1).P(E\square_2)\ldots P(E\square_n)$

از طرفی $P(E\square_i)=1-P(E\square_i)$ است ، بنابراین :

$$P(E_1 \text{ or } E_2 \text{ or } E_3 \text{ or} \ldots \text{or } E_n) = 1 - \{[1 - P(E_1)]\,[1 - P(E_2)]\,[1 - P(E_3)]\ldots[1 - P(E_n)]\}$$

در ساده‌ترین حالت وقتی احتمال وقوع تمامی رویدادها با هم برابر باشد ، یعنی :

$$P(E_I) = P(E_2) = \ldots = P(E_n) = p$$

معادله بالا به شکل زیر در می‌آید:

$$P(E_1 \text{ or } E_2 \text{ or } E_3 \text{ or} \ldots \text{or } E_n) = 1 - (1- p)^n$$

رابطه فوق کاربردهای زیادی در تحلیل درخت خطا دارد.

برای مثال سیستمی را در نظر بگیرید که توقف سیستم تنها وقتی اتفاق بیفتد که یکی از رویدادهای مستقل $E_1$ ، $E_2$ ، ... یا $E_n$ (حالت های شکست سیستم) ، رخ دهد. در این صورت احتمال شکست سیستم توسط معادله فوق الذکر قابل حصول است. در مورد درخت خطا این حالت‌های شکست مجموعه برش‌های حداقل نامیده شده و اگر مستقل باشند (یعنی هیچکدام از برش‌ها شکست قطعه مشترک نداشته باشند)، در این صورت استفاده از معادله فوق مجاز خواهد بود.

## قضیه بیز Bayes' Theorm

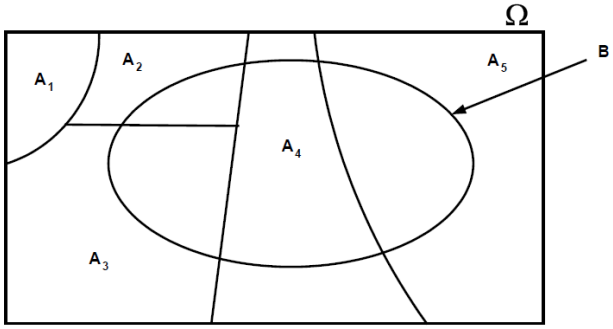
فرمولی که برای اولین بار توسط توماس بیز مطرح گردید، نقش قابل توجه‌ای در ساختار نظریه احتمال داشت. برای تشریح این قضیه، توجه شما را به تصویر (ب- ۷) جلب

مـی‌کنـیم. در ایـن تصـویر Ω مجموعـه مرجـع اسـت کـه شـامل ۵ زیـر مجموعـه $A_1$ ، $A_2$ ، $A_3$ ، $A_4$ و $A_5$ ، می‌باشد.این زیرمجموعه ها دارای ویژگی زیر هستند:

$$A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5 = \bigcup_{i=1}^{i=5} A_i = \Omega$$

$$A_i \cap A_j = \phi \text{ for } i \neq j.$$

مجموعه‌هایی که دارای این ویژگی‌ها باشند (اجتماع آنها برابر با مجموعه مرجع بـوده و دو به دو اشتراکی نداشته باشند) یک افـزار[1] از مجموعـه مرجـع نامیـده مـی‌شـوند. درتصـویر (ب-۷) ، زیرمجموعه B نیز دیده می‌شود.




**تصویر ب ۷ : افزار نمودن مجموعه مرجع**

خواننده به راحتی با استفاده از نمودار ون می‌تواند درستی رابطه زیر را بررسی کند.

$$(B \cap A_1) \cup (B \cap A_2) \cup (B \cap A_3) \cup (B \cap A_4) \cup (B \cap) A_5) = B$$

معادله بالا را حتی می‌توان با علائم ریاضی خلاصه تر کرد:

$$B = \bigcup_{i=1}^{i=5} B \cap A_i$$

حالا با توجه به معادله احتمالات شرطی بخش قبل ، یعنی :

$$P(A \cap B) = P(A|B)\, P(B) = P(B|A)\, P(A)$$

[1] Partition

برای هر ناحیه مشترک رویداد $A_k$ با رویداد B می توان نوشت :

$$P(A_k \cap B) = P(A_k|B)\, P(B) = P(B|A_k)\, P(A_k)$$

و یا :

$$P(A_k|B) = \frac{P(A_k \cap B)}{P(B)} = \frac{P(B|A_k)P(A_k)}{P(B)}$$

حالا می‌توان با استفاده از معادلات بالا ، P(B) را به شکل دیگری نوشت :

$$P(B) = P\left\{\bigcup_{i=1}^{i=5} B \cap A_i\right\}$$

$$= \sum_{i=1}^{i=5} P(B \cap A_i) \;=\; \sum_{i=1}^{i=5} P(B|A_i)\, P(A_i)$$

البته نوشتن احتمال جمع رویداد ها بصورت جمع احتمالات آنها به این دلیل است که طبق تصویر ب-۷ ، رویدادها مانع الجمع هستند . با جایگزین کردن مقدار بدست آمده برای P(B) ، داریم :

$$P(A_k|B) = \frac{P(B|A_k)\, P(A_k)}{\sum_i P(B|A_i)\, P(A_i)}$$

این همان قضیه بیزاست. تعبیر این معادله را با مثالی توضیح می‌دهیم :

فرض کنید رویداد B مشاهده شده و بتوان فهرستی از دلایل مانع الجمع وقوع رویداد B را تهیه کرد (مانند رویدادهای $A_i$ با تغییرات ۱ تا n برای i ) . حال بعد از مشاهده رویداد B، ممکن است به دنبال این باشیم که سهم یکی از علت ها (مانند $A_K$ ) را در وقوع رویداد B بیابیم.این خواسته ما، با استفاده از معادله بیز قابل حصول است. روش بیز جزء گرا است یعنی در مورد یک رویداد سیستمی به دنبال مقدار احتمال عوامل ایجاد کننده آن می باشد . این

روش در مقابل روش‌های کل گرا است که رفتار سیستم را در صورت بـروز برخـی کارکردهـای اشتباه اجزاء آن، بررسی می‌کند. برای توضیح بیشتر به مثال زیر توجه کنید.

فرض کنید ۳ کارتن داریم که به ترتیب دارای برچسب I ، II و III ، باشـند .کـارتن هـا از نظـر شکل ظاهری و اندازه ، یکسان هستند و محتویات آنها تعداد متفاوتی پمپ از کارخانه های X ، Y و Z باشد (تصویر ۸ را ببینید) . فرض کنید یک آزمون تصادفی به شکل زیر انجام دهیم : ابتدا یکی از کارتن ها بصورت تصادفی انتخاب شود ، سپس ۲ پمپ از کارتن انتخابی ، خارج و مشخص شود پمپ ها از کارخانه Z بوده اند . (این رویداد آخری همان رویداد B اسـت کـه در فرمول بیز آمده است ) . علل $A_i$ برای این مثال عبارتند از :

$A_1$ = انتخاب کارتن I

$A_2$ = انتخاب کارتن II

$A_3$ = انتخاب کارتن III

گفتیم که پمپ ها از کارخانه Z بوده اند ، حال احتمال اینکه کـارتن I در ابتـدا انتخـاب شـده باشد ، را با استفاده از قضیه بیز محاسبه می کنیم :

$$P(A_1|B) = \frac{P(B|A_1)P(A_1)}{P(B|A_1)P(A_1) + P(B|A_2)P(A_2) + P(B|A_3)P(A_3)}$$

طبیعی است که :

$$P(A_1) = P(A_2) = P(A_3) = \frac{1}{3}$$

(فراموش نکنیم که کارتن ها هم شکل و هم اندازه اند) . از طرفی با توجه به تصویر ب-۸ داریم :

$$P(B|A_1)=\left(\frac{2}{9}\right)\left(\frac{1}{8}\right)=\frac{1}{36}$$
$$P(B|A_2)=\left(\frac{3}{6}\right)\left(\frac{2}{5}\right)=\frac{1}{5}$$
$$P(B|A_3)=\left(\frac{4}{9}\right)\left(\frac{3}{8}\right)=\frac{1}{6}.$$

بنابراین :

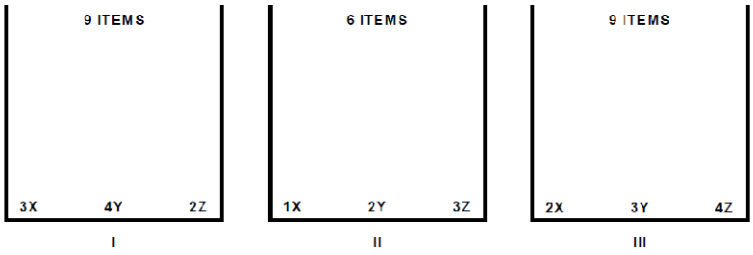
$$P(A_1|B)=\frac{\left(\frac{1}{36}\right)\left(\frac{1}{3}\right)}{\left(\frac{1}{36}\right)\left(\frac{1}{3}\right)+\left(\frac{1}{5}\right)\left(\frac{1}{3}\right)+\left(\frac{1}{6}\right)\left(\frac{1}{3}\right)}=\frac{5}{71}$$

و به همین طریق :

$$P(A_2|B)=\frac{36}{71}$$
$$P(A_3|B)=\frac{30}{71}$$

بنابراین اگر رویداد B مشاهده شود ، احتمال اینکه در ابتدا کارتن II انتخاب شده باشد ، ۵۰ درصد است .

**تصویر ب ۸ : کاربرد قضیه بیز با یک مثال**



## ضمیمه ج) تحلیل احتمالی و آماری

در این ضمیمه مفاهیم پایه احتمال و آمار مرتبط با درخت خطا، ارائه خواهد شد که عمدتاً مربوط به فصل ۷ کتاب است. همچنین به نظریه توزیع احتمال خواهیم پرداخت که شامل توابع توزیع تجمعی[۱] و توابع چگالی[۲] می‌باشد.از طرفی در مورد پارامترهای توزیع، نظیر مد[۳]، میانه[۴] ومیانگین[۵] بحث خواهد شد.

در ادامه توابع نرخ شکست[۶] که گاهی توابع مخاطره[۷] نامیده می‌شوند، تعریف و مثالهایی از توابع توزیع آنها ارائه می‌شود. همچنین در مورد توزیع خاص نمایی با نرخ شکست ثابت توضیح داده و ضمیمه را با بحثی درباره مفاهیم تحلیل بیزی که روش آماری اصولی متداول در کمی سازی احتمالات رویدادهاست، به پایان می‌رسانیم.

### ج-۱) تابع توزیع تجمعی

از نماد X برای نشان دادن نتایج ممکن از یک تجربه تصادفی، استفاده می‌شود و آن را متغیر تصادفی[۸] می‌نامند. یک متغیر تصادفی یا مقادیر گسسته دارد (مانند تعداد موارد عیب یک دستگاه) یا پیوسته (مثلاً قد یا وزن افراد).

[1] Cumulative distribution functions
[2] Density functions
[3] Mode
[4] Median
[5] Mean
[6] Failure rate functions
[7] Hazard functions
[8] Random variable

در ادامه بحث، از حرف کوچک x به عنوان مقدار متناظر متغیر تصادفی X ، استفاده خواهد شد. فرمول‌هایی که از این پس خواهد آمد مربوط به حالت پیوسته است و در صورت لزوم تفاوت فرمولها با حالت گسسته ارائه خواهد شد. عموماً برای تبدیل از حالت پیوسته به گسسته بایستی علامت انتگرال را با علامت سیگمای جمع تعویض کرد. تابع توزیع تجمعی F(x) به عنوان احتمال اینکه متغییر تصادفی X ، مقداری کمتر یا مساوی مقدار خاص x داشته باشد، تعریف می‌شود:

$$F(x) = P\,[\mathbf{X} \le x]$$

طبق معادله بالا، F(x) یک احتمال بوده و مقداری بین صفر و یک دارد:

$$0 \le F(x) \le 1$$

و مقادیر آن در کران بالا و پایین عبارت است از:

$$F(-\infty) = 0$$

$$F(+\infty) = 1$$

اگر x حد بالا و پایین مانند $x_l < \mathbf{X} < x_u$ داشته باشد، داریم:

$$F(x_u) = 1 \qquad \text{و} \qquad F(x_l) = 0$$

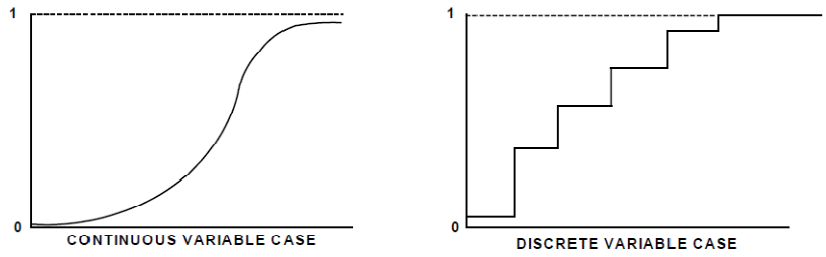
یکی از ویژگیهای مهم تابع توزیع این است که با افزایش x، کاهش نمی‌یابد. یعنی F(x) تابعی غیرنزولی است . تعبیر ریاضی این مطلب به شکل زیر نوشته می شود :

اگر $x_2 > x_1$ باشد ، آنگاه : $F(x_2) \ge F(x_1)$ خواهد بود .

ویژگی مهم دیگر F(x) عبارت است از:

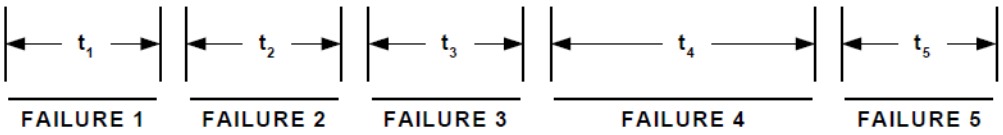
$$P[x_1 \le X \le x_2] = F(x_2) - F(x_1)$$

توزیع تجمعی دو جمله‌ای[1] ، $B(x; n, p)$ ، نمونه‌ای خاص از تابع $F(x)$ می‌باشد. در تصـویر (ج-۱) نمونه‌ای از توابع توزیع در حالت پیوسته وگسسته نمایش داده شده است.




**تصویر ج ۱ ) تابع F(X) در حالت پیوسته(منحنی سمت چپ) و گسسته(منحنی سمت راست)**

به عنوان مثالی از متغیر تصادفی و توزیع تجمعی آن، آزمونی را در نظر بگیرید کـه مـوارد زمانی خرابی یک قطعه منفرد، ثبت می‌شود و هرگاه قطعه خراب می‌شـود، تعمیـر شـده و زمان صفر می‌گردد و دوباره زمان خرابی بعدی ثبت می‌شود.(طرح زیررا ببینید)




فرض کنید انجام تعمیر (بازسازی) وضعیت قطعه را بهتر نکند (یعنی احتمال تعمیر مجـدد قطعه هیچگاه صفر نباشد). متغیر تصادفی T را، زمان خرابی در فاصله بازسازی‌هـا، تعریـف می‌کنیم و مقدار خاص آن را با $t_i$ نشان می‌دهیم. در این صورت تابع توزیع تجمعی $F(t)$ ، احتمال اینکه زمان رسیدن به شکست کوچکتر یا مساوی t باشد را نمایش می‌دهد.

[1] Binomial cumulative distribution

### ج-۲) تابع چگالی احتمال

برای یک متغیر تصادفی پیوسته، تابع چگالی احتمال یا pdf ، با مشتق‌گیری از F(X) به دست می‌آید. که رابطه معادل آن عبارت است از:

$$f(x) = \frac{d}{dx}F(x)$$

البته رابطه بالا را می توان بدین شکل هم نوشت :

$$F(x) = \int_{-\infty}^{x} f(y)dy$$

و چون f(x) به عنوان شیب تابعی غیر نزولی تعریف می‌شود، مقدار آن همواره مثبت است :

$$f(x) \geq 0$$

اگر از f(x) در کل بازه مقادیرش، انتگرال‌گیری شود، حاصل عدد یک است :

$$\int_{-\infty}^{\infty} f(x)dx = 1$$

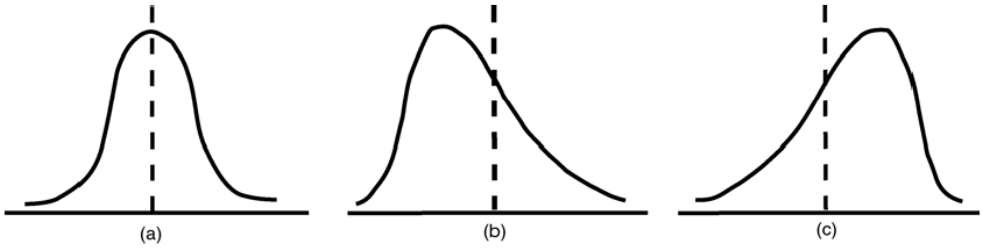
رابطه اخیر، نشان می‌دهد که تابع چگالی نیز از جنس احتمال است. اما رابطه زیر ، مفهوم بنیادی f(x) را بیان می کند :

$$f(x)dx = P[x < \mathbf{X} < x + dx]$$

که می‌توان آن را به شکل کاربردی‌تری، نیز نوشت:

$$P[x_1 \leq \mathbf{X} \leq x_2] = \int_{x_1}^{x_2} f(x)dx$$

نمونه هایی از تابع f(x) در تصویر (ج-۲) آمده است:




**تصویر ج ۲ : شکل های مختلف تابع f(x)**

در این تصویر : شکل (a ) یک توزیع متقارن (b) یک توزیع با چولگی راست و (c ) یک توزیع با چولگی چپ ، می باشد . و در تمامی موارد افزایش x از چپ به راست است. در مورد متغیر تصادفی پیوسته، احتمالات با انتگرال معین در بازه‌ای از x بیان می‌شوند چرا که احتمال مربوط به یک مقدار خاص x، همواره صفراست. همچنین f(x)dx ، احتمال قرار گرفتن متغیر تصادفی X در فاصله x تا x + dx ، می باشد . در مورد متغیرهای گسسته ، علامت انتگرال با علامت سیگما (∑) تعویض می شود و تجمیع روی مقادیر گسسته x در هر بازه دلخواه صورت می پذیرد .بخصوص اگر مقادیر مشاهده شده زیاد باشد ، f(x)dx را می توان به شکل زیر تخمین زد :

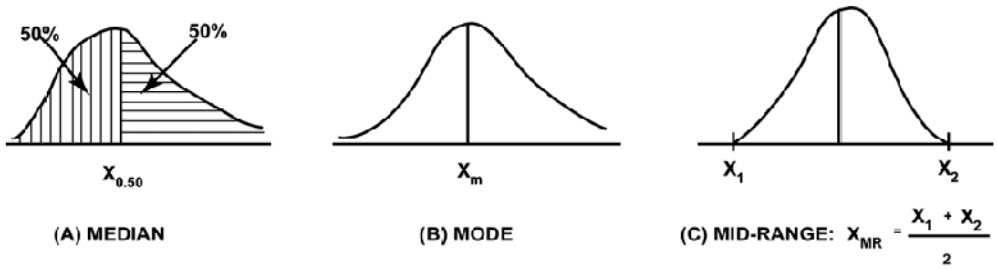
$$f(x)\Delta x = \frac{\Delta n_i}{n}$$

که در آن n ، تعداد کل آزمون ها و $\Delta n_i$ ، تعداد آزمون هایی است که در آن ، X در فاصله x تا x + dx قرار می گیرد .

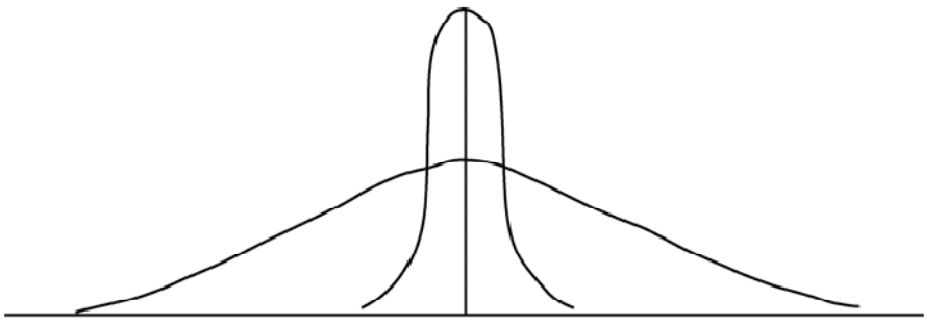
## ج-۳) پارامترهای توزیع وگشتاورها

خواص توابع چگالی احتمال با پارامترهای توزیع[1] آنها شناخته می‌شود. پارامترها دو دسته هستند: مرکزی و پراکندگی

پارامترهای مرکزی (نظیر میانگین، میانه، و مد)، وضعیت قرارگیری توزیع احتمال را نسبت به محور افقی مشخص می‌کنند.پارامترهای پراکندگی (مانند واریانس و انحراف معیار) پراکندگی توزیع را نسبت به مرکز، ارائه می‌دهند تصویر (ج-۳) پارامترهای مرکزی و تصویر (ج-۴) توزیع متقارن ولی با پارامترهای پراکندگی متفاوت را نشان می‌دهند.




**تصویر ج ۳ ) میانه ، مد و MID-RANGE**



**تصویر ج ۴ ) دو توزیع متقارن با پارامترهای پراکندگی متفاوت**

[1] *Distribution parameters*

نحوه محاسبهٔ پارامترهای توزیع، عموماً از طریق گشتاورها است که به تعریف آن‌ها می‌پردازیم.

**گشتاور حول مبدأ**[1]

گشتاور اول نسبت به مبدأ، اینگونه تعریف می‌شود.

$$\mu_1' = \int_{-\infty}^{\infty} x\ f(x)dx$$

امید ریاضی x که با نماد $E[\mathbf{X}]$ نشان داده می‌شود (نماد دیگر آن $\mu$ است) همان گشتاور اول نسبت به مبدأ می‌باشد. یعنی : $E[\mathbf{X}] = \mu_1'$

گشتاور دوم نسبت به مبدأ، عبارت است از:

$$\mu_2' = \int_{-\infty}^{\infty} x^2 f(x)dx$$

که همان امید ریاضی $\mathbf{X^2}$ یا $E[\mathbf{X}^2]$ می‌باشد. و در حالت کلی گشتاور n ام حول مبدأ عبارت است از:

$$\mu_n' = \int_{-\infty}^{\infty} x^n f(x)dx$$

اگر $Y = g(X)$ ، تابعی از X باشد و pdf متغیر تصادفی X را با $f(x)$ نمایش دهیم ، امید ریاضی Y ، عبارت است از :

$$E[Y] = E[g(X)] = \int_{-\infty}^{\infty} g(x)f(x)dx$$

[1] Moments About the Origin

**گشتاور حول میانگین**[1]

گشتاور اول حول میانگین ، بدین شکل تعریف می‌شود:

$$\mu_1 = \int_{-\infty}^{\infty} (x - \mu) f(x) dx$$

و برای گشتاور دوم حول میانگین (واریانس[2] توزیع یا $\sigma^2$) داریم:

$$\mu_2 = \int_{-\infty}^{\infty} (x - \mu)^2 f(x) dx$$

مانند بخش قبل، گشتاور n ام حول میانگین می‌شود:

$$\mu_n = \int_{-\infty}^{\infty} (x - \mu)^n f(x) dx$$

رابطه جالبی بین $\mu_2$ و $\mu'_2$ برقرار است:

$$\mu_2 = \mu'_2 - (\mu'_1)^2$$

که راه‌حل ساده‌تری برای محاسبه واریانس توزیع است و به شکل زیر اثبات می شود :

$$\mu_2 = \int_{-\infty}^{\infty} (x-\mu)^2 f(x) dx$$
$$= \int_{-\infty}^{\infty} x^2 f(x) dx - 2\mu \int_{-\infty}^{\infty} x f(x) dx + \mu^2 \int_{-\infty}^{\infty} f(x) dx$$
$$= \mu'_2 - 2\mu^2 + \mu^2 = \mu'_2 - \mu^2 = \mu'_2 - (\mu'_1)^2.$$

در مورد متغییرهای گسسته، گشتاور اول حول مبدأ عبارت است از:

$$\mu = \mu'_1 = \sum_{i=1}^{n} x_i \, p(x_i)$$

که در آن $p(x_i)$ احتمال مرتبط با مقدار $x_i$ می‌باشد. همچنین فرمول محاسبه میانگین برای متغیرهای گسسته می‌شود:

$$\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i$$

[1] Moments About the Mean
[2] Variance

برای محاسبه واریانس نیز از فرمول زیر استفاده می‌کنیم:

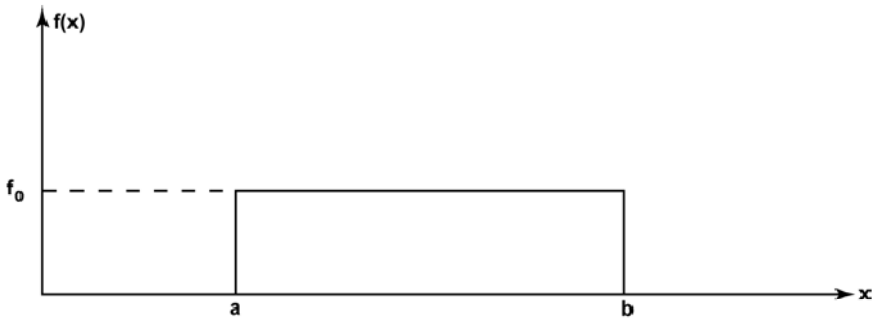
$$\mu^2 = \sum_{i=1}^{n} (x_i - \mu)^2 \, p(x_i)$$

در صورتیکه n نمونه از یک جامعه آماری با احتمال انتخاب یکسان $\frac{1}{n}$ ، مدنظر باشد. فرمول واریانس با تلفیق معادلات بالا تبدیل به واریانس نمونه می‌شود:

$$s^2 = \frac{1}{n} \sum_{i=1}^{n} (x_i - \bar{x})^2$$

حال برای یک توزیع کاربردی محاسبات میانگین و واریانس را انجام می‌دهیم فرض کنید متغیر تصادفی x دارای توزیع یکنواخت در فاصله a تا b باشد (تصویر ج-۵) . با توجه به اینکه سطح زیر منحنی pdf ، همواره برابر عدد یک می شود ، میتوانیم مقدار ثابت $f_0$ را محاسبه کنیم :

مساحت زیر منحنی = $f_0(b-a) = 1$ در نتیجه : $f_0 = \frac{1}{(b-a)}$




**تصویر ج ۵ : توزیع مستطیلی**

نحوه محاسبه میانگین و واریانس توزیع به شرح زیر است:

$$\mu = \mu_1' = E[X] = \int_a^b x \frac{1}{b-a} \, dx$$

$$= \frac{1}{b-a} \left[ \frac{x^2}{2} \right]_a^b = \frac{b^2 - a^2}{2(b-a)} = \frac{(b-a)(b+a)}{2(b-a)} = \frac{b+a}{2}$$

$$\text{Var} = \alpha^2 = \mu_2 = \mu_2' - (\mu_1')^2 = \int_a^b x^2 \left(\frac{1}{b-a}\right) dx - \left(\frac{b+a}{2}\right)^2$$

$$= \left(\frac{1}{b-a}\right)\left[\frac{x^3}{3}\right]_a^b - \left(\frac{b+a}{2}\right)^2$$

$$= \left(\frac{1}{b-a}\right)\left(\frac{b^3-a^3}{3}\right) - \left(\frac{b+a}{2}\right)^2$$

$$= \left(\frac{1}{b-a}\right)\left[\frac{(b-a)(b^2+ab+a^2)}{3}\right] - \left(\frac{b+a}{2}\right)^2$$

$$= \frac{b^2-2ab+a^2}{12} = \frac{(b-a)^2}{12}.$$

### ج-۴) نرخ شکست یا تابع مخاطره

در بخش قبل توابع توزیع تجمعی و چگالی احتمال اینگونه تعریف شدند:

F (t) = احتمال شکست قبل از زمان t

f (t)dt = احتمال شکست در فاصله زمانی( t تا t+dt )

احتمال شرطی، λ(t) ، که تابع نرخ شکست یا تابع مخاطره[1] نامیده می‌شود . اینگونه تعریف می شود :

λ (t) = [احتمال شکست در فاصله زمانی( t تا t+dt ) به شرط آنکه تا زمان t شکستی اتفاق نیفتاده باشد ]

برای هر توزیع عام، ارتباط مهمی بین این ۳ تابع وجود دارد:

$$\lambda(t) = \frac{f(t)}{1-F(t)}$$

صحت رابطه فوق به راحتی قابل بررسی است . فرض کنید متغیر تصادفی T زمان بین شکست‌ها باشد. از تعریف تابع نرخ شکست داریم :

[1] Hazard function

$$\lambda(t)dt = P\,[t<\mathbf{T}<t+dt \mid t<\mathbf{T}]$$

به جای رویداد شکست در زمان ($t<\mathbf{T}<t+dt$) از حرف A و به جای رویداد شکست در زمان ($t < \mathbf{T}$) از حرف B استفاده می‌کنیم حال با توجه به فرمول کلی احتمال شرطی داریم:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

بنابراین :

$$\lambda(t)dt = \frac{P[(t < \mathbf{T} < t + dt) \cap (t < \mathbf{T})]}{P(t < \mathbf{T})}$$

حال با توجه به تعاریف تابع توزیع تجمعی $F(x)$ و چگالی احتمال $f(x)$ ، داریم :

$$\lambda(t)dt = \frac{P[t < \mathbf{T} < t + dt]}{P(t < \mathbf{T})} = \frac{P[A]}{P[B]} = \frac{f(t)dt}{1 - F(t)}$$

و بدین شکل رابطه

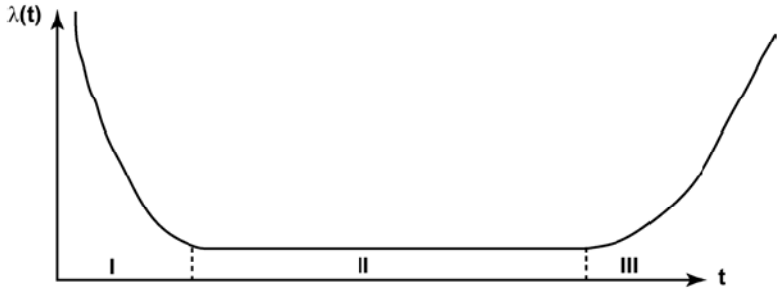
$$\lambda(t) - \frac{f(t)}{1 - F(t)}$$

اثبات می شود . اگر $\lambda(t)$ را برحسب زمان کلی سیستم (طول عمر) رسم کنیم، اغلب، منحنی تصویر (ج-۶) را به دست می‌آوریم که به bathtub curve مشهور است. این منحنی را می‌توان به ۳ ناحیه I, II, III تقسیم کرد. در ناحیه I که اصطلاحاً ناحیه مرگ و میر اولیه[1] نامیده می‌شود ( در این ناحیه ، سیستم یا دستگاه شروع به کار می کند یا اصطلاحاً راه اندازی می شود )، به دست آوردن تابع توزیع، گاهی پیچیده است. توزیع مناسب با این بخش از منحنی، بستگی زیادی به ماهیت طبیعی سیستم دارد. کارخانجات سازنده ، مکرراً محصولات خود را به

[1] Infant mortality

منظور کاهش نرخ شکست در ناحیه فوق مورد تست های اولیه قرار می دهند . در ناحیه II ظاهراً نرخ شکست ثابتی داریم به همین دلیل از تابع توزیع نمایی[1] برای بیان نرخ شکست استفاده می‌شود منظور از نرخ شکست ثابت دراین بازه زمانی این است که شانس خراب شدن دستگاه دراین فاصله، یکسان است.

ناحیه III به زمان فرسودگی و پایان عمر دستگاه مربوط می‌شود. که برای مدل نمودن نرخ شکست دستگاه در این دروه زمانی، می‌توان از توزیع نرمال یا **وی بال**[2] استفاده کرد. در مورد یک سیستم واقعی، منحنی $\lambda(t)$ برحسب زمان ممکن است تفاوت زیادی با منحنی رسم شده در تصویر (ج-۶) داشته باشد. برای مثال ممکن است ناحیه نمایی II را اصلاً نداشته باشیم یا ناحیه شروع به کار دستگاه (ناحیه I) بسیار اندک باشد.




**تصویر ج ۶ : طرحی از نرخ شکست برای یک سیستم عمومی**

[1] Exponential distribution
[2] Weibull Distribution

حال با توجه به معادله $\lambda(t)$ بر حسب $F(x)$ و $f(x)$ ، سعی می‌کنیم آن را بر حسب $\lambda(t)$ حل نماییم. بدین منظور با توجه به اینکه تابع چگالی احتمال در واقع مشتق تابع توزیع احتمال است داریم:

$$\lambda(t)dt = -\frac{[-F'(t)dt]}{1-F(t)}$$

که در آن :

$$F'(t) = -\frac{dF(t)}{dt}$$

با انتگرال گیری از دو طرف این معادله داریم:

$$-\int_0^t \lambda(x)dx = \ln[1-F(t)]$$

که معادل است با :

$$1-F(t) = \exp\left[-\int_0^t \lambda(x)dx\right]$$

و بنابراین :

$$F(t) = 1-\exp\left[-\int_0^t \lambda(x)dx\right]$$

و با مشتق گیری از رابطه فوق بر حسب زمان داریم :

$$f(t) = \lambda(t)\exp\left[-\int_0^t \lambda(x)dx\right] \qquad \text{(ج -۲۴)}$$

اگر $\lambda(t) = \lambda$ مقدار ثابت داشته باشد معادلات بالا به شکل زیر ساده می‌شوند:

$$F(t) = 1 - e^{-\lambda t} \text{ and } f(t) = \lambda e^{-\lambda t}$$

که همان توزیع نمایی است. بنابراین در توزیع نمایی نرخ شکست عددی ثابت و مستقل از زمان است . ( به همین دلیل است که معمولاً توزیع نمایی را توزیع بدون حافظه می نامند ) اگر نرخ شکست قطعه‌ای را با توزیع نمایی مدل کنیم بدین معنی است که قطعه در ناحیه ثابت و پایدار منحنی نرخ شکست قرار دارد. به خاطر ثبات نرخ شکست در این فاصله زمانی، توزیع نمایی اغلب «توزیع شکست تصادفی» نامیده می‌شود . بدین معنی که احتمال شکست دستگاه در آینده، ارتباطی به کارکرد موفقیت آمیز آن در گذشته ندارد.

با استفاده از معادلات نرخ شکست و تابع توزیع شکست ، می توان موارد بسیاری از مدلهای نرخ شکست را آنالیز کرد . برای مثال اگر فرض کنیم $\lambda(t) = kt$ باشد (نرخ شکست افزاینده خطی)، داریم.

$$R(t) = 1 - F(t) = \exp(-kt^2/2)$$

که در آن $R(t)$ تابع **قابلیت اطمینان**[1] سیستم است. معادله بالا مربوط به توزیع مشهور رایلی[2] است. توزیع مهم دیگری از زمان تا شکست[3]، توزیع وی بال[4]، با قرار دادن $\lambda(t) = Kt^m \ (m > -1)$ در معادله (ج-۲۴) به دست می‌آید:

$$f(t) = kt^m \exp\left(-\frac{kt^{m+1}}{m+1}\right)$$

و همچنین

$$R(t) = 1 - F(t) = \exp\left(-\frac{kt^{m+1}}{m+1}\right)$$

[1] Reliability
[2] Rayleigh distribution
[3] times-to-failure
[4] Weibull distribution

توزیع «وی بال» یک توزیع دو پارامتری است که در آن K به عنوان پـارامتر مقیـاس[1] و m بـه عنوان پارامتر شکل[2] شناخته می‌شود. با نزدیک شدن m به عدد ۲، به توزیع نرمال مـی‌رسـیم. اگر m=0 باشد ، توزیع وی بال تبدیل به توزیع نمایی منفی می شود . برای مدل کردن زمـان راه‌اندازی (ناحیه I) از توزیع وی بال با فرض( 1- < m> 0 ) اسـتفاده مـی‌کنـیم و بـا افـزایش بیشتر m، ناحیه فرسودگی (ناحیه III) مدل می‌شود. بنابراین با تغیر مقدار m، توزیـع وی بـال نواحی مختلف منحنی نرخ شکست را مدل می‌کند.

### (ج-۵) تحلیل بیزی (Bayesian)

در تحلیل بیزی، پارامترهای توزیع ثابت نبوده و متغیرهایی تصـادفی هسـتند. مـثلاً در توزیـع نمایی با فرمول :

$$f(x) = \frac{1}{\theta} e^{-x/\theta}$$

می‌توان برای زمان میانگین تا شکست ($\theta$) نیز یک تابع توزیع احتمال، در نظر گرفـت. حـال اگر توزیع نمایی را بر حسب نرخ شکست بنویسیم:

$$\lambda = 1/\theta,\ f(x) = \lambda e^{-\lambda x}$$

اگر $\theta$ یک متغیر تصادفی باشد، $\lambda$ نیز یک متغیر تصادفی است. فرض کنید تابع چگالی احتمال $\lambda$ با $p(\lambda)$ نشان داده شود. در این صورت $p(\lambda)$ توزیع مقدم[3] نامیده می شود ، چرا که اطلاعات اولیه ما از $\lambda$ را قبل از نمونه‌گیری نشان می‌دهد. حال فرض کنید نمونه‌ای از زمان‌های شکست

[1] Scale parameter
[2] Shape parameter
[3] Prior distribution

یک قطعه مانند $(t_1,t_2,\ldots,t_n)$ جمع آوری کرده باشیم. با داشتن این اطلاعات جدید و با داشتن تابع توزیع مقدم $p(\lambda)$ می‌توانیم، تابع توزیع تالی[1] را به دست آوریم یا به عبارتی اطلاعات خود را در مورد نرخ شکست، به روز کنیم.

توزیع تالی که چگالی احتمال آن با $p(\lambda|D)$ نشان داده می‌شود به راحتی با بکارگیری قضیه بیز قابل حصول است: (D همان نمونه داده یا $(t_1,t_2,\ldots,t_n)$ است)

$$P(B|A) = \frac{P(A|B)\,P(B)}{\sum P(A|B)P(B)}$$

با جایگزینی A با نمونه گرفته شده D و با این فرض که B رویداد قرارگیری نرخ شکست بین $\lambda$ و $\lambda + d\lambda$ باشد ، داریم :

$$p(\lambda|D) = \frac{\exp\left[-\sum_{i=1}^{n}\lambda t_i\right]\lambda^n p(\lambda)}{\int \exp\left[-\sum_{i=1}^{n}\lambda t_i\right]\lambda^n p(\lambda)\,d\lambda}$$

و با تعویض علامت انتگرال گیری با علامت سگیما در مخرج (به این علت که انتگرال گیری بر روی $\lambda$ بوده، در صورتیکه سیگما برروی زمان انجام می‌شود) ، به معادله زیر می‌رسیم:

$$p(\lambda\,|\,D) = K\exp\left[-\sum_{i=1}^{n}\lambda t_i\right]\lambda^n p(\lambda)$$

که در آن K ضریب نرمال ساز[2] است. توزیع $p(\lambda|D)$ توزیع تالی بوده و حاوی اطلاعات اولیه ومشاهده شده در مورد نرخ شکست می‌باشد.

[1] Posterior distribution
[2] Normalizing constant

بنابراین نظریه بیز، راهی برای به روز کردن اطلاعات قبلی در مورد نرخ شکست را ارائه می‌دهد. حال اگر نمونه‌گیری دومی انجام شود داده‌های جدیدی مانند $(t_1',t_2',\ldots,t_n')$ تولید می‌کند و می‌توانیم با استفاده از این نظریه، تابع تالی نرخ شکست را با توجه به هردو نمونه مشاهده شده، به شکل زیر بدست آوریم:

$$p(\lambda|D,D') = K\exp\left[-\sum_{i=1}^{n}\lambda t_i\right]\lambda^n p(\lambda|D)$$

انتخاب تابع چگالی احتمال مقدم $p(\lambda|D)$ و تکنیک‌های کار با انواع داده به تفصیل در متون مختلف احتمال آمده است که خواننده می‌تواند برای کسب اطلاعات بیشتر به آن‌ها مراجعه نماید.

با داشتن تابع تالی، اطلاعات باارزش در مورد، تغییرات ممکن و عدم قطعیت[1] در پارامترها به دست می‌آید. همچنین مقادیر نقطه‌ای از قبیل محتمل‌ترین مقدار $\lambda$ یا مقدار میانگین $\lambda$ قابل حصول است. از طرفی مقادیر فاصله‌ای که فاصله اطمینان بیزی[2] نامیده می‌شوند نیز محاسبه می‌شوند. به عنوان مثال ممکن است علاقه‌مند به این باشیم که بدانیم به احتمال ۹۵ درصد احتمال نرخ شکست درچه فاصله‌ای قرار دارد که حل این مسئله به یافتن کران بالا $(\lambda_U)$ و کران پایین $(\lambda_L)$ فاصله اطمینان ۹۵ درصد منتهی شده و با عبارت ریاضی بدین شکل بیان می‌شود:

$$\int_{\lambda_L}^{\lambda_U} p(\lambda|D)d\lambda = 0.95$$

[1] Uncertainty
[2] Bayesian confidence intervals

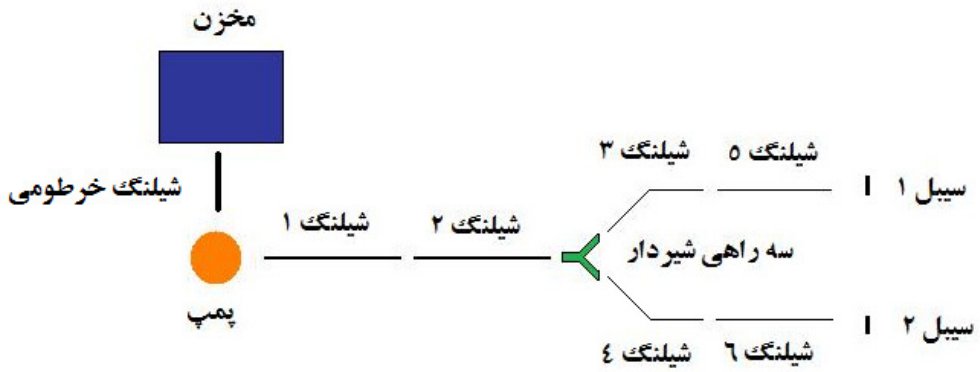
نظریه بیز، هر دو مزیت تجربه مهندسی و دانش عمومی را به همراه داده‌های آماری صـرف، بـا خود دارد.

## ضمیمه د: تحلیل درخت موفقیت یا واکاوی قابلیت اطمینان سیستم

در فصل اول ، شرح مختصری از درخت موفقیت به عنوان مکمل منطقی درخت خطا ، ارائه دادیم . در این ضمیمه قصد داریم در باره قابلیت اطمینان سیستم و ارتباط آن با درخت موفقیت بحث نماییم . اما قبل از آن ، لازم است مفهوم درخت موفقیت را با ذکر یک مثال ، بسط دهیم :

### د-۱ ) مسابقه آبرسانی

یکی از مواد آزمون مسابقات جهانی آتش نشانان ، ماده آبرسانی است که در آن تیم مسابقه دهنده بایستی آب را از یک منبع روباز با اتصال شیلنگ های آب آتش نشانی (Fire Hose) و به کمک یک پمپ قابل حمل به سیبل های هدف برساند . تصویر د-۱ ، نمایی از این مسابقه را نشان می دهد .




**تصویر د-۱ : نمونه ای از تجهیزات مسابقه آبرسانی**

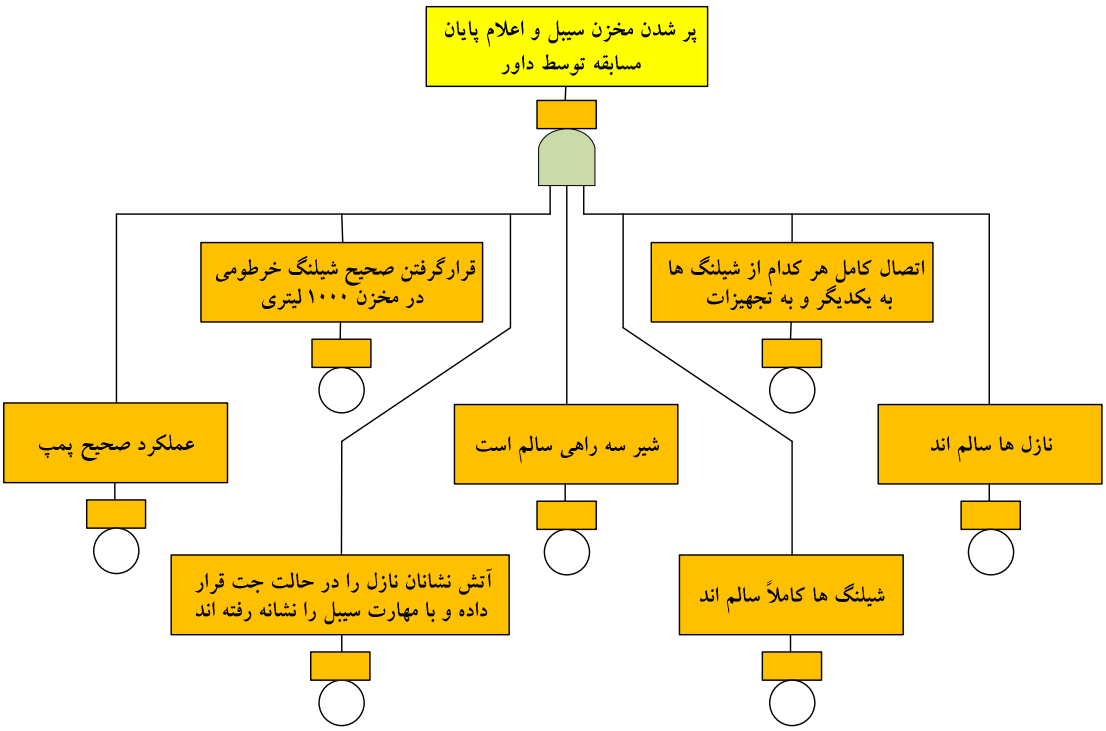
در این مسابقه آتش نشانان باید با استفاده از مهارت خود و سرعت عمل بالا ، شیلنگ خرطومی را از یک طرف داخل مخزن آب کرده و از طرف دیگر به پمپ وصل کنند . سپس شیلنگ های

آب آتش نشانی شماره ۱ و ۲ را که ۲/۵ اینچ هستند ، علاوه بر اتصال به هم ، از یک طـرف بـه پمپ و از طرف دیگر به سه راهی شیردار وصل می کنند . بعد شیلنگ هـای آب آتـش نشـانی ۱/۵ اینچ را به هم متصل کرده ، یک سمت آنها را به سه راهی و سمت دیگـر آنهـا را در محـل تعیین شده (در فاصله ۵ متری از سیبل ها) روی زمین قرار می دهند . در این محل نازل های آب به انتهای شیلنگ ها متصل شده و دو آتش نشان نازل ها را به طرف سیبل هـا نشـانه مـی گیرند و منتظر رسیدن آب می شوند . این انتظار خیلی طولانی نیست چرا که به محض وصـل شدن اتصالات و دریافت علامت ، آتش نشانی که عهده دار پمپ است ، آن را روشن می کند و آب از مخزن و از طریق شیلنگ ها با فشار کافی به نازل ها می رسد و دو آتش نشان نازل هـا را به سمت مرکز سیبل هـا هـدف گرفتـه و نـازل را در حالـت جـت بـاز مـی کننـد . مهـارت آتش نشانان در نشانه روی دقیق و هدر ندادن آب در این مرحله ضروری است . با پر شدن آب در مخزن ۱۰ لیتری که در پشت صفحه فلزی هر سیبل نصب شده است ، چـراغ اعـلان پایـان مسابقه روشن می شود . برای اطمینان ، سر ریزی در بالای مخزن ۱۰ لیتری تعبیـه شـده کـه در صورت عمل نکردن چراغ گردان ، آب را به بیرون هدایت می کند و داوران با بیرون زدن آب ، پایان مسابقه را اعلام می کنند .

به دلیل محدود بودن آب مخزن ، هدایت آب به نحو صحیح و محکـم بسـتن اتصـالات ، نقـش مهمی را در پیروزی تیم ها دارد . بعد از ایـن توضـیحات ، قصـد داریـم درخـت موفقیـت ایـن سیستم را رسم کنیم . اگر آب مخزن ۱۰ لیتری تا حد تعیین شـده پـر نشـود ، تـیم شکسـت کاملی را متحمل می شود . در فصل ۲ طیف موفقیت/شکست سیستم را رسم کردیم . در مورد

مسابقه آبرسانی ، حداقل موفقیت تیم در این است که مخزن ۱۰ لیتری پر شود و داوران پایان مسابقه را اعلام کنند و موفقیت حداکثر تیم این است که رتبه اول را در این آزمون بدست آورد . برای سادگی ما حداقل موفقیت یعنی پر شدن مخزن سیبل و اعلام پایان مسابقه توسط داور را به عنوان رویداد رأس درخت موفقیت در نظر می گیریم . هر کدام از رویدادهای زیر اگر رخ دهد ، این حداقل موفقیت بدست نخواهد آمد :

- ✓ قرار نگرفتن صحیح شیلنگ خرطومی در مخزن ۱۰۰۰ لیتری
- ✓ عدم اتصال کامل هر کدام از شیلنگ ها به یکدیگر و به تجهیزات مسابقه
- ✓ روشن نشدن پمپ
- ✓ باز نشدن شیر سه راهی
- ✓ شکست نازل ها
- ✓ عدم مهارت آتش نشانان در نشانه روی و کار با نازل ( قرار دادن نازل در حالت افشان)
- ✓ پاره شدن هر یک از شیلنگ ها در حین مسابقه




**تصویر د-۲ : درخت موفقیت مسابقه آبرسانی**

البته ممکن است عوامل دیگری نیز در شکست کامل تیم ، نقش داشته باشد که بدلیل احتمال وقوع ناچیز آن در مقابل دیگر عوامل از آنها صرف نظر می کنیم . چون هر یک از رویداد های فوق الذکر به تنهایی منجر به شکست تیم می شود ، برای رسم درخت موفقیت کافی است ، رویدادها را به شکل مثبت بنویسیم و همه را در زیر گیت AND قرار دهیم .(از گیت AND استفاده می کنیم چرا که برای رسیدن به حداقل موفقیت ، وقوع همزمان رویدادهای مثبت ، ضروری است) . درخت موفقیت مسابقه در تصویر د-۲ مشاهده می کنید .

## د-۲ ) تبدیل درخت خطا به درخت موفقیت

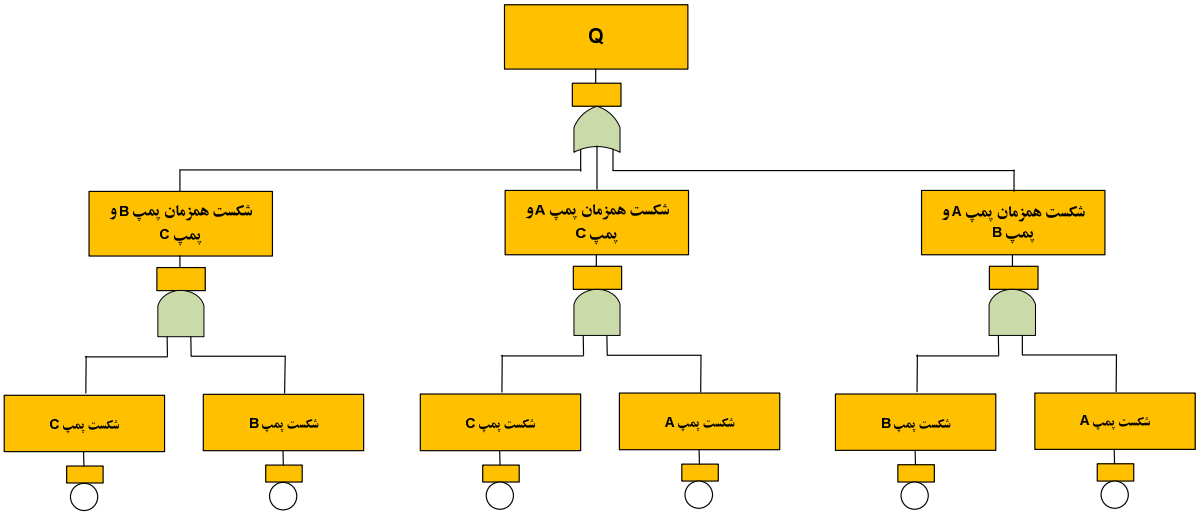
**روش گرافیکی :**

برای تبدیل درخت خطا به درخت موفقیت ، مراحل زیر را باید انجام داد :

۱- بازنویسی رویداد های خطا به شکل موفقیت .

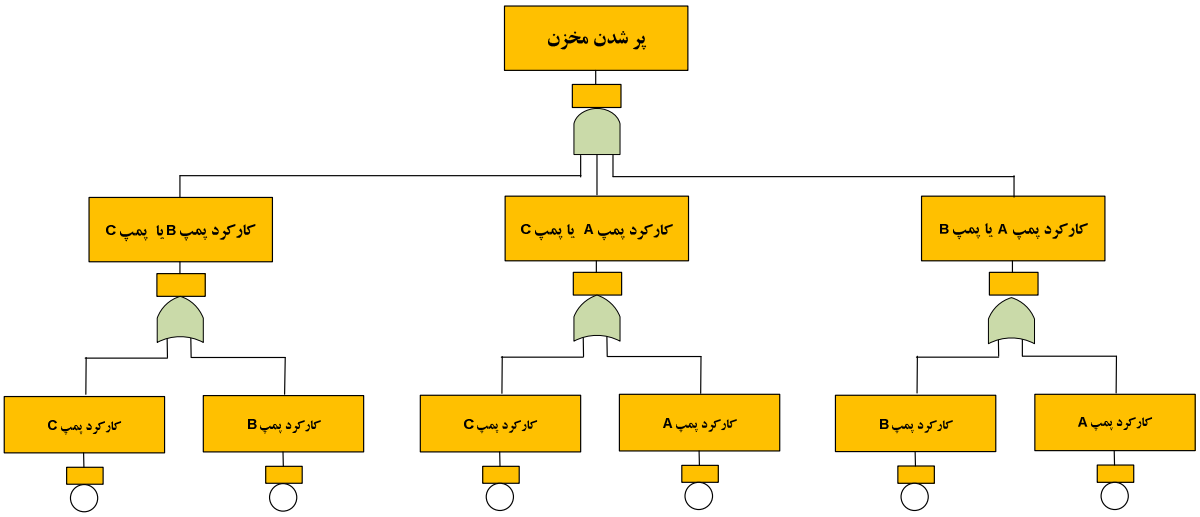
۲- تعویض گیت های AND با گیت های OR و بالعکس .

به عنوان مثال درخت خطای رسم شده در تصویر د-۳ را که از فصل چهارم اقتباس شده و مربوط به پر نشدن یک مخزن بدلیل شکست دو پمپ از سه پمپ می باشد را در نظر بگیرید :




**تصویر د-۳ : درخت خطای مربوط به پر نشدن مخزن**

برای تبدیل این درخت خطا به درخت موفقیت ، ابتدا عبارت های شکست را به موفقیت تبدیل می کنیم . سپس گیت های AND را با OR و تنها گیت OR را با گیت AND ، عوض می کنیم . تصویر د-۴ ، درخت موفقیت پر شدن مخزن را با اعمال تغییرات بالا نمایش می دهد :




**تصویر د-٤** : درخت موفقیت پر شدن مخزن

**روش ریاضی**

از نظر ریاضی و جبر بول ، برای تبدیل معادله ریاضی درخت خطا به درخت موفقیت ، کافی است مراحل زیر را انجام دهیم :

۱- متمم ریاضی تمامی رویداد ها از جمله رویداد رأس را بنویسید .

۲- علائم جمع را به ضرب تبدیل کنید .

۳- علائم ضرب را به جمع تبدیل کنید .

به عنوان مثال در تصویر د-۳ ، اگر حروف A ، B و C ، به ترتیب نشان دهنده رویداد های شکست پمپ A ، B و C باشد . رویداد خروجی Q را می توان برحسب این رویدادها به شکل زیر نوشت :

$$Q=A.B+A.C+B.C$$

که Q ، رویداد رأس درخت خطا است . حال برای نوشتن معـادل جبـری رویـداد رأس درخـت موفقیت ، مراحل فوق الذکر را انجام می دهیم . حاصل معادله زیر است :

$$\overline{Q} = (\overline{A} + \overline{B}).(\overline{A} + \overline{C}).(\overline{B} + \overline{C})$$

که نمایش ریاضی همان درختی است که در تصویر د-۴ رسم کرده ایم .

### د-۳ ) مجموعه مسیرها[1]

همچون درخت خطا ، درخت موفقیت هم عبارت معادلی برای مجموعه برش هـا دارد . دیـدیم که یک مجموعه برش ، ترکیبی از رویدادها است که با وقوع آنها ، رویداد رأس رخ خواهد داد و مجموعه برش های حداقل ، ترکیبی حداقل از این رویدادها است . در مورد درخـت موفقیـت ، مجموعه مسیرها ، ترکیبی از رویدادهای موفقیت آمیز است که با وقوع آنهـا ، رویـداد رأس رخ نخواهد داد و حداقل مجموعه مسیرها[2] ، ترکیبی حداقل از این رویدادهاست . برای مثال معادله بولی درخت موفقیت تصویر د-۴ یعنی :

$$\overline{\mathrm{Q}} = (\overline{A} + \overline{B}).(\overline{A} + \overline{C}).(\overline{B} + \overline{C})$$

را با استفاده از قانون دمورگان ، می توان به شکل ساده تری هم نوشت :

$$\overline{\mathrm{Q}} = [\overline{A}.\overline{A} + \overline{A}.\overline{C} + \overline{B}.\overline{A} + \overline{B}.\overline{C}].(\overline{B} + \overline{C})$$

و بعد از اعمال قوانین جبر بول ، داریم :

$$\overline{\mathrm{Q}} = [\overline{A} + \overline{B}.\overline{C}].(\overline{B} + \overline{C})$$

[1] Path Sets
[2] Minimal Path Sets=(MPSs)

$$\overline{Q} = \overline{A}.\overline{B} + \overline{B}.\overline{C} + \overline{A}.\overline{C}$$

که معادله آخر ، نمایش رویداد رأس درخت موفقیت بر حسب مجموعه مسیرهای حداقل آن است .

## د-۴) قابلیت اطمینان[1]

قابلیت اطمینان از موضوعات مهم مهندسی صنایع است و کاربرد وسیعی در بحث تعمیر و نگهداری دارد . قابلیت اطمینان یک قطعه بنابه تعریف ، احتمال عدم شکست آن در فاصله زمانی 0 تا t است . یعنی احتمال اینکه قطعه از زمان شروع به کار خود تا زمانی دلخواه ، مثلاً t (که می تواند کل زمان کاری یا مأموریت قطعه باشد) ، خراب نشود و بطور موفقیت آمیز به کار خود ادامه دهد . بنابراین :

R (t) = احتمال عدم شکست قبل از زمان t

برای کشف ارتباط این تابع با توابع شکست و مخاطره به ضمیمه ج ، مراجعه می کنیم . در این ضمیمه توابع توزیع تجمعی و چگالی احتمال اینگونه تعریف شدند:

F (t) = احتمال شکست قبل از زمان t

f (t)dt = احتمال شکست در فاصله زمانی( t تا t+dt )

و احتمال شرطی، $\lambda(t)$ ، که تابع نرخ شکست یا تابع مخاطره۲ نامیده می‌شود . اینگونه تعریف شد :

[1] Reliability
[2] Hazard function

λ (t) = [احتمال شکست در فاصله زمانی( t تا t+dt ) به شرط آنکه تا زمان t شکستی اتفاق نیفتاده باشد ]

همچنین برای هر توزیع عام، ارتباط مهم بین این ۳ تابع عبارت است از:

$$\lambda(t) = \frac{f(t)}{1-F(t)}$$

در واقع مخرج این تابع شرطی همان تابع قابلیت اطمینان است . یعنی :

$$R(t) = 1-F(t)$$

از طرفی در ادامه محاسبات همین ضمیمه داشتیم :

$$F(t) = 1 - \exp\left[-\int_0^t \lambda(x)dx\right]$$

بنابراین :

$$R(t) = 1-F(t) = \exp\left[-\int_0^t \lambda(x)dx\right]$$

دیدیم که در منحنی bathtub و در منطقه وسط آن ، نرخ شکست تقریباً ثابت است . اگر مقدار ثابت نرخ شکست برابر با λ باشد داریم :

$$R(t) = e^{-\lambda t}$$

## ضمیمه ه ) مثالی از رسم درخت خطا

در این ضمیمه برای روشن شدن ذهن خوانندگان و انجام تمرین بیشتر به ذکر یک مثال که کاربرد درخت خطا را حتی در زندگی روزمره نشان می دهد ، می پردازیم :

**ه-۱) دیر بیدار شدن از خواب :**

فرض کنید فردی به جزء ایام تعطیل و مرخصی ، بایستی هر روز صبح سر ساعت ۶ صبح از خواب بیدار شود و بعد از آماده شدن و صرف صبحانه ، منزل را ساعت ۶:۳۰ دقیقه ترک کند تا به سرویس برسد. این فرد یک ساعت برقی عقربه دار دارد که هر شب زنگ بیدارباش آن را برای ساعت ۶ تنظیم می کند. او برای اطمینان ساعت دیگری را تهیه کرده که شماطه دار است و برای فعال کردن زنگ آن ، بایستی تنظیم و کوک شود . این ساعت را نیز برای ساعت ۶:۰۵ دقیقه کوک می کند .

دیر بیدار شدن از خواب ، تبعات ناخوشایندی را برای این فرد دارد . اول اینکه سرویس اداره را از دست می دهد و به دلیل آنکه در آن موقع صبح ، دسترسی به وسیله دیگری ندارد ، مجبور است به آژانس زنگ بزند و درخواست یک خودرو کند . ممکن است بر حسب اتفاق ، آزانس مزبور خودرویی در اختیار نداشته باشد و ضمن معذرت خواهی از متقاضیان بخواهد حداقل نیم ساعتی را صبر کنند .

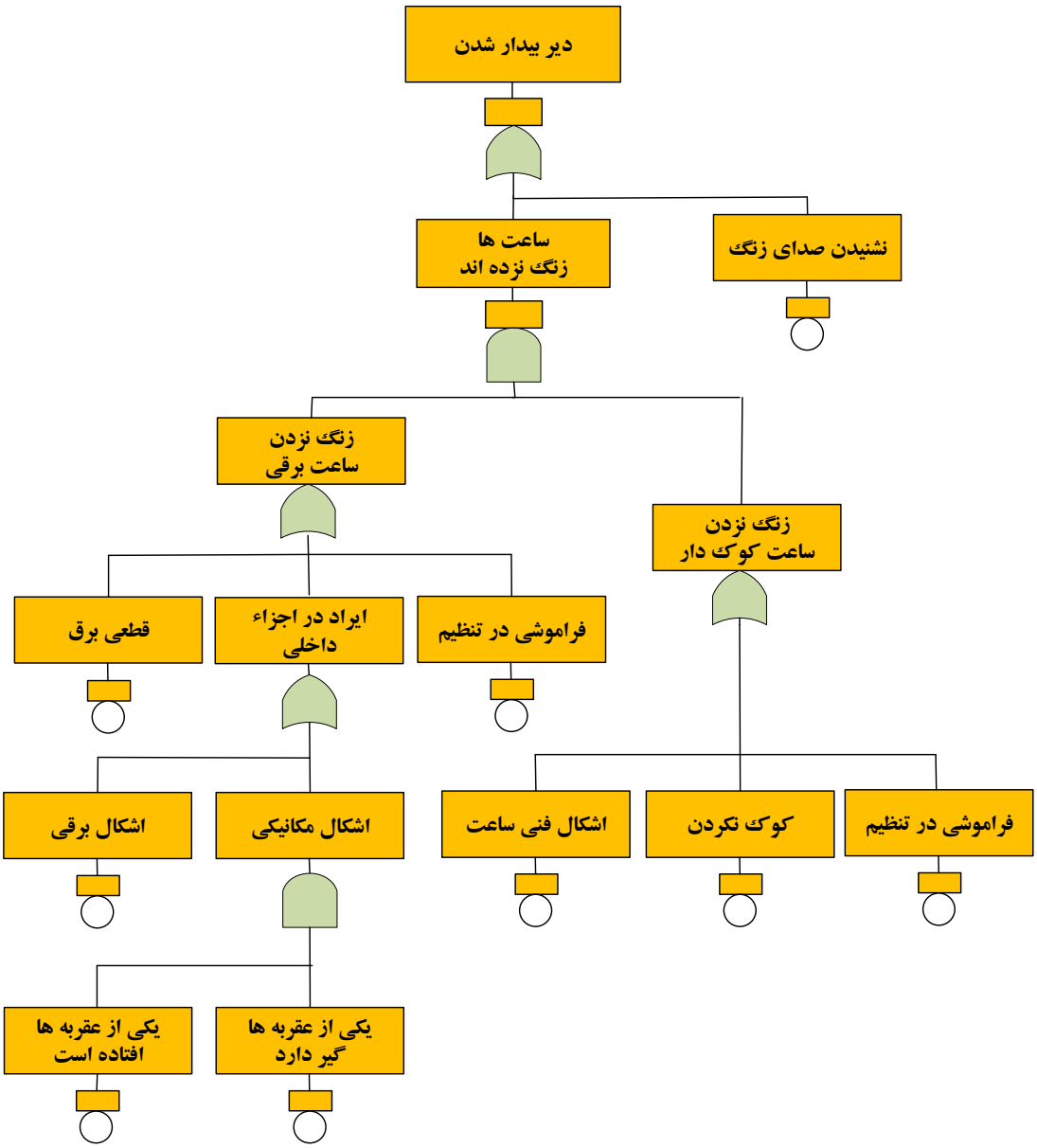
دوم اینکه بدلیل دیر رسیدن به محل کار بدون هماهنگی و گرفتن مرخصی ساعتی در روز قبل و بدلیل اینکه احتمالاً اینگونه دیر رسیدن ها سابقه قبلی هم داشته است ، به عنوان کارمندی بی نظم شناخته می شود و ممکن است فوق العاده اضافه کاری را از دست بدهد و یا اثرات حقوقی منفی دیگری برایش بوجود بیاید .

و سوم اینکه استرس دیر رسیدن به محل کار و تصّور چهره ی غضبناک کارفرما یا رییس ممکن است ، یک روز خوب او را کاملاً خراب کند و این اتفاق ناخوشایند باعث شود که هیچ یک از کارهایش را بدرستی انجام ندهد.

در تصویر ه-۱ ، درخت خطای مربوط به دیر بیدار شدن از خواب نامبرده علیرغم داشتن دو ساعت زنگ دار ، رسم شده است . ساعت برقی و کوک دار به ترتیب ساعت اصلی و پشتیبان هستند . البته مفروضات این مسئله اختیاری بوده و تنها برای یادگیری است .

**ه-۲) شرح درخت**

دیر بیدار شدن فرد از خواب را به عنوان رویداد رأس انتخاب کرده ایم . برای رسم درخت سعی کرده ایم که از تمامی قواعد رسم ، پیروی کنیم . به عنوان مثال در منطق درخت خطا نباید انتظار معجزه یا یک اتفاق عجیب و غریب را داشته باشیم . مثلاً تصوّر کنیم ، فرد مزبور علیرغم کار نکردن ساعت ها ، بدلیل وقوع آتش سوزی در ساختمان مجاور و سروصدای زیاد خودروهای آتش نشانی بیدار شده است . یا اینکه یکی دیگر از ساکنین خانه بدلیل اینکه گرفتار یک کابوس وحشتناک شده ، درست سر ساعت ۶ با فریاد دلهره آوری از خواب بیدار می شود .




**تصویر ه-۱ : درخت خطای مربوط به دیر بیدار شدن**

## ۵-۳) ارزیابی کیفی

ارزیابی درخت خطای تصویر ه-۱ ، نیاز به نامگذاری رویدادهای پایه و گیت دارد . رویدادها را بدین شکل نامگذاری کرده ایم :

A = یکی از عقربه ها گیر دارد.

B= یکی از عقربه ها افتاده است.

C= اشکال برقی

D= قطعی برق

$E_1$ = فراموشی در تنظیم ساعت برقی

$E_2$ = فراموشی در تنظیم ساعت شماطه دار

F= اشکال فنی ساعت ساعت شماطه دار

G= کوک نکردن ساعت شماطه دار

K= نشنیدن صدای زنگ

S= اشکال مکانیکی ساعت برقی

U=ایراد در اجزاء داخلی

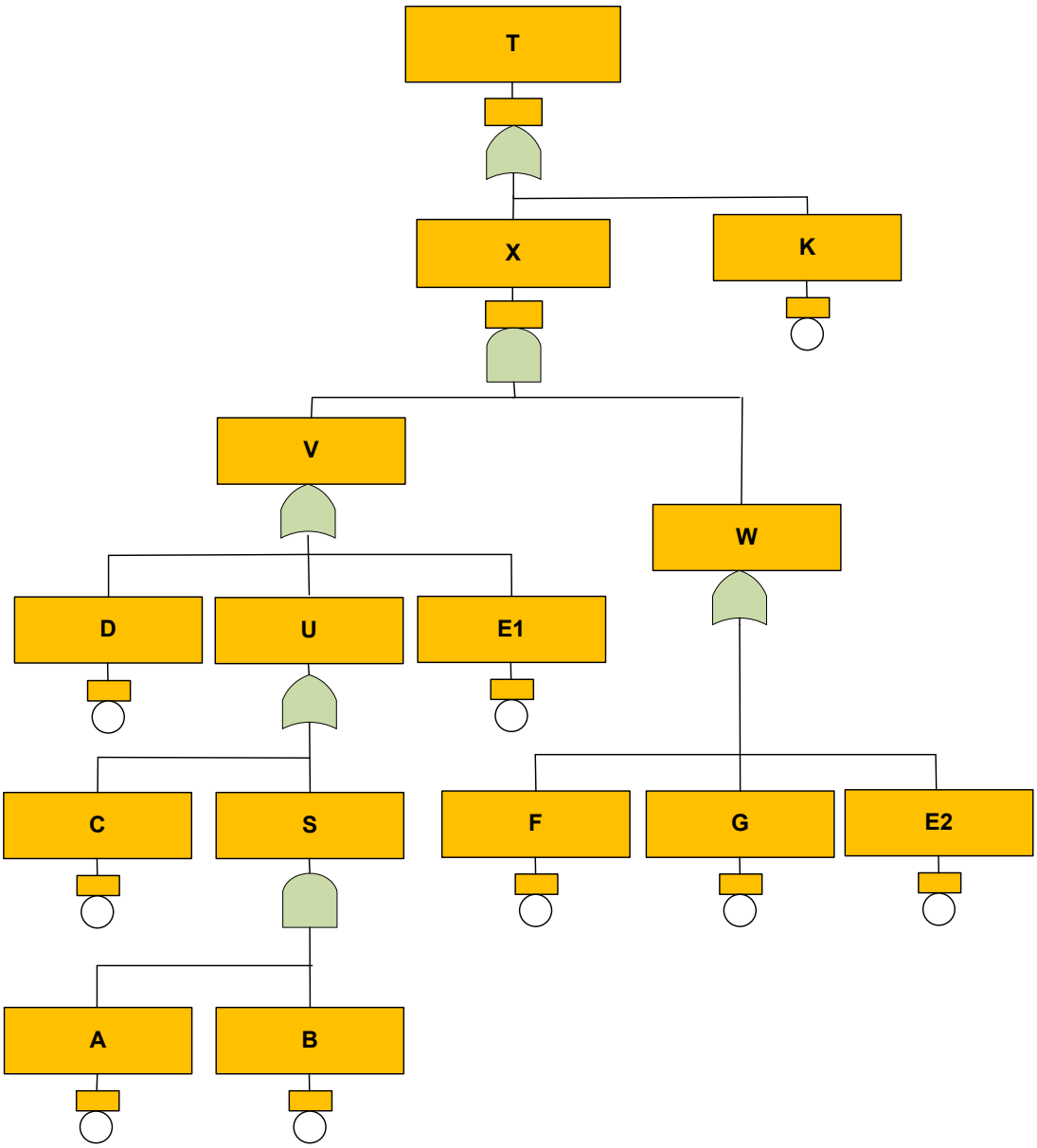
V = زنگ نزدن ساعت برقی

W=زنگ نزدن ساعت شماطه دار

X= ساعت ها زنگ نزده اند

T= دیر بیدار شدن

برای راحتی کار و جلوگیری از اشتباه درخت خطای تصویر ه-۱ را مجدداً با نوشتن علائم ، بازنویسی می کنیم . نتیجه کار را در تصویر ه-۲ مشاهده می کنید .




**تصویر ه-۲ : درخت خطای نامگذاری شده**

حال رویداد رأس را برحسب رودادهای پایه اش می نویسیم . اگر بخواهیم از روش گیت استفاده کنیم ، دو راه داریم : اول بسط گیت ها از پایین به بالا و دوم بسط گیت ها از بالا به پایین . هر دو راه را امتحان می کنیم :

**الف ) بسط رویداهای گیت از پایین به بالا :**

$S=A.B$
$U=S+C=C+A.B$
$V=D+E_1+U=D+E_1+C+A.B$
$W=F+G+E_2$
$X=V.W= (D+E_1+C+A.B). (F+G+E_2)$
$X= E_1.F+ E_1.G + E_1. E_2 +D.F+D.G+ D. E_2 +C.F+C.G+ C. E_2 +A.B.F+A.B.G+ A.B.E_2$
$T=X+K=K+E_1.F+E_1.G+E_1.E_2+D.F+D.G+D.E_2 +C.F+C.G+ C.E_2 +A.B.F+A.B.G+ A.B. E_2$
**$T= K+E_1.F+E_1.G+E_1. E_2 +D.F+D.G+ D.E_2 +C.F+C.G+ C.E_2 +A.B.F+A.B.G+ A.B.E_2$**

**ب) بسط رویدادهای گیت از بالا به پایین :**

$T=X+K$
$X=V.W$
$T=V.W+K$
$V= D+E_1+U$
$W= F+G+E_2$
$T= (D+E_1+U). (F+G+E_2)+K$
$T=K+ E_1.F+ E_1.G+ E_1. E_2 +D.F+D.G+ D. E_2 +U.F+U.G+ U. E_2$
$U =S+C$
$T= K+ E_1.F+ E_1.G+ E_1. E_2 +D.F+D.G+ D. E_2 +S.F+S.G+ S. E_2+C.F+C.G+ C. E_2$
$S=A.B$
**$T= K+ E_1.F+ E_1.G + E_1.E_2 +D.F+D.G+ D.E_2 +C.F+C.G+ C.E_2+A.B.F+A.B.G+ A.B. E_2$**

همانطور که مشاهده می کنید نتیجه یکی است . برای ارزیابی کیفی بایستی رویداد رأس را بر حسب مجموعه برش های حداقل نوشت و سپس برش ها را از نظر ترکیب و تعداد رویدادهای پایه ، بررسی نمود . برش هایی که تنها یک رویداد پایه دارند (برش های منفرد) ، بخصوص اگر عدد احتمال وقوع آنها در مقابل بقیه ی برش ها قابل قیاس باشد ، اهمیت خاصی در ارزیابی کیفی دارند .

در رابطه بالا ، تنها برش منفرد ، رویداد **K** است که از همان ابتدا جلب توجه می کند . اهمیت این رویداد در این است که اگر رخ دهد ، بدون واسطه سبب بروز رویداد رأس می شود . شرح این رویداد عبارت است از :

K= نشنیدن صدای زنگ

نشیدن صدای زنگ به علت کری شبانه ناشی از خواب عمیق است . فرض ما بر این است که فرد مورد نظر، شب قبل به موقع خوابیده و به صدای زنگ حساس است . بنابراین احتمال نشیدن صدای زنگ خیلی کم است .

**۵-۴) ارزیابی کمّی**

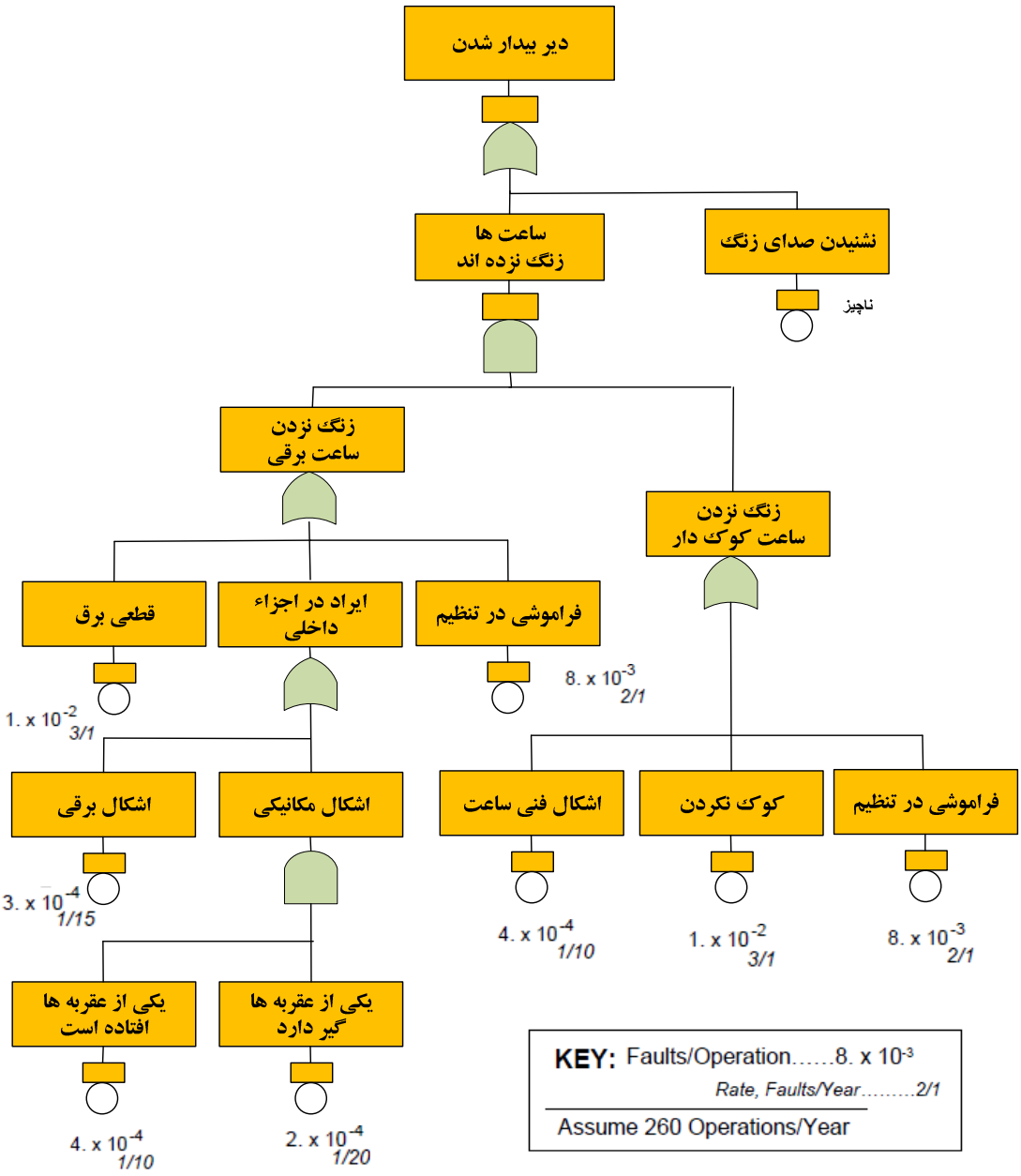
برای انجام ارزیابی کمّی نیاز به اطلاعات نرخ شکست رویدادهای پایه و تبدیل آنها به احتمال شکست داریم . در تصویر ه-۳ نرخ شکست رویدادها در کنار شناسه آنها ، نوشته شده است . فرض بر این است که کارمند مورد علاقه ما در مدت یک سال ، ۲۶۰ روز به محل کار می رود .

در این تصویر در کنار هر رویداد دو عدد دیده می شود : عدد پایینی نرخ شکست رویدادها است . مثلاً 1/20 به معنی یک بار شکست در ۲۰ سال است . عدد بالایی احتمال شکست رویداد بر حسب تعداد خطا در روز (یا در هر بار استفاده) است و از عدد بالایی بدست می آید . به عنوان مثال برای یک بار شکست در ۲۰ سال ، اینگونه محاسبه می شود :

$20\times260=5200$ تعداد روزهایی که در سال از ساعت استفاده می شود

$$\frac{1}{5200}\cong 2\times10^{-4}$$

احتمال شکست بقیه رویدادها نیز به همین شکل محاسبه می شود . برای محاسبه احتمال وقوع رویداد رأس (یعنی دیر بیدار شدن) ، بایستی مقدار $P(T)$ را محاسبه کنیم . برای این کار باید از رابطه $T$ که در ارزیابی کیفی بدست آورده ایم ، احتمال بگیریم .




**تصویر ه-۳ : نرخ خطای مربوط به رویدادهای پایه**

داریم :

$$P(T)=P(K+E_1.F+E_1.G+E_1.E_2+D.F+D.G+D.E_2+C.F+C.G+C.E_2+A.B.F+A.B.G+A.B.E_2)$$

$$P(T)=P(K)+P(E_1.F)+P(E_1.G)+P(E_1.E_2)+P(D.F)+P(D.G)+P(D.E_2)+P(C.F)+P(C.G)+P(C.E_2)+P(A.B.F)+P(A.B.G)+P(A.B.E_2)-\theta$$

مقدار θ ، بر اساس قانون جمع احتمالات (بخش ب-۱ از ضمیمه ب) ؛ محاسبه می شود . طبق این قانون اگر I و J دو رویداد دلخواه و مستقل باشند ، داریم :

$$P(I+J) = P(I) + P(J) - P(I).P(J)$$

بنابراین برای احتمال جمع دو رویداد ، مقدار θ می شود :

$$\theta = P(I).P(J)$$

با افزایش تعداد رویداد ها ، بایستی عبارت مفصل تری برای θ نوشت . در این حالت θ برابر با جمع احتمال ترکیبات دوتایی منهای احتمال ترکیبات سه تایی بعلاوه احتمال ترکیبات چهار تایی منهای احتمال ترکیبات پنج تایی (و به همین ترتیب تا آخر) است . با استفاده از تقریب رویدادهای نادر[1] و با توجه به کوچک بودن احتمال ترکیبات سه تایی و بالاتر ،می توان با یک تقریب خوب از آنها صرف نظر کرد . از طرفی با توجه به مطالبی که در ارزیابی کیفی عنوان شد و ناچیز بودن احتمال وقوع رویداد K ، می توان از احتمال وقوع آن و تمامی ترکیباتی که این رویداد را در خود دارند ، صرف نظر کرد . با استفاده از این مفروضات تنها به ترکیبات سه تایی می پردازیم که عدد احتمال آنها قابل توجه باشد :

$$\theta \approx P(E_1.D.G) + P(E_2.D.G)$$

درخت خطا را طوری رسم کرده ایم که رویدادها از هم جدا و مستقل باشند . بنابراین طبق نظریه اساسی احتمال ، احتمال حاصلضرب چند رویداد مستقل با حاصلضرب احتمال آنها برابر است و داریم :

$P(E_1.D.G) = P(E_1).P(D).P(G) = (8\times10^{-3}) \times (1\times10^{-2}) \times (1\times10^{-2}) = 8\times10^{-7}$
$P(E_2.D.G) = P(E_2).P(D).P(G) = (8\times10^{-3}) \times (1\times10^{-2}) \times (1\times10^{-2}) = 8\times10^{-7}$
$\theta = 8\times10^{-7}+8\times10^{-7} = 1.6\times10^{-6}$
$P(A.B.G) = P(A).P(B).P(G) = (4\times10^{-4}) \times (2\times10^{-4}) \times (1\times10^{-2}) = 8\times10^{-10}$
$P(A.B.F) = P(A).P(B).P(F) = (4\times10^{-4}) \times (2\times10^{-4}) \times (4\times10^{-4}) = 3.2\times10^{-11}$
$P(A.B.E_2) = P(A).P(B).P(E_2) = (4\times10^{-4}) \times (2\times10^{-4}) \times (8\times10^{-3}) = 6.4\times10^{-10}$
$P(C.G) = P(C).P(G) = (3\times10^{-4}) \times (1\times10^{-2}) = 8\times10^{-6}$
$P(C.F) = P(C).P(F) = (3\times10^{-4}) \times (4\times10^{-4}) = 1.2\times10^{-7}$
$P(C.E_2) = P(C).P(E_2) = (3\times10^{-4}) \times (8\times10^{-3}) = 2.4\times10^{-6}$
$P(D.G) = P(D).P(G) = (1\times10^{-2}) \times (1\times10^{-2}) = 1\times10^{-4}$
$P(D.E_2) = P(D).P(E_2) = (1\times10^{-2}) \times (8\times10^{-3}) = 8\times10^{-5}$
$P(D.F) = P(D).P(F) = (1\times10^{-2}) \times (4\times10^{-4}) = 1\times10^{-6}$
$P(E_1.F) = P(E_1).P(F) = (8\times10^{-3}) \times (4\times10^{-4}) = 3.2\times10^{-6}$
$P(E_1.G) = P(E_1).P(G) = (8\times10^{-3}) \times (1\times10^{-2}) = 8\times10^{-5}$
$P(E_1.E_2) = P(E_1).P(E_2) = (8\times10^{-3}) \times (8\times10^{-3}) = 6.4\times10^{-5}$
$P(T) = P(K)+P(E_1.F)+P(E_1.G)+P(E_1.E_2)+P(D.F)+P(D.G)+P(D.E_2)+P(C.F)+P(C.G)+P(C.E_2)+P(A.B.F)+P(A.B.G)+P(A.B.E_2)-\theta$
$P(T) = 3.2\times10^{-6}+8\times10^{-5}+6.4\times10^{-5}+1\times10^{-6}+1\times10^{-4}+8\times10^{-5}+1.2\times10^{-7}+8\times10^{-6}+2.4\times10^{-6}+8\times10^{-10}+3.2\times10^{-11}+6.4\times10^{-10}-1.6\times10^{-6}$
**$P(T) = 3.3713\times10^{-4}$**

[1] Rare Event Approximation

که با حساب ۲۶۰ بار استفاده در سال ، این مقدار احتمال برابر با یک بار وقوع در هر ده سال می شود . مشاهده می کنید که احتمال وقوع رویداد رأس ، بسیار کم است . شاید علت اصلی این مطلب استفاده همزمان از دو ساعت زنگ دار باشد که ضریب اطمینان بیدار شدن فرد را بالا می برد .

البته هدف از آوردن این مثال نشان دادن ابعاد دیگری از تحلیل درخت خطا بود . در واقع این تحلیل ابزار بسیار خوبی در تمامی زمینه ها و حوزه ها است . ابزاری که به مدیران و تحلیل گران اجازه عبور از ارزیابی کیفی به سمت ارزیابی کمی را می دهد و به توانایی ودقت تصمیم گیری آنها ، کمک می کند .

در این مثال ، احتمال وقوع رویداد رأس محاسبه گردید اما هنوز کار تمام نشده است . خواننده به عنوان تمرین می تواند میزان اهمیت رویدادهای فرعی و حداقل برش ها را محاسبه و رتبه بندی را انجام دهد . با رتبه بندی برش ها ، رویدادهای پایه غالب (dominant) شناسایی شده و براحتی در زیر ذره بین تحلیل گر قرار می گیرند . در مرحله بعد خواننده بایستی راهکارهایی را برای کاهش احتمال وقوع رویدادهای پایه دردسر ساز ارائه دهد . به عنوان مثال ممکن است برای کاهش احتمال وقوع رویداد فراموشی در تنظیم ساعت (رویدادهای $E_1$ و $E_2$ ) می توان از تداعی ذهنی استفاده کرد . و این تصور را در ذهن تکرار و پرورش داد که جدیداً ساعتی ساخته اند که شبیه به بالش است و به محض سر نهادن بر آن کوک می شود . روش دیگر داشتن یک چک لیست ذهنی و حتی عینی است . این چک لیست می تواند موارد متعددی را که قرار است قبل از خواب بررسی و انجام شوند ، در بر بگیرد . مثلاً مسواک زدن ، دارو خوردن ، آماده کردن کیف ، نوشتن یک صفحه از دفتر خاطرات و تنظیم زنگ ساعت ، ممکن است عناوینی از این چک لیست باشند .

## واژگان

# A

Active

**فعال ، عامل** - در تحلیل درخت خطا منظور قطعه یـا تجهیـزی اسـت کـه بنـوعی تغییـری در فرآیند بوجود آورد . مانند شیر کنترل نصب شده در مسیر یک خط لوله که بر جریـان فرآینـد تاثیر گذار است . مثال های دیگری از این دست ، اندازه گیر های سطح جریان ، صافی ، فیلتـر و تفکیک گرهای نفت وگاز می باشد .

Additive

افزاینده – موادی که برای تکمیل فرآیند به واکنش اضافه می شود .

Approach

**دیدگاه ، نگرش ، نقطه نظر**

Associative Law

**قانون شرکت پذیری در ریاضی**

Availability

**دسترس پذیری ، قابلیت دسترسی**

زمانی که سیستم در شرایط کاری است یا به عبارت دیگر نسبت زمان قابل استفاده بودن یـک تجهیز به کل زمان کاری آن . به عنوان مثال اگر یک دستگاه در یک هفته ، تنها ۱۰۰ سـاعت قابل استفاده باشد ، دسترس پذیری آن $\frac{100}{168} = 0.595$ است .

ساده ترین فرمول قابلیت دسترسی به شکل زیر است :

$$A = \frac{E[\text{Uptime}]}{E[\text{Uptime}] + E[\text{Downtime}]}$$

که در آن E(Uptime) ، زمان قبل از خرابی و توقف دستگاه می باشد که به آن زمـان متوسـط قبل از شکست یا MTBF مـی گوینـد . همچنـین E(Downtime) ، زمـان بازیـابی یـا تعمیـر دستگاه بعد از وقوع خرابی می باشد که MTR ، نامیده می شود . بنابراین فرمول بالا به شـکل زیر هم نوشته می شود :

Availability= MTBF/ (MTBF+MTR)

# B

Backwards

**رو به عقب**

**Basic Event**

**رویداد پایه** - یک خطای آغازین پایه که نیازی به توسعه بیشتر آن نیست .

Basic symbol

**نماد پایه یا اساسی**

Bayes theorem

**تئوری بیز**

Bayesian confidence intervals

**فاصله اطمینان بیزی**

Binary

**دودوئی**

Binary Decision Diagram

**نمودارهای تصمیم دودوئی**

Binomial cumulative distribution

**توزیع تجمعی دوجمله ای**

Bottom

**انتها ، کف ، پایین**

Bottom-up

**از پایین به بالا**

Bottom-up substitution

**جایگذاری از پایین به بالا**

Brain Storming

**خرد جمعی ، طوفان مغزی** - یک تکنیک خلاقانه گروهی است که به منظور ایجاد تعداد زیادی نظر در باره حل یک مشکل طراحی شده است . این روش در سال ۱۹۵۳توسط آلکس اُسبرن در کتابی به نام **تخیل کاربردی** آورده شد و عمومیت یافت . او عقیده داشت با تکنیک فوق ، خلاقیت دوبرابر خواهد شد .

به منظور افزایش خلاقیت در گروه ، تشویق به ارائه نظر و رفع موانع کارگروهی ، استفاده از خرد جمعی منوط به رعایت ۴ اصل به شرح زیر می باشد .

**۱- تمرکز بر روی تعداد** : این قانون ابزاری برای افزایش نظرات به شکل واگرا است . یعنی با حداکثر شدن کمّیت ، کیفیت پربار خواهد شد و این امر باعث تسهیل در حل مسئله خواهد گردید . به زبان ساده تر با بیشتر شدن نظرات ، شانس حل مسئله به شکل مؤثر و ریشه ای بیشتر خواهد شد .

**۲- پرهیز از نقد :** در روش خرد جمعی ، بایستی از نقد نظرات ارائه شده ، ممانعت نمود . به جای این کار شرکت کنند گان باید به بسط نظرات و افزودن ایده به آن بپردازند و انتقاد را به مرحله نقد و بررسی فرآیند ، موکول کنند . بدینوسیله با رها کردن قضاوت ها ، شرکت کنندگان احساس آزادی بیشتری کرده و ایده های مفیدتری خلق خواهد شد .

**۳- استقبال از نظرات غیر معمول :** برای رسیدن به فهرستی خوب و طولانی از نظرات ، بایستی پذیرای ایده های غیرمعمول و عجیب بود . چرا که این نظرات ممکن است از زاویه ای جدید به مسئله نگاه کرده و مفروضات آن را رها کنند و چه بسا راه های بهتری برای حل مسئله باشند .

**۴- ترکیب و رشد نظرات :** نظرات خوب را می توان با هم ترکیب کرد و نظری واحد و بهتری یافت . اسلوگان (slogan) عقیده دارد جمع ریاضی نظرات بدین شکل است :

**۱+۱=۳**

**مراحل انجام تکنیک خرد جمعی :**

**تعریف مسئله :** قبل از نشست جمعی ، تعریف مسئله یا مشکل ، حیاتی است . صورت مسئله بایستی به شکلی واضح و نه خیلی بسیط ، تهیه شود . اگر صورت مسئله خیلی بزرگ باشد ، بایستی آن را به اجزاء کوچکتری تقسیم نمود و برای هر یک سؤالی واضح طرح نمود .

**زمینه سازی :** در این بخش ، نامه ای جهت اطلاع و دعوت اعضاء آماده می شود . این نامه ، شامل نام شرکت کننده ، شرح مسئله ، تاریخ ، ساعت و مکان تشکیل جلسه می باشد . مسئله بایستی به شکل عبارت سؤالی و با ذکر بعضی راه حل های نمونه ، آورده شود . این نامه بعد از

انتخاب اعضاء برای آنها ارسال می شود . بدین ترتیب شرکت کنندگان ، فرصت کافی برای فکر و ایده سازی خواهند شد و بستر حل مسئله فراهم می گردد .

**انتخاب اعضاء** : در این مرحله با توجه به نوع مسئله ، اعضاء انتخاب می شوند . همچنین یک نفر بایستی به ثبت ایده ها بپردازد . عموماً یک گروه ۱۰ نفره (یا کمتر) ، بهره وری بهتری خواهند داشت . برای اتنخاب اعضاء ممکن است گزینه های متعددی داشته باشیم اما ترکیب زیر پیشنهاد می شود :

- ✓ اعضاء کلیدی پروژه که قابلیت خود را به اثبات رسانده باشند .
- ✓ مهمانانی از خارج پروژه که با مسئله مأنوس باشند .
- ✓ یک نفر که نظرات را ثبت کند .

**تهیه فهرستی از سؤالات راهگشا** : در خلال جلسه ، ممکن است خلاقیت کاهش یافته و ایده سازی متوقف شود . در این زمان ، دبیر جلسه بایستی با استفاده از سؤالاتی که از قبل آماده شده است ، به تحریک خلاقیت و ایجاد انگیزه در اعضاء ، بپردازد . سؤالاتی نظیر :

آیا می شود این نظرات را با هم ادغام نمود ؟ (برای رسیدن به نظر بهتر)

چطور است از منظر دیگری به مسئله نگاه کنیم ؟

**هدایت جلسه** : جلسه بایستی بر پایه اصول تکنیک خرد جمعی هدایت شود .به عنوان مثال شامل مراحل زیر باشد :

۱- مقدمه سازی و گرم نمودن فضای جلسه : برای آنکه شرکت کنندگان در فضای بدون انتقاد قرار بگیرند ، یک سؤال ساده طرح کنید . مثلاً چگونه می توان سیستم عامل مایکروسافت را ارتقاء داد؟

۲-مسئله اصلی را طرح کنید و اگر نیاز باشد توضیح بیشتری در مورد هدف از طرح سؤال بدهید .

۳- از گروه بخواهید تا ارائه نظر کند .

۴- اگر ایده ای مطرح نشد ، با طرح سؤال انگیزه ایجاد کنید . اگر فردی شروع به طرح نظر کرد او را تشویق کنید .

۵- هنگام طرح ایده ها و صحبت در مورد آنها ، عضو مسئول ، آنها را ثبت کند .

۶- به منظور شفاف سازی ، به شرکت کنندگان امکان دهید جزئیات بیشتری از نظر خود را بیاورند .

۷- بعد از اتمام زمان طرح نظریات ، آنها را بر اساس هدف ، منظم کنید (سعی کنید سازماندهی نظریات به شکل طبقه بندی باشد)

۸- فهرست ایده ها را دوباره بررسی و مطمئن شوید همه اعضا درک متقابلی از آنها پیدا کرده اند .

۹- نظریات تکراری و ایده هایی را که غیر قابل انجام هستند را حذف کنید .

۱۰ – حال به مرحله ارزیابی راه حل ها رسیده ایم . این ارزیابی گاه نیازمند استفاده از فرد یا گروه متخصص تری می باشد . همچنین برآورد هزینه ها و میزان سودآوری هر ایده ممکن

است در بخش  مالی صورت پذیرد . آنچه مهم است داشتن معیارهای خوب برای ارزیابی است . به عنوان مثال خطی مشی سازمان یا اهداف استراتژیک آن می تواند معیار خوبی باشد .

۱۱- اولویت دهی راه حل ها و انتخاب اولین راه حل : این مرحله گاهی با استفاده از مدل های تصمیم گیری نظیر درخت تصمیم ، انجام می گیرد .

۱۲- راه حل انتخاب شده را مجدداً با پرداختن به جزئیات بیشتر ، بازکنید . فرآیند انجام آن را با گراف یا چارت رسم کرده و یک دستورالعمل برای انجام مراحل آن تهیه نمایید

۱۳- در این دستورالعمل بایستی منابع مورد نیاز مشخص شود و زمانبندی انجام طرح با توجه به گلوگاه ها رسم شود .

۱۴- اگرچه بعد از سازمان دهی ایده ها ، فرآیند انتخاب و اجرای بهترین راه حل در حیطه وظایف اعضای گروه نیست . اما می توان از آنها کمک گرفت .

۱۵- در پایان از شرکت کنندگان قدردانی کرده و به طریقی همکاری آنها را در سازمان منعکس کنید .

# C

## Case Study

**مطالعه موردی** – روشی برای درک بهتر و اثبات نتایج یک ایده یا نظریه است . بدین شکل که محقق برای بسط و کاربردی نمودن یک تکنیک یا ایده ، کلی گویی را رها کرده و به تفضیل مراحل انجام آن در یک گروه یا سازمان ، می پردازد . در این تفضیل ، گاهی نیاز به جمع آوری اطلاعات می باشد که محقق بایستی روش جمع آوری داده ها را معلوم کند . همچنین بعد از

توضیح نمونه اجرا شده طرح ، ممکن است در مـورد چـالش هـای انجـام آن بحـث شـود و یـا مسیرهای دیگری برای تحقیق بیشتر باز شود . به طور خلاصه در یک مطالعه موردی محقق به طرح و ایجاد مفروضات و چگونگی آزمودن آنها می پردازد

Category

**طبقه**

Child node

**گره فرزند**

Circuit Breaker

**مدار شکن ، کلید قدرت قطع کننده برق فشار قوی** – این کلید الکترونیکی به گونـه ای طراحـی گردیده تا مدار را در مقابل خسارات ناشی از اتصال کوتاه یا بار غیرمجاز ، حفـظ کنـد . تفـاوت این وسیله حفاظتی با فیوز این است که فیوز یکبار مصرف بوده و بعد از عمل بایسـتی تعـویض شود اما مدار شکن را مجدداً با ری ست نمودن آن ، می توان استفاده نمود .

Command Fault

**خطای فرمان** - خطای فرمان، مربوط به عملکرد صحیح تجهیز، اما در زمان یا مکان اشتباه است به عنوان مثال بسته شدن یک شیر کنتـرل، در زمـان نامناسـب و بـه علـت دریافـت سـیگنال ناخواسته، یک خطای فرمان برای شیر محسوب می‌شود. همینطور متوقف شدن یک خط تولید، به علت خاموشی برق، مثالی دیگر از بروز خطای فرمان است.

Common Cause

**علت مشترک**

Common Cause Failures

**شکست های علت مشترک** - منظور از شکست‌های علت مشترک (CCF ) ، شکست (خرابی) دو یا چند قطعه به طور همزمان یا در فاصله‌ای نسبتاً کوتاه است که به خاطر یک علت مشترک باشد. قطعه ، ممکن است هر عنصری از یک سیستم (مانند شیر کنترل، پمپ یا زیر سیستم-هایی نظیر منبع تغذیه برق) باشد . شکست‌های علت مشترک در تحلیل درخت خطا ، مانند دیگر شکست‌ها، به طور صریح دیده نمی‌شوند و در لفافه هستند بنابراین وابستگی یک قطعه را از نظر وظیفه و کارکرد به بخش تامین کننده سیستم (مانند تغذیه برق) نشان نمی‌دهند که مثلاً اگر جریان از طرف این بخش قطع شود، چه شکست‌های چندگانه ای ممکن است بوجود آید . منظور ما از شکست‌های علت مشترک، یک وابستگی ضمنی است که می‌تواند باعث ایجاد شکست‌های یکسان در قطعات شبیه به هم شود.

Commutative Law

**قانون جابجایی**

Complementation

**متمم گیری**

Component failure probability

**احتمال شکست قطعه**

Component failure rate

**نرخ شکست یا خرابی قطعه**

Component Fault

**خطای قطعه**

Component unavailability

**عدم دسترسی به قطعه** – بدین معنی است که در صورت تقاضا یا مراجعه بـه یـک قطعـه بـرای انجام وظیفه اش در سیستم ، چقدر احتمال می رود که قطعه پاسخگو نباشد . به عنـوان مثـال قطع ای که عدم دسترسی به آن ۰/۱ باشد ، به این معنی است که در ۱۰ درصد موارد ، قطعـه در دسترس نیست و کار نمی کند . اگر دسترس پـذیری (availability) یـک قطعـه را داشـته باشیم (به معنای این کلمه در همین بخش مراجعه کنید) ، می توانیم آنـر را از عـدد یـک کـم کنیم تا عدم دسترسی به آن بدست آید .

Contacts

**اتصالات**

Control valve

شیر کنترل – در واحدهای فرآیندی از شیرها برای کنترل دبی خط استفاده می شود . شیر ها گاهی **عملکرد** ساده ای دارند و مثلاً بصورت دستی برای قطع یا برقراری جریـان در یـک لولـه مورد استفاده قرار می گیرند . اما در پاره ای از موارد نقش مؤثرتری در کنترل جریـان دارنـد . مانند شیر کنترل که بر روی آن یک سیستم کنترل ابزاردقیق قرار دارد و بـر اسـاس سـیگنال

فرمان که معمولاً از اتاق کنترل ، ارسال می شود . شیر را با درصد دلخواه باز یا بسته می کند . شیر کنترل ها در فرآیندهایی که پیچیده تر هستند ، نقش بسیار مهمی را بازی می کنند .

Cooling Water

**آب خنک کننده** – در واحد های فرآیندی ، معمولاً واکنش ها گرما زاست و برای کنترل درجه حرارت از روش های مختلفی استفاده می شود . یکی از این روش ها استفاده از ژاکت آب در جداره مخازن است . بدین شکل که آب در ژاکت مخزن جریان یافته و گرمای واکنش را به خود می گیرد و از مسیر دیگری خارج می شود . به این آب که به منظور کنترل درجه حرارت واکنش یا سیال مورد استفاده قرار می گیرد ، آب خنک کننده می گویند .

Cumulative distribution function

**تابع توزیع تجمعی**

Cut Set

**مجموعه برش** : مجموعه ای از رویدادها که وقوع آنها باعث رخداد رویداد رأس می گردد . یک مجموعه برش در واقع مسیری را در درخت خطا مشخص می کند که از رویدادهای پایه شروع شده و به رویداد رأس ختم می شود .

# D

De Morgan's Theorem

**قضیه دمورگان**

Deductive

**جزء گرا ،رسیدن از کل به جزء**

De-energized

**بدون برق یا انرژی** – اصطلاحی است که برقکاران و تکنسین های الکترونیک در مورد قطع تغذیه برق به کار می برند . وقتی یک تجهیز یا وسیله برقی بدون برق شود ، تغذیه برق از روی آن برداشته می شود یا به عبارتی دستگاه خاموش (OFF) می گردد . معمولاً این کار علاوه بر قرار دادن کلید در حالت خاموش ، به طریق مکانیکی نیز صورت می پذیرد . یعنی مثلاً برای حالت سه فاز ، پانل تغذیه برق از داخل پست ، بیرون کشیده می شود . در این صورت حتی با وصل کلید تغذیه ، دستگاه روشن نمی شود و بدین ترتیب ضریب ایمنی بالا می رود .

Defect

**عیب ، نقص**

Demand

**تقاضا** – اصطلاحی است که بیشتر در زنجیره عرضه بکار می رود . در مورد کالا یا خدمات، تقاضا به معنای درخواست مشتری برای خرید یا تمایل وی در استفاده از کالا یا خدمات است . اما در مبحث قابلیت اطمینان و تعمیر و نگهداری ، تقاضا به معنی درخواست سرویس یا خدمت دهی یک دستگاه یا تجهیز می باشد . مثلاً اگر نرخ شکست یک پمپ یک بار در ۱۲۰ تقاضا باشد . یعنی در هر ۱۲۰ بار روشن کردن پمپ ، یک بار پمپ به هر دلیلی روشن نمی شود .

Probability Density function

**تابع چگالی احتمال**

Detection and Recovery errors

**خطاهای (حاصل از ) کشف و بازیابی** - این خطاها مربوط به زمانی است که انسان در کشف و بازیابی یک شکست سیستمی ، اشتباه کند. برای مثال اگر قطعه ای خراب شود وبه موقع تعمیر گردد ممکن است به کاهش آثار یک حادثه کمک کند. اما خطا در کشف خرابی این قطعه و تعمیر آن در زمان مقتضی یک خطا از نوع کشف و بازیابی است.

Distribution parameters

**پارامترهای توزیع**

Distributive Law

**قانون توزیع پذیری**

Dominant

**برجسته ، شاخص ، غالب**

Downtime

**مدت از کار افتادگی** ، پریودی که یک تجهیز دراثر نقص فنی از فعالیت باز مانده است - این اصطلاح وقتی به کار می رود که در یک دوره زمانی سیستم یا تجهیز قابل استفاده نبوده و در دسترس نباشد . در این مدت ، سیستم قادر به سرویس دهی و انجام کار خود نیست .

# E

End state

**وضعیت نهایی**

Entities

**هویت ، موجودی ، شناسه ،بوده**

Environmental sensitivity

**حساسیت محیطی**

Errors of commission

**خطاهای اقدام یا ارتکاب** - خطاهایی هستند که اغلب همراه با خطاهای اجرایی هستند به عنوان مثال اپراتور بجای انجام دستوالعمل مناسب، دست به اقدامات دیگری بزند که به مشکل دامـن بزند (دردسرساز شود)

Event occurrence probability

**احتمال وقوع رویداد**

Event occurrence rate

**نرخ وقوع رویداد**

Event Tree Analysis

**تحلیل درخت واقعه (رویداد)**

Exponential distribution

**توزیع نمایی** – به دسته ای از توابع توزیع در نظریه آمار و احتمال اشاره دارد که متغیر تصادفی آنها ، زمان بین رویدادها در یک فرآیند پواسون است . یعنی فرآیندی کـه در آن رویـدادها بـه شکل پیوسته و مستقل و با نرخ متوسط ثابتی رخ می دهند .

تابع چگالی احتمال یک توزیع نمایی به شکل زیر است :

$$f(x;\lambda) = \begin{cases} \lambda e^{-\lambda x}, & x \geq 0, \\ 0, & x < 0. \end{cases}$$

که در آن $\lambda > 0$ پارامتر توزیع می باشد . در بحث تعمیرونگهداری و تحلیل درخت خطا ، ثابت می شود که اگر رابطه بالا ، تابع چگالی احتمال شکست یک تجهیز باشد ، در این صـورت $\lambda$ ، نرخ شکست تجهیز است .

تابع توزیع تجمعی متغیر تصادفی با ماهیت نمایی ، عبارت است از :

$$F(x;\lambda) = \begin{cases} 1 - e^{-\lambda x}, & x \geq 0, \\ 0, & x < 0. \end{cases}$$

# F

Failure

**شکست ، خرابی**

Failure rate

**نرخ شکست**

Failure rate function

**تابع نرخ شکست که به آن تابع مخاطره هم می گویند**

Failure to close

**خطا در بسته شدن**

Failure to open

**خطا در باز شدن**

Fault

**خطا**

Fault Tree

**درخت خطا**

Feed

**خوراک ، تغذیه**

Forwards

**رو به جلو**

# G

Gate

واژه Gate در فارسی ترجمه های متفاوتی بسته بـه کـاربرد کلمـه و موضـوع دارد. در مـدارات الکترونیکی به معنای درگاه استفاده شده است . در کاربردهـای دیگـر ترجمـه هـای دریچـه ، مدخل ، دروازه ، ورودیه و دربزرگ را برای این کلمه داریم . در این کتاب از گیـت کـه بیشـتر رایج است ، استفاده کرده ایم .

# H

Hazard function

**تابع مخاطره** – این تابع ، میزان تکرار (فرکانس) شکست یک سیستم یا قطعه را (مثلاً بر حسب ساعت) بیان می کند . این تابع اغلب با حرف یونانی λ نشان داده شده و اهمیت بالایی در مهندسی قابلیت اطمینان دارد .

البته نرخ شکست بستگی زیادی به چرخه حیات سیستم دارد . به عنوان مثال در مورد خودرو ، طبیعی است که با فاصله گرفتن از تولید آن ، احتمال استهلاک و خرابی قطعات آن بیشتر می شود و نرخ شکست ۵ سال دوم آن به مراتب بیشتر از ۵ سال اول است . شاید در سال های اولیه نیازی به تعمیرات اساسی بر روی موتور نباشد . یا مشکلی برای سیستم ترمز آن پیش نیاید . اما در سال های بعد نیاز باشد که مثلاً لوله اگزوز آن تعویض شود . در عمل به جای نرخ شکست از واژه زمان متوسط بین شکست ها (MTBF) ، استفاده می شود . این واژه ، پارامتر مهمی در سیستم شده است که رابطه مستقیمی با ایمنی آن دارد . در واقع با کنترل MTBF ، می توان هزینه ها و مخاطرات ناشی از تعمیر ونگهداری را پایین آورد و بازرسی ها را در دوره های زمانی طولانی تری انجام داد . از طرفی با پایین آمدن نرخ شکست سیستم ، قابلیت اطمینان و ایمنی آن ، بالا می رود . در صورتیکه زمان بازیابی سیستمی که دچار شکست شده ، قابل اغماض باشد و شکست ها در طول زمان نرخ ثابتی داشته باشند ، نرخ شکست عکس MTBF خواهد شد .

$$(\lambda = 1/\ MTBF)$$

Hazard Identification

**شناسایی مخاطرات ، شناسایی عوامل بالقوه آسیب رسان**

Hazardous Event

**رویداد مخاطره آمیز** – مخاطره یا عامل بالقوه آسیب رسانی که بالفعل شده است . مثلاً اختلاف سطح (ارتفاع) ، مخاطره و سقوط رویداد مخاطره آمیز آن است .

Hazard

**مخاطره ، عامل بالقوه آسیب رسان**

Heat Exchanger

**مبدل گرمایی**

Human Reliability Analysis

**تحلیل قابلیت اطمینان انسان** – این تحلیل رابطه نزدیکی با مهندسی عوامل انسانی ، دارد و به بررسی میزان اطمینان به انسان در تولید ، حمل ونقل ، امور نظامی یا پزشکی ، می پردازد . البته عوامل زیادی مانند سن ، سلامت فیزیکی ، روحیه ، نگرش و احساسات بر عملکرد انسان تأثیر گذارند .

سیستمی را تصور کنید که انسان نقش مهمی در کنترل و پردازش آن داشته باشد . درچنین سیستمی هر گونه خطای انسانی می تواند به عواقب فاجعه آمیزی ختم شود . بنابراین نیاز است تحلیل خوبی از میزان اعتماد به انسان در آن بشود و مثلاً سیستم را از همان ابتدا به گونه ای طراحی کنیم تا احتمال خطای انسانی را به حداقل برساند .

I

Idempotent Law

**قانون همانی**

Identical valves

**شیرهای یکسان**

Immediate Cause

**علت فوری ، دلیل بلافصل**

Importance

**اهمیت**

Importance Measure

**سنجش اهمیت** – در این کتاب منظور از این عبارت ، اندازه‌گیری اهمیت نتایج حاصله از تحلیل درخت خطا است . این سنجش‌ها، هم به صورت نسبی و هم مطلق محاسبه می‌شود آنچه اغلب به هنگام محاسبه این اهمیت‌ها نتیجه‌گیری و استنباط می‌شود این است که تنها تعداد اندکی از رویدادها، نقش برجسته‌تری در وقوع رویداد رأس دارند. در بسیاری موارد کمتر از ۲۰ درصد رویدادها در ۹۰ درصد وقوع رویداد رأس ، نقش دارند. البته میزان اهمیت رویدادها را می‌توان در تمامی سطوح درخت خطا و برای رویدادهای فرعی انجام داد تا سهم آنها در وقوع رویداد رأس مشخص شود و با توجه به نتایج آن، بتوان رویدادهای میانی و حتی رویدادهای پایه را بر اساس اهمیتشان، الویت بندی کرد.

Independent

**مستقل**

Inductive

**کل گرا**

Infant mortality

**مرگ و میر اولیه** – عبارتی است که ارتباط مستقیم با نرخ شکست دارد . به هنگام رسم تابع مخاطره یا نرخ شکست یک سیستم ، متوجه می شویم که نرخ شکست در اوایل استفاده از یک قطعه یا میزان مرگ و میر اولیه نوزادان ، نسبت به دوره های میانی ، مقدار بیشتری دارد .

Initial Event

**رویداد آغازین** – رویدادی که حلقه اول از زنجیره یک سری وقایع متوالی باشد . مثلاً گرم شدن بدنه یک موتور ممکن است منجر به ذوب شدن کابل ها شود . ذوب شدن کابل ها ، اتصال کوتاه و جرقه را در پی خواهد داشت . جرقه به نوبه خود در یک محیط قابل اشتعال باعث آتش سوزی خواهد شد . آتش سوزی ممکن است منجر به نابودی بخشی از یک واحد فرآیندی شود . نابودی این بخش احتمال توقف تولید را خواهد داشت که بسته به زمان توقف و بازیابی سیستم ، خسارت های گرانباری به دنبال خواهد داشت . مشاهده کنید که رویداد گرم شدن بدنه موتور ، ممکن است تولید زنجیره ای از وقایع کند که سرچشمه و نقطه شروع آن گرم شدن بیش از حد بدنه موتور است . به همین دلیل این رویداد را رویداد آغازین می نامند .

Initiator

**پیشقدم ، آغازگر**

Inoperable

**غیر قابل استفاده**

Inspection

**بازرسی**

Inverter

**معکوس کننده ، اینورتر**

# L

Law of Absorption

**قانون جذب**

Lifecycle

**چرخه حیات**

Logic Circuit

**مدار منطقی**

Loops and Feedback

**حلقه ها و بازخورد**

# M

Maintenance

**تعمیر و نگهداری**

Mean

**متوسط**

Median

**میانه**

Minimal Cut Set

**مجموعه برش حداقل** - ترکیبی از رویدادهای اولیه است کـه بـرای وقـوع رویـداد رأس کفایـت می‌کنند. به این ترکیب در صورتی حداقل می‌گویند که برای وقوع رویداد رأس به رخداد تمامی رویدادهای شکست موجود در برش، نیاز باشد. یعنی اگر تنها یکی از این رویدادها حذف شـود، مسیر منتهی به وقوع رویداد رأس قطع گردد.

Mode

**مُد**

Moments about the Mean

**گشتاور حول میانگین**

Moments about the Origin

**گشتاور حول مبدأ**

Motor Operated Valve

**شیری که راه انداز آن یک موتور الکتریکی باشد**

Multiplication rule for probabilities

**قانون ضرب احتمالات**

Mutually exclusive

**مانع الجمع ، نامتداخل**

Mutually independent

**استقلال متقابل** – رویدادهایی که دو بدو مستقل باشند

# N

No Miracle Rule

**انتظار معجزه نداشتن**

Normalizing constant

**ثابت نُرم** - در نظریه احتمال ، ضرب ثابت نُرم در هر تابع غیر منفی ، باعث می شود تا سطح زیر منحنی آن برابر با عدد یک شود .بدین ترتیب می توان از آن تابع یک تابع چگالی احتمال ساخت . به عنوان مثال با توجه به رابطه انتگرالی زیر

$$\int_{-\infty}^{\infty} e^{-x^2/2}\,dx = \sqrt{2\pi}\,,$$

ثابت نُرم بدست آمده و می توان تابع نرمالیزه زیر را به عنوان تابع چگالی احتمال تعریف کرد .

که همان تابع چگالی احتمال نرمال استاندارد است .

$$\varphi(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2}$$

به همین ترتیب عبارت زیر یک ثابت نُرم برای تولید تابع چگالی احتمال گسسته پواسون است .

$$\sum_{n=0}^{\infty} \frac{\lambda^n}{n!} = e^{\lambda},$$

# P

Partition

**افراز**

Passive

**غیر فعال ، غیر عامل**

Pivotal events

**رویدادهای محوری** – رویدادهایی که بعد از یک رویداد آغازین قرار می گیرند .

Point Function

**تابع نقطه ای**

Posterior distribution

**توزیع تالی** – تابع توزیعی که از توزیع مقدم یک متغیر تصادفی بدست می آید . در نظریه احتمال و با استفاده از نظریه بیز ، می توان توزیع پیشنهادی ، مشاهده شده یا تخمینی یک

نمونه تصادفی را با ورود اطلاعات جدید ، تغییر داد و اصطلاحاً به روز کرد . به این تابع بـه روز شده ، تابع توزیع تالی می گویند .

Pressure Switch

کلید یا سوئیچ فشار - منظور از سوئیچ فشار در اصطلاح ابزاردقیق ، کلیدی است که با افـزایش یا کاهش فشار از یک مقدار از پیش تعیین شده ، با توجه به حالت پیش فرض آن ، باز یا بسته می شود

Prevention activities

**اقدامات پیشگیرانه**

Primary Event

**رویداد اولیه** - این رویدادها ، خطا یا شکست های آغازگر درخـت خطـا هسـتند و در مرزهـای تحلیل قرار گرفته اند و بیش از این بسط نخواهند یافت .

Prior distribution

**توزیع مقدم** – تابع توزیعی که براساس مشاهده یا آزمون های آماری بـه عنـوان اولـین حـدس برای یک نمونه تصادفی (مثلاً زمان بین شکست های یک قطعه) در نظر گرفته می شود .

Proactive

**پیش فعال**

Probabilistic Risk Assessment

**ارزیابی ریسک بر اساس احتمال** ، ارزیابی احتمالی ریسک – اشاره به یک روش عـام در ارزیـابی ریسک دارد که بر اساس محاسبات احتمال وقوع رویدادها می باشد .

Probability distribution

**توزیع احتمال**

Process Flow

**جریان(مواد در) فرآیند**

Product

**محصول**

Pump

**پمپ**

Pure event probability

**احتمال صرف رویداد**

# Q

Quality control

**کنترل کیفیت**

# R

Random variable

**متغیر تصادفی**

Ranking

**رتبه بندی**

Rare event approximation

**تقریب رویداد نادر** – منظور از رویداد نادر ، رویدادی است که به ندرت اتفاق می افتد .

Rayleigh distribution

**توزیع رایلی**

Re-assembly

**سوار کردن دوباره (قطعه)**

Reduced Ordered BDD

**دیاگرام تصمیم گیری دودوئی با رتبه کاهش یافته**

Regulating Rectifier

**یکسوساز قابل تنظیم**

Reliability

**قابلیت اطمینان ، قابلیت اعتماد**

Relief Valve

**شیر اطمینان**

Repair

**تعمیر**

Reset

**ری ست** – صفر کردن مجدد یک دستگاه یا وسیله دیجیتالی . مانند صفر کـردن مجـدد زمـان یک کرنومتر . در حالت کلی ریست کردن به معنای برگرداندن سیستم به تنظیمات اولیـه اش است .

Restructure

**بازسازی**

Risk Level

**سطح ریسک** – اصطلاحی است که نقطه عطف ارزیابی ریسک می باشد و حاصلضـرب احتمـال وقوع و شدت یک رویداد مخاطره آمیز می باشد .

Risk Matrix

**ماتریس ریسک** – ماتریسی است که برای ارزیابی کیفی ریسک مورد استفاده قرار مـی گیـرد . عموماً سطر های این ماتریس شدت پیامد یک جنبه (مانند ایمنی ، بهداشت و محیط زیسـت ) و ستون های آن احتمال وقوع یا تواتر آن ، بر اساس درجه های از پیش تعریف شده می باشد

ماتریس ریسک بر اساس این درجه بندی ، ناحیه بندی می شود . در یک ماتریس نمونه ، سه ناحیه ریسک به شرح زیر مشاهده می شود :

**ناحیه قابل قبول** (منطقه سبز) : مربوط به ریسک هایی است که مشکلی برای سیستم ندارند و یا خسارات و لطمات اندکی به سازمان وارد می کنند .

**ناحیه قابل تحمل** (منطقه زرد) : ریسک هایی با خسارات متوسط ولی قابل تحمل که بایستی با اقدامات کنترلی از شدت یا احتمال وقوع آنها کاست تا تبدیل به ریسک های قابل قبول شوند .

**ناحیه غیر قابل قبول** (منطقه قرمز) : این ریسک ها ، خسارات عمده ای به سازمان وارد می کنند و اعتبار آن را زیر سؤال می برند . ریسک هایی که منجر به کشته شدن افراد زیادی می شوند و یا آلودگی های زیست محیطی وسیعی را بدنبال دارند . بهر حال اینگونه ریسک ها هر چه سریعتر بایستی تحت کنترل قرار گرفته و اقدامات فوری برای آنها تعریف شود .

Root node

**گره ریشه**

Rupture

**ازهم گسیختگی ، ترکیدن**

# S

Safeguard

**پادمان ، حفاظ ایمنی** – وقتی سیستم به چالش کشیده می شود و یک عامل بالقوه آسیب رسان آن را تهدید می کند ، بایستی آمادگی مقابله با حوادث احتمالی را داشته باشد . پادمان ها در

واقع سپر بلای سیستم در برابر تلاطم و اغتشاشات احتمالی است . به عنوان مثـال مخـاطره ی اختلاف سطح (ارتفاع ) ، ممکن است منجر به رویداد مخاطره آمیز (پیامد) سقوط شـود . حـال برای مقابله با این پیامد ، ممکن است از وسایلی نظیر تـوری ایمنـی یـا حفـاظ هـای نـرده ای استفاده شود . به این وسایل پادمان یا حفاظ ایمنی می گویند .

Scale parameter

**پارامتر مقیاس** – پارامتری است که در یک تابع توزیـع احتمـال ، میـزان گسـتردگی توزیـع را مشخص می کند . یعنی هر چه پارامتر مقیاس بزرگتر باشد ، توزیع پهن تر و هر چه کوچک تر باشد ، متمرکز تر خواهد بود . به عنوان مثال در توزیع نرمال پارامتر مقیاس ، انحراف معیار ($\sigma$) است

Sensitivity analysis

**تحلیل حساسیت** – بررسی تاثیرپذیری خروجی یـک مـدل ریاضـی در اثـر دسـتکاری و تغییـر ورودی های آن

Set Function

**تابع مجموعه ای** - نگاشت یک مجموعه برروی بازه‌ای از اعداد ، تابع مجموعه‌ای نامیده شود.

Shape parameter

**پارامتر شکل** –پارامتری از یک توزیع احتمال است که نه بـه جابجـایی آن مربـوط مـی شـود (مانند پارامتر مکان) و نه به باریک و پهن بودن آن (مانند پارامتر مقیاس) . بلکه مستقیماً شکل

آن را معلوم می کنند . به عنوان مثال تابع نمایی پارامتر شکل ندارد چراکه شکل آن همواره یکسان است بلکه پهنای آن تغییر می کند و یا ممکن است توسط پارامتر مکان ، جابجا شود . در واقع اگر چولگی و درجه اوج یک توزیع ثابت باشد ، شکل آن تغییری نمی کند و فقط ممکن است باریک و پهن شود یا تغییر مکان دهد . چنین توزیعی پارامتر شکل ندارد . مثال دیگری از این نوع توابع ، توزیع یکنواخت و توزیع نرمال می باشد .

Sprinkler

**آب افشان ، اسپرینکلر** – یک نوع سیستم اطفاء حریق است که یا بصورت خودکار و یا دستی بکار می افتد و بوسیله پاشش آب ، آتش را خاموش می نماید .

Static Voltage Regulator

**تنظیم کننده ولتاژ ساکن**

Success

**موفقیت**

Sum of products approximation

**تقریب جمع حاصل ضرب ها**

Symbology

**نماد شناسی**

# T

Tank

**مخزن**

Test

**تست ، آزمون**

Timer relay

**رله زمان سنج**

Time-related

**مرتبط با زمان**

Times-to-failure

**زمان تا شکست**

Top Event

**رویداد رأس**

Top-down substitution

**جایگذاری از بالا به پایین**

Transfer Function

**تابع تبدیل** – برای سهولت در عملیات ریاضی ، از تبدیل لاپلاس برای نشان دادن نگاشت خطی خروجی بر روی ورودی متغیر با زمان استفاده می شود و به شکل زیر تعریف می گردد :

$$H(s) = \frac{Y(s)}{X(s)} = \frac{\mathcal{L}\{y(t)\}}{\mathcal{L}\{x(t)\}}$$

که در آن H(s) تابع تبدیل می باشد .

# U

Uncertainty

**عدم قطعیت** – این واژه کاربرهای زیادی در علوم مختلف نظیر فلسفه ، روان شناسی ، آمار ، اقتصاد ، امور مالی ، بیمه ، فیزیک ، جامعه شناسی ، مهندسی و فن آوری اطلاعات ، پیدا کرده است . بنا بر تعریف عدم قطعیت به معنای نداشت اطمینان و خاطرجمعی ، عدم توانایی شرح دقیق یک وضعیت یا پیش بینی آینده بدلیل داشتن دانش محدود ، می باشد .

Undeveloped Event

**رویداد توسعه نیافته** - این رویداد پایه ، حکایت از این دارد که بدلیل ناشناخته بودن توالی رویدادهای بعدی یا نداشتن اطلاعات کافی ، تحلیل گر قادر نیست یا نمی خواهد توالی شکست های بعدی این رویدادها را دنبال کند . ممکن است حتی علت بسط ندادن رویداد این باشد که بسط رویداد ، اطلاعات جدیدی به تحلیل اضافه نکند یا ادامه آن در ارزیابی ریسک مشابه ای آمده باشد .

Universal Set

**مجموعه مرجع**

Unreliability

**عدم اطمینان**

Utility

**سرویس های جانبی**

# V

Valve

**شیر**

Variance

**واریانس**

# W

Weibull Distribution

**توزیع وی بال** – یکی از مهم ترین توابع توزیع احتمال در مبحث مهندسی اطمینـان و ارزیـابی احتمالی ریسک می باشد . با تغییر پارامترهای این توزیع می توان تمامی اشکال تابع مخـاطره یک سیستم را در چرخه حیات آن بدست آورد . چرخه حیاتی که تولد ، کـارکرد و فرسـودگی سیستم را در بر می گیرد . تعریف ریاضی این تابع توزیع به شکل زیر می باشد :

$$f(x;\lambda,k)=\begin{cases}\frac{k}{\lambda}\left(\frac{x}{\lambda}\right)^{k-1}e^{-(x/\lambda)^k} & x\geq 0\\ 0 & x<0\end{cases}$$

که در آن ، $k > 0$ پارامتر شکل و $\lambda > 0$ پارامتر مقیاس توزیع است . با مقدار $k = 1$ ، توزیع فوق تبدیل به توزیع نمایی و با $k = 2$ تبدیل به تابع رایلی می گردد .

## فهرست تصاویر

## فهرست جداول