F T A

(Fault Tree Anlaysis)

تاریخچه FTA :

آنالیز درخت خطا (Fault Tree Analysis) توسط H.R. Watson در سال 1962 و درآزمایشگاه های تلفن Bell و به درخواست نیروی هوایی آمریکا برای مطالعات قابلیت اطمینان و ایمنی سیستم های موشکی بالستیک بین قاره ای طرح ریزی شد .

روش آنها برای تشریح و توصیف تجهیزات داده پردازی و همچنین تجزیه و تحلیل منطقی خطاهای آن مورد استفاده قرار می گرفت .

بعد از آن مهندسین شرکت بوئینگ از جمله David Haasl این روش را مورد بازنگری و توسعه داد .

امروزه این تکنیک بطور وسیع در آنالیز ایمنی مخصوصاً در سیستم های تولید انژری هسته ای کاربرد دارد.

تعریف :

آنالیز درخت خطا نموداری است تصویری و متشکل از کلیه علل منطقی که می تواند هر یک به تنهایی و یا مجموعاً منجر به یک حادثه نهایی گردد .

مثال هایی از حادثه نهایی (Top Event) می تواند به شرح زیر باشد :

1 ـ جراحت فرد

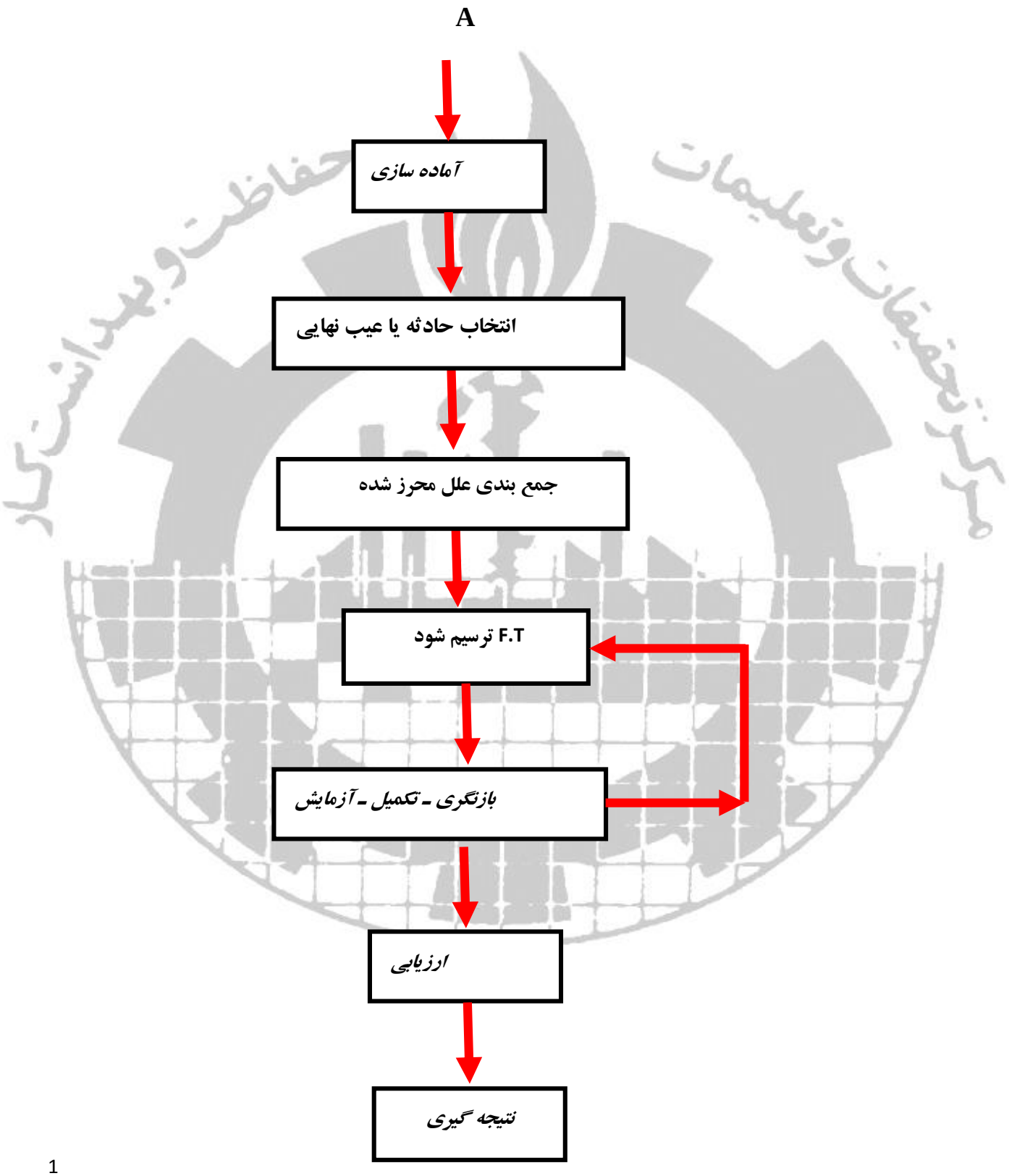
2 ـ بروز اشکال در تجهیزات

3 ـ نشت گاز سمی و مواد شیمیایی خطرناک

4 ـ توقف در سیستم تولید

مراحل انجام کار :

نمودار انجام یک FTA بصورت زیر است .



آماده سازی :

قبل از شروع به کار پیش شرط هایی باید جهت تجزیه و تحلیل ایمنی تعریف شود .

بدلیل اینکه ترسیم نمودار عیب یابی شامل تجزیه و تحلیل مفصل سیستم بوده و مجموعه وسیعی از فرضیات مورد نیاز می باشد . ابتدا باید انواع معایبی که می توانند رخ دهند را لیست نموده و در مورد حذف معایبی که از اهمیت خاصی برخوردار نیستند تصمیم گرفت .

انتخاب حادثه نهایی:

اولین گام در ترسیم نمودار عیب یابی انتخاب حادثه نامطلوبی است که باید تجزیه و تحلیل گردد و هدف ، جلوگیری از وقوع آن می باشد . به همین دلیل باید به درستی تعریف شود .

جمع بندی علل محرز شده:

هنگام ترسیم نمودار عیب یابی می بایست از دانش موجود در زمینه علل خرابی و عیب منجر به حادثه بهره جست . اگر بررسی های اولیه از معایبی که می توانند بروز نمایند بعمل آید تسریع در اجرای تجزیه و تحلیل پدید می آید . در این راستا می توان از نتایج تجزیه و تحلیل انحراف ها یا Hazop (بررسی مخاطرات بالقوه در فرآیندهای صنعتی) نیز بهره جست . این مطالب می تواند در ترسیم قسمتی از نمودار مورد استفاده قرار گیرد . پس از این مرحله یک فهرست از معایبی که می توانند در رخداد حادثه نهایی مؤثر باشد بدست خواهد آمد .

ترسیم نمودار عیب یابی :

ترسیم نمودار عیب یابی از حادثه نهایی یعنی از بالا به پایین شروع می شود . در ترسیم نمودار عیب یابی از علائمی استفاده می شود که برخی از آنها را در زیر شرح خواهیم داد .

الف : نماد AND ( )

نماد AND برای بیان حالتی استفاده می شود که رویداد خروجی در زمانی اتفاق می افتد که فقط و فقط باید همه رویدادهای ورودی اتفاق بیافتد .

ب ـ نماد OR: ( )

نماد OR برای بیان حالتی استفاده می شود که رویداد خروجی در زمانی رخ دهد که حداقل یکی از رویدادهای ورودی رخ دهند.

ج ـ نماد NOT ( )

نماد NOT برای بیان حالتی استفاده می شود که خروجی زمانی اتفاق می افتد که رویداد ورودی اتفاق نیافتد .

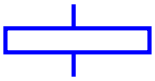
د ـ نماد رویداد اساسی ( )

یک رویداد اساسی ، رویدادی است که دیگر نتوان آنرا تجزیه نمود به عبارت دیگر این رویداد در پائین ترین سطح یک درخت قرار دارد و مسیر درخت به آن محدود می شود . این رویدادها می توانند خطاهای سخت افزاری ، فیزیکی . نرم افزاری ، شیمیایی ، خطاهای انسانی ، خطاهای سیستم و غیره باشند .

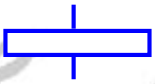
ه ـ رویداد نیمه تمام ( )

رویداد نیمه تمام یا توسعه نیافته رویدادی است که تجزیه بعدی آن در بهبود درک مساله نقشی نداشته باشد و یا اینکه در تحلیل فعلی نیاز به تجزیه آن نباشد . این رویداد شبیه رویداد

اساسی است ولی نماد آن متفاوت است . علت تفاوت این شکل با رویداد اساسی در این است که ممکن است رویداد توسعه نیافته در تحلیل های آینده توسعه داده شود .

و ـ رویداد میانی ( **)**

این رویداد معرف رویدادی است که در اثر خروجی نمادهای منطقی رخ می دهد . در واقع عیب منتج از یک نقص اساسی تر است.

ز ـ نقص شرطی ( **)**

این نقص می تواند بصورت عادی و طبیعی رخ دهد .

ک ـ نمادهای انتقال : (**)**

نمادهای انتقال جهت متصل کردن نواحی جداگانه یک درخت خطا استفاده می شوند . توجه شود که دو نماد انتقال وجود دارد . نوع اول زمانی است که تمام درخت رویداد در یک صفحه قرار نگیرد تا تحلیل گر بخواهد قسمتی از آن را در جای دیگری نمایش دهد . در اینصورت نماد انتقال به خارج را باید بکار برد . زمانیکه در صفحه مورد نظر بخواهند ادامه درخت رویداد را ارائه نمایند باید ابتدا نماد انتقال به داخل استفاده شود .

اولین گام این است که بررسی نماییم آیا حادثه نهایی از بیش از یک را ه مستقل می تواند رخ دهد یا نه ؟

اگر چنین باشد از دروازه OR استفاده نموده و نمودار را تقسیم بندی کرده و تجزیه و تحلیل به همین نحو از بالا به پایین ادامه خواهد یافت در اینجاست که باید به علل اساسی تر توجه نموده و می توان فهرست اولیه معایب که از قبل تهیه شده است نیز بهره جست .

بازنگری ــ تکمیل و آزمایش نمودار

ترسیم نمودار عیب یابی یک فرآیند سعی و خطا است و بهینه سازی آن د ر طی مراحل مختلفی باید صورت گیرد که در این راستا یکسری قوانین تجربی برای ادامه کار پیش بینی شده است . لازم به توضیح است که اعلام پایان کار بسیار مشکل است . در واقع نباید به هیچ وجه علل مهم بروز نقایص را نادیده انگاشت .

اولین کاری که باید انجام شود این است که ببینیم آیا تمام نکات در فهرست اولیه معایب که قبلاً تهیه شده است مدنظر قرار گرفته اند یا نه ؟

ارزیابی :

پس از ترسیم و تکمیل نمودار باید آن را مورد ارزیابی قرار داده و پس از تائید مورد بهره برداری قرار گیرد . بستگی به نوع هدف از تجزیه و تحلیل ، شماری از مراحل مختلف را می توان در این مرحله گنجانید .

الف ــ ارزیابی مستقیم حادثه نهایی :

نمودار ، تصویر فشرده ای است که می تواند از طرق مختلف منجر به حادثه نهایی شود . و همچنین تصویری از موانع موجود (توابع ایمنی) را در اختیار می گذارد . و نیز نشان می دهد که بعضی از نقایص و خطاها می توانند بصورت مستقیم به حادثه نهایی ختم شوند .

ب ــ تهیه فهرست کوچکترین زیر مجموعه ها :

زیر مجموعه ، شامل مجموعه ای از حوادث اساسی است که می تواند به حادثه نهایی منتج گردند .

کوچکترین زیر مجموعه ها ، زیر مجموعه ای است که خود زیر مجموعه دیگری ندارد . (حادثه اساسی)

ج ــ رده بندی رویدادهای اساسی :

از روی رویدادهای اساسی می توان احتمال رخداد حادثه را محاسبه نمود . داشتن اطلاعاتی در مورد احتمالات وقوع حادثه اولیه و یا برآورد آنها تسریع در کار می شود .

قواعد تجربی برای ترسیم F.T :

در هنگام ترسیم نمودار عیب یابی می توان قواعد تجربی زیر را مورد استفاده قرار داد .

1 ـ با در نظر گرفتن نواقص قابل قبول و واقعی کار کنید .

2ـ یک نقص را به حادثه دیگری که بیشتر واقعی و قابل قبول است بسط دهید .

3 ـ یک حادثه را به نقایص جزئی تر تقسیم کنید . (از دروازه های OR استفاده نمایید .)

4 ـ عللی را که با تاثیر متقابل بر هم باعث بروز حادثه می شوند را شناسایی کنید . (دروازه های AND)

5 ـ علت آغاز کننده حادثه را به فقدان یک عامل ایمنی ربط دهید .

6 ـ بطور مکرر زیر گروه ایجاد کنید .

7 ـ برای هر دروازه عنوان مشخص قائل شوید .

8 ـ فرضیات باید صحیح باشند و بر اساس پیش داوری نباشند .

9 ـ بصورت منطقی فکر کنید و بصورت ساختاری و اصولی عمل کنید و علت و معلول را از هم تفکیک کنید .

10 ـ گهگاه منطق نمودار را هنگام ترسیم کنترل کنید . از نقایص اولیه زیرین شروع کنید و فرض کنید که همهٔ آنها اتفاق افتاده اند . ببینید چه اتفاقی در بر دارد ؟

مزایای FTA :

1 ـ این روش کمکی است به منظور شناسایی مخاطرات در سیستمهای پیچیده

2 ـ از این روش می توان برای تجزیه و تحلیل خطاهای انسان و تجهیزات استفاده کرد .

3 ـ این روش وسیله ای است که تمرکز روی یک عیب را همزمان (بدون از دست دادن تصویر و نمای کلی خطرات) انجام می دهد .

4 ـ این روش چشم اندازی را ایجاد می کند که نشان می دهد معایب چگونه می توانند منتج به عواقب جدی تر و خطرناک تر شوند .

5 ـ این روش کمی و کیفی است و امکان برآوردهای احتمالی یک عیب یا حادثه را فراهم می کند .

معایب FTA :

1 ـ نیازمند داشتن اطلاعات جامع و تخصصی از سیستم است .

2 ـ برای سیستم های بزرگ و حجیم به راحتی قابل استفاده نیست .

3 ـ این روش وقت گیر و نسبتاً مشروح و کلی است .

4 ـ تکمیل و اجرای این روش نیاز به مدارک مشروح و مستند دارد که باید در دسترس باشد .

تحلیل کمی درخت خطا :

در تحلیل کمی درخت خطا احتمال و فرکانس حوادث نهایی و رویدادهای نامطلوب محاسبه می شود.

همچنین احتمال وقوع هر کدام از رویدادهای اساسی مورد بررسی قرا می گیرد .

برای انجام این تحلیل، اطلاعات مربوط به قابلیت اطمینان از قبیل احتمال خطا ، نرخ خطا ، نرخ تعمیر و غیره نیاز می باشد .

اطلاعات مربوط به رویدادهای اساسی از تحلیل کیفی بدست می آیند. در تحلیل درخت خطا به علت آنکه تحلیل بر روی خطر (یا خطا) صورت می پذیرد از مقادیر عدم قابلیت اطمینان و عدم قابلیت در دسترس بودن استفاده می شود .

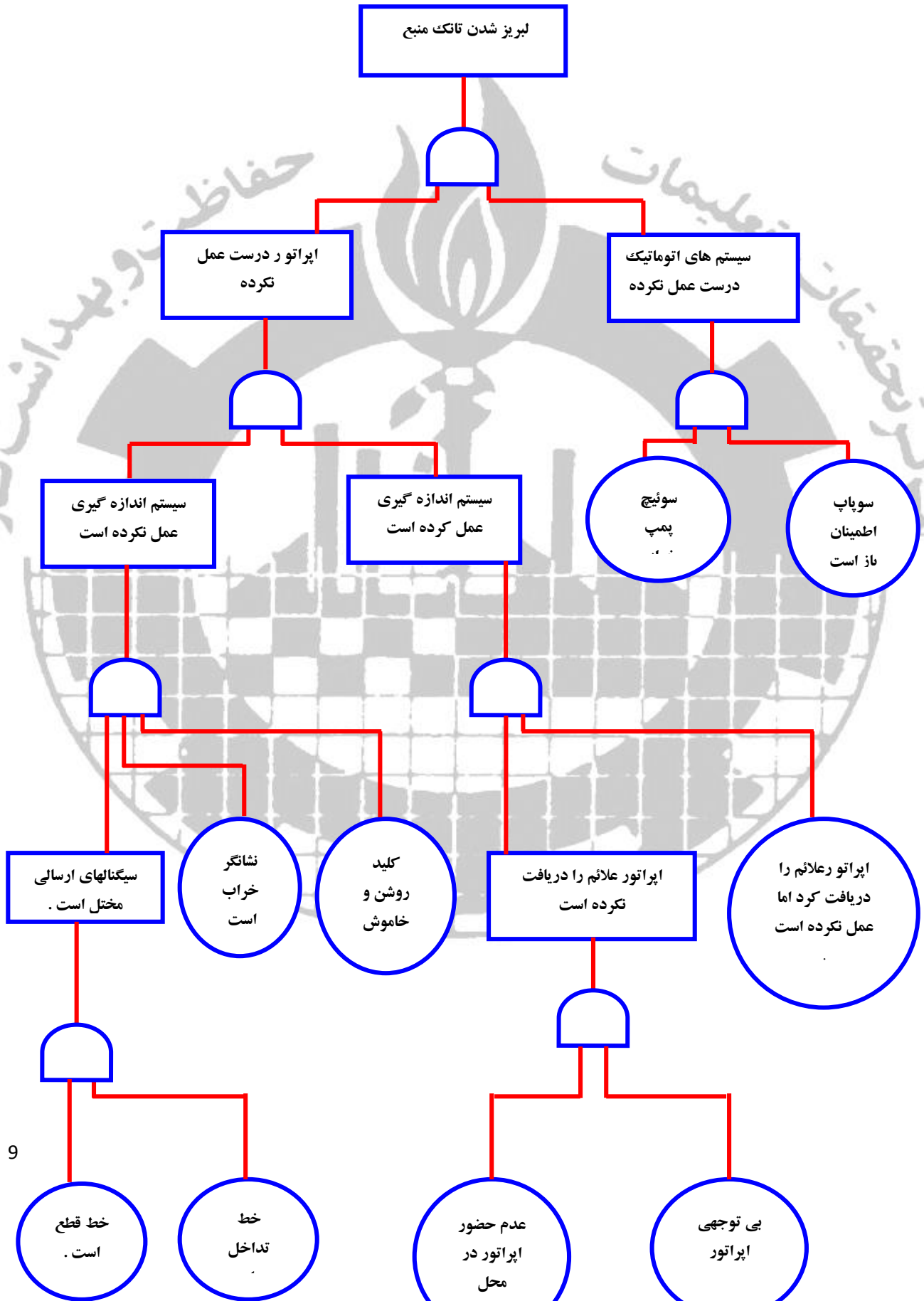
بررسی کمی احتمال رخ دادن حادثه نهایی در درخت خطا به طور ساده به دو صورت انجام می گیرد .

در راه اول از جبر بول و ساختار منطقی درخت خطا برای ترکیب رویدادهای اساسی استفاده می شود و در روش دوم از قواعد احتمال و ساختار منطقی درخت خطا برای ترکیب و الحاق رویدادهای اساسی استفاده می شود

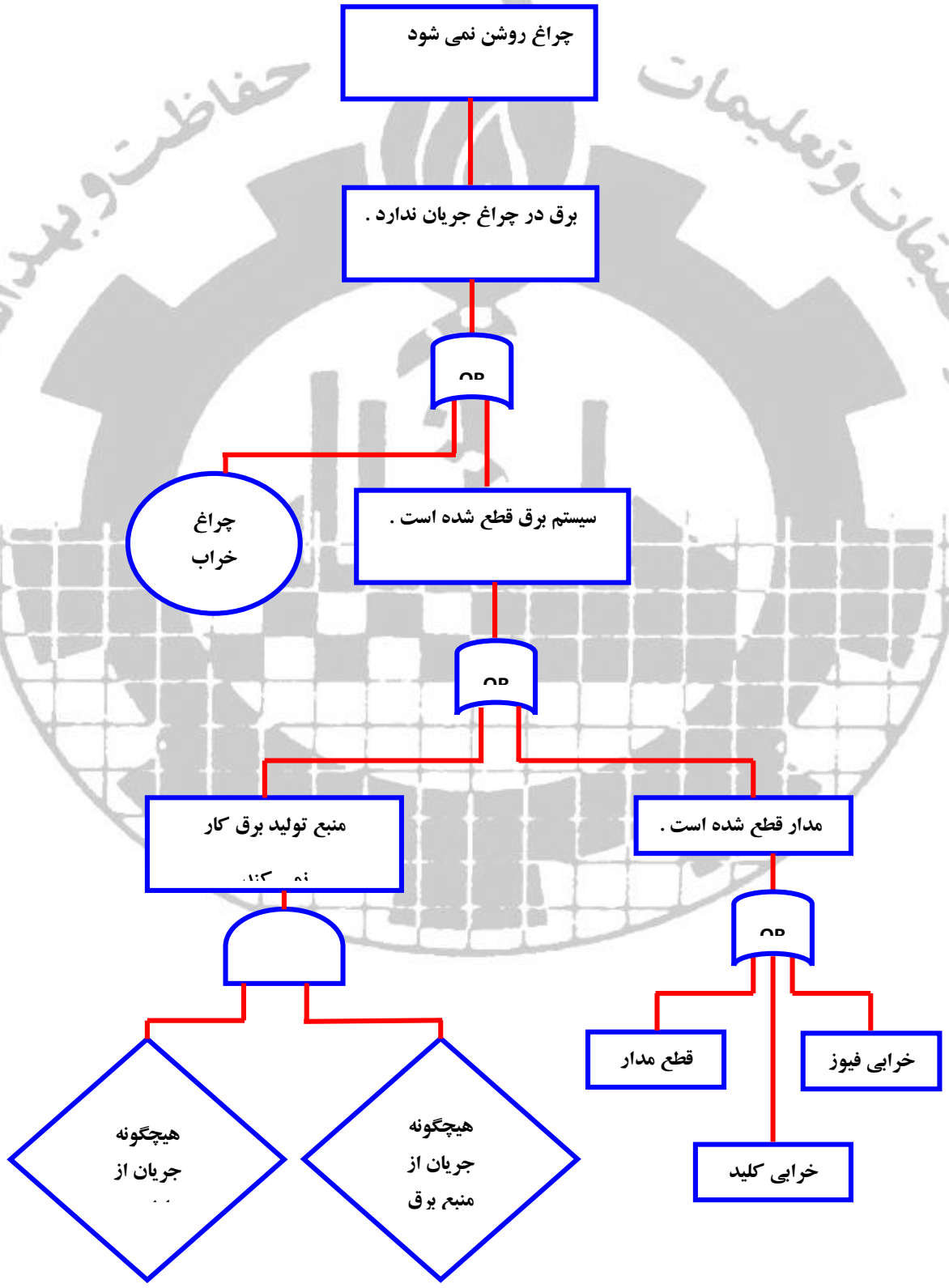
مثال :

حادثه یا نقص نهایی در اینجا روشن نشدن لامپ می باشد این بدلیل عدم جریان برق از لامپ می باشد که می تواند بدلیل خرابی خود لامپ باشد و یا اینکه هیچ جریان برقی به آن وصل نباشد . جریان برق فقط در صورت ساقط شدن هر دو واحد تغذیه برق و باطری قطع می گردد . نمودار شامل سه نقص اساسی و سه عیب توسعه نیافته است .

معیوب بودن فیوز می تواند بعلت فرسودگی و یا علل دیگر باشد اما این امکان هم وجود داراد که فیوز over loadکرده باشد (بار زیادی از مدارعبور کرده باشد) که می تواند در نتیجه ایجاد یک اتصال کوتاه موقتی در مدار متصل به لامپ اتفاق افتاده باشد . به همین صورت در مورد اینکه چرا جریان از واحد تولید برق یا باطری تامین نمی شود می توان بررسی ها را ادامه داد.


لبریز شدن تانک منبع
اپراتو ر درست عمل نکرده
سیستم های اتوماتیک درست عمل نکرده
سیستم اندازه گیری عمل نکرده است
سیستم اندازه گیری عمل کرده است
سوئیچ پمپ
سوپاپ اطمینان باز است
سیگنالهای ارسالی مختل است .
نشانگر خراب است
کلید روشن و خاموش
اپراتور علائم را دریافت نکرده است
اپراتو رعلائم را دریافت کرد اما عمل نکرده است
خط قطع است .
خط تداخل
عدم حضور اپراتور در محل
بی توجهی اپراتور

مثال 2 : **Risk Management Haim's**



Sooner than	باز کردن درب کوره قبل از تنظیم فشار.	انفجار کوره	خطای اپراتور	استفاده از علائم هشدار دهنده آموزش اپراتور نظارت کامل	واحد مهندسی
More than	فشار بیش از حد طراحی است .	انفجار کوره	خطای اپراتور خطای گیج خطای اطلاعات داده شده	برنامه نت نظارت کامل یک متخصص بر کوره	واحد نت واحد مهندسی و طراحی
Less than	وزن فلز درون بوته کمتر از یک تن است .	تنها میزان مذاب تولیدی را کاهش می دهد .			
More than	وزن فلز درون بوته بیش از یک تن است .	ریزش و سرریز شدن مذاب درون کوره	عدم رعایت اپراتور خرابی دستگاه (کالیبره نبودن)	آموزش و توجیه اپراتور برنامه کالیبراسیون دقیق	سرپرست واحد تضمین کیفیت
کلمه راهنما	**انحراف**	**اثرات ونتایج**	**علل**	**اقدامات اصلاحی وپیشنهادی**	**مسئولیت / تاریخ بازنگری**
HAZOPانسان **شخص مورد مطالعه :** اپراتور کوره **زمان مورد مطاله :**					
مثال Hazop انسان : یک اپراتور کوره را در نظر بگیرید .وظیفه اپراتور می بایست بوته حاوی فلز را به میزان یک تن پر کرده و به داخل کوره هدایت نماید و بوته حاوی فلز را به میزان یک تن پر کرده و به داخل کوره هدایت نماید . توزین توسط یک باسکول مجاور کوره انجام می گیرد . بعد از مدت 30 دقیقه اپراتور می بایست فشار کوره را تنظیم کرده و بوته را خارج سازد . هدف بررسی انحرافات اپراتور از وظیفه محوله با کمک روش Hazop است .					

Un successful	نمایان نبودن علامت مشخصه بشکه ها	انفجار و آسیب شخصی	کاربرد اشتباه علم تشخیص پرسنل کارخانه	استفاده از علائم هشدار دهنده استفاده از علائم شناسایی	واحد آتش نشانی سرپرست
Un clear	دمای مطلوب مبهم است	انفجار و آسیب شخصی	نگهداری بشکه ها در انبار مسقف نگهداری بشکه ها در	نگهداری بشکه ها در هوای آزاد و دور از منابع تولید جرقه	مدیر کارخانه سرپرست
Omitted	چیدمان بشکه ها نامشخص است (از نظر افقی یا عمودی)	سقوط بشکه و انفجار	عمودی قرار دادن بشکه ها روی هم	چیدمان افقی و عمودی مشخص شود	واحد تضمین کیفیت سرپرست
کلمه راهنما	**انحراف**	**اثرات ونتایج**	**علل**	**اقدامات اصلاحی وپیشنهادی**	**مسئولیت / تاریخ بازنگری**
HAZOP رویه **شخص مورد مطالعه :** دستورالعمل انبارش و نگهداری بشکه های تینر **زمان مورد مطالعه :**					
مثال **Hazop** رویه : دستور العمل انبارش بشکه های حاوی تینر به این صورت تهیه شده است . **1** _ قرار دادن بشکه ها روی هم تا سه ردیف **2** _ نگهداری بشکه ها در دمای مطلوب **3** _ شناسایی بشکه ها به وسیله نوشتن کلمه تینر روی بشکه ها					