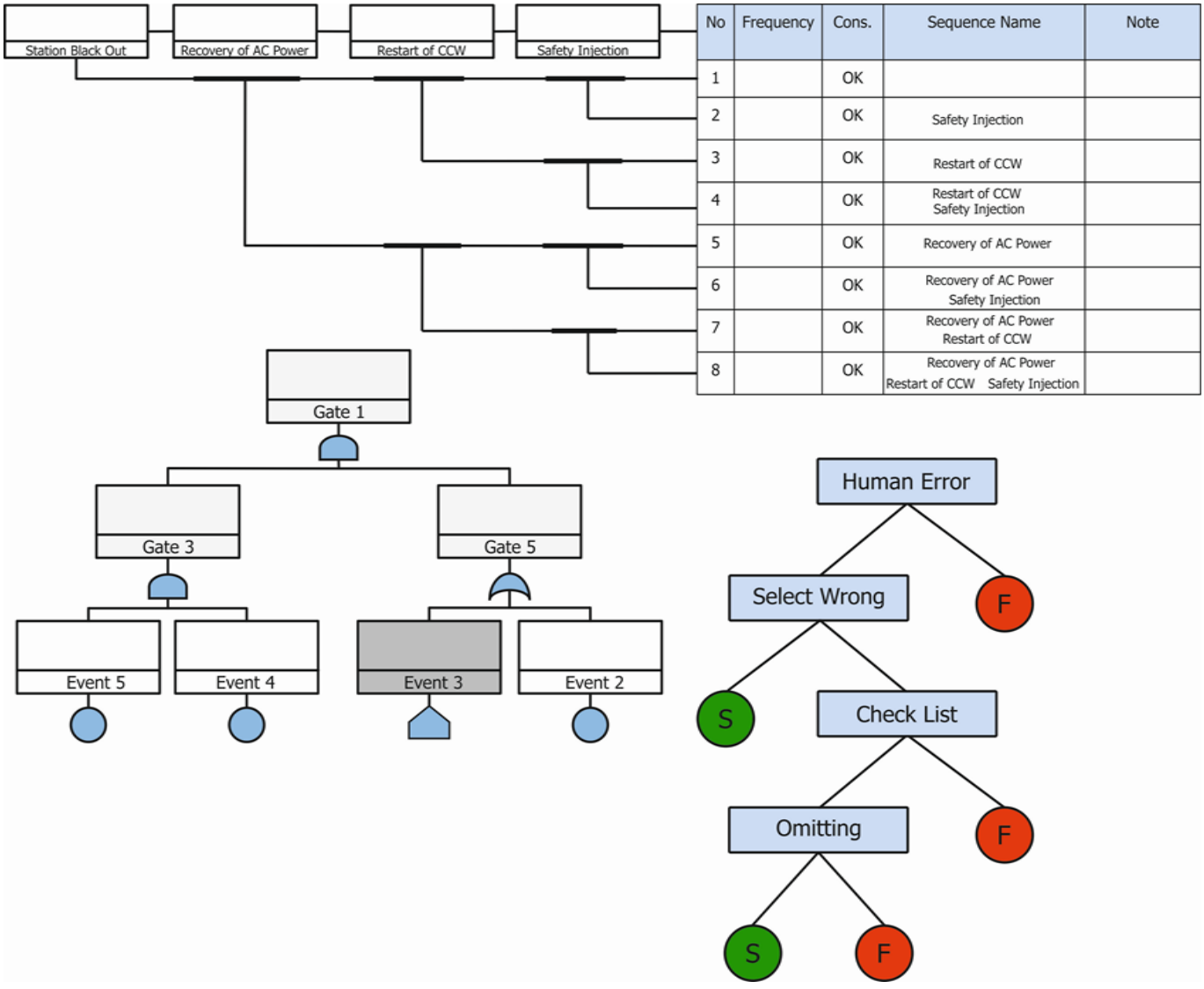
مبانی تحلیل ایمنی احتمالاتی



No	Frequency	Cons.	Sequence Name	Note
1		OK		
2		OK	Safety Injection	
3		OK	Restart of CCW	
4		OK	Restart of CCW Safety Injection	
5		OK	Recovery of AC Power	
6		OK	Recovery of AC Power Safety Injection	
7		OK	Recovery of AC Power Restart of CCW	
8		OK	Recovery of AC Power Restart of CCW Safety Injection	

شناسه مدرک: 1401-ANCC-PUB-03-01
تاریخ انتشار: ۱۴۰۱/۱۲/۱۰

www.ancc.ir
info@ancc.ir

«بسم الله الرحمن الرحیم»

درباره مرکز

مرکز محاسبات پیشرفته هسته‌ای (ANCC) در سال ۱۳۸۹ به دستور رییس محترم وقت سازمان انرژی اتمی ایران و با مسئولیت شهید بزرگوار دکتر مجید شهریاری آغاز به کار نمود. در سند چشم‌انداز ۲۰ ساله مرکز، اهداف و مأموریت‌های زیر برای این نهاد در نظر گرفته شده است:

- توسعه و تأمین نرم‌افزارهای حرفه‌ای مورد نیاز برای صنعت هسته‌ای کشور؛
- پرورش نیروی انسانی مورد نیاز برای توسعه و کاربری نرم‌افزارهای هسته‌ای در کشور؛
- فراگیری روش‌های محاسباتی نوین و پیاده‌سازی آن‌ها در نرم‌افزارهای هسته‌ای؛
- آموزش کاربری نرم‌افزارهای هسته‌ای با برگزاری کارگاه‌های آموزشی؛
- ایجاد پایگاهی از نرم‌افزارها و داده‌های هسته‌ای و به‌روز نگهداشتن آن‌ها؛
- راستی‌آزمایی و اعتبارسنجی نرم‌افزارهای هسته‌ای و پیگیری دریافت پروانه بهره‌برداری از مراجع قانونی؛
- تبدیل شدن به یک مرجع ملی در زمینه کدهای هسته‌ای؛
- همکاری با دانشگاه‌ها و مراکز صنعتی و پژوهشی؛

این مرکز امیدوار است که با توکل بر پروردگار متعال و با تکیه بر توان‌مندی کارشناسان و مدیران خود در سایه حمایت‌های سازمان انرژی اتمی ایران به اهداف یادشده دست‌یافته و کشور را به ترازی از دانش محاسبات پیشرفته هسته‌ای برساند که شایسته آن است.

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

چکیده

به منظور اشراف بر مباحث مختلف ایمنی، به‌روزرسانی دانش فنی موجود و نیز ارائه مستندات و گزارش‌هایی با رویکرد آموزشی، فعالیت‌هایی در برنامه جامع ایمنی در نظر گرفته شده است. در این سند، به موضوع تحلیل ایمنی احتمالاتی پرداخته شده است و حاوی مطالبی از جمله آشنایی با تحلیل ایمنی احتمالاتی و مفاهیم اصلی آن، معرفی مقولهٔ ریسک، قابلیت اطمینان، ابزارهای تحلیل ایمنی شامل درخت خطا و درخت رویداد، خرابی عامل مشترک، تحلیل مودهای خرابی و اثرات آنها، تحلیل لایه‌های حفاظت به همراه ضمیمهٔ اصول و اهداف ایمنی هسته‌ای می‌باشد. این گزارش به عنوان گزارش اولیه شامل مطالب اصلی ایمنی احتمالاتی در راستای تدوین یک مدرک جامع می‌باشد که در آینده بر جزئیات و تفصیلات آن افزوده خواهد شد.

کلیدواژه

تحلیل ایمنی احتمالاتی، ریسک، قابلیت اطمینان، درخت خطا، درخت رویداد، خطای انسانی، خرابی عامل مشترک، تحلیل مود خرابی، لایه‌های حفاظت، اصول ایمنی.

اختصارات

عبارت اصلی	اختصار	عبارت اصلی	اختصار
HAZard and Operability Analysis	HAZOP	Probabilistic Safety Assessment	PSA
Failure Mode and Effects Analysis	FMEA	Probability Risk Assessment	PRA
Preliminary Hazard Analysis	PHA	Fault Tree Analysis	FTA
Screening Level Risk Analysis	SLRA	Event Tree Analysis	ETA
Failure Mode and Effects Criticality Analysis	FMECA	Common Cause Failure	CCF
Layer Of Protection Analysis	LOPA	Probability Distribution/Density Function	PDF
Probability of Failure on Demand	PFD	Cumulative Distribution Function	CDF

۱- مقدمه‌ای در زمینهٔ نقشهٔ کلان تحلیل ایمنی احتمالاتی و مفاهیم اصلی آن

تحلیل ایمنی احتمالاتی روشی با زبان احتمالات برای پیش‌بینی عملکرد (موفقیت یا عدم موفقیت) یک سیستم در اثر مخاطرات اجتناب‌ناپذیر، بر اساس داده‌های آماری بدست آمده در طول زمان است. این بیان شامل مفاهیمی مانند سیستم، خرابی، مخاطرات، ریسک، قابلیت اطمینان، حوادث، داده‌های آماری، محاسبات احتمالاتی و ... است. در بخش اول این گزارش، مقدمه‌ای در زمینهٔ تحلیل ایمنی احتمالاتی شامل ابزارها و مفاهیم اصلی و نیز تعریف اصطلاحات رایج در آن ارائه می‌شود. در بخش دوم به تحلیل ریسک پرداخته شده است که شامل اجزای ریسک، مراحل ارزیابی، مدیریت ریسک و انواع آن است. بخش سوم مربوط به مبحث مهندسی قابلیت اطمینان و ایمنی است که شامل تاریخچه، دلیل نیاز به مهندسی قابلیت اطمینان و ایمنی، خرابی‌های اجتناب ناپذیر، روش‌های ارتقای قابلیت اطمینان، چالش‌های موجود، ریاضیات پایه در قابلیت اطمینان، تحلیل داده‌های خرابی، مدل‌های قابلیت اطمینان و خرابی و روش‌های مدل‌سازی قابلیت اطمینان می‌باشد. در فصل چهارم ابزارهای تحلیل ایمنی احتمالاتی شامل درخت خطا و درخت رویداد معرفی شده‌اند. مبحث خرابی عامل مشترک به صورت تفصیلی در فصل پنجم ارائه شده است. فصل ششم و هفتم به ترتیب شامل مباحث تحلیل حالت‌های خرابی و اثرات آنها و تحلیل لایه‌های حفاظتی است. در این گزارش سعی شده است مطالب اصلیِ جامعی از مباحث تحلیل ایمنی احتمالاتی ارائه شود.

۱-۱- ابزارهای اصلی تحلیل ایمنی احتمالاتی

در فرایند تحلیل ایمنی احتمالاتی، ابتدا مخاطراتی که سیستم با آنها مواجه است، شناسایی می‌شوند و رویدادهای آغازگرِ حوادث تهدید کنندهٔ سیستم تعیین می‌شوند. پس از آن با لحاظ عملکرد تمهیدات ایمنی که به عنوان سدهای دفاعی در برابر مخاطرات در طراحی سیستم لحاظ شده‌اند، سناریوی حادثه توسعه می‌یابد و حالت‌های مختلف ممکن شناسایی می‌شوند. در ادامه، پیامد هر یک از حالت‌های مختلف حادثه تعیین می‌شود. این اقدامات توسط ابزار درخت رویداد انجام می‌شود. احتمال خرابی برای هر یک از اجزا و سیستم‌های ایمنی، به خصوص سیستم‌های پیچیده، به روشنی مشخص نیست و نیاز به ابزاری است که با کمک آن، ترکیب حالت‌های ممکن منجر به خرابی سیستم استخراج و احتمال خرابی کل سیستم محاسبه می‌شود. این ابزار، درخت خطا است.

۱-۲- مفاهیم اصلی تحلیل ایمنی احتمالاتی

۱-۲-۱- خطای انسانی

یکی از عوامل خرابی سیستم می‌تواند ناشی از خطای انسانی باشد. قابلیت اعتماد انسانی به صورت احتمال اینکه یک فرد، اولاً عملکرد مورد نیاز برای یک سیستم را در یک بازهٔ زمانی مشخصی با موفقیت انجام دهد و ثانیاً هیچ اقدام اضافی دیگری که عملکرد سیستم را دچار اختلال می‌کند، انجام ندهد. تحلیل قابلیت اعتماد انسانی، فرایند مورد استفاده در تخمین میزان قابلیت اعتماد انسانی است که معمولاً در چهارچوب یک تحلیل جامع‌تر، مانند تحلیل ایمنی احتمالاتی، انجام می‌شود. پس از تجزیهٔ یک وظیفه به عناصر تشکیل دهندهٔ آن و پیش از آنکه مقادیر احتمال مربوط به هر عنصر محاسبه و تعیین شوند، این عناصر در یک درخت دودویی که درخت رویداد تحلیل قابلیت اعتماد انسانی نامیده می‌شود، قرار داده می‌شوند. این درخت رویداد، روند منطقی انجام وظیفهٔ عناصر مختلف توسط اپراتورها را نمایش می‌دهد.

برای تحلیل خطای انسانی، ابتدا باید یک رویداد پایه از نوع خطای انسانی در یک درخت خطا ایجاد شود. از طریق تحلیل خطای انسانی، کاربر می‌تواند وظیفهٔ اپراتور را تحلیل کرده، برای آن درخت دودویی رسم کند و در نهایت احتمال محاسبه شده در این تحلیل، به عنوان احتمال خرابی رویداد پایه در درخت خطا مورد استفاده قرار گیرد. کاربرد دیگر تحلیل خطای انسانی به این شکل است که مستقل از تحلیل درخت خطا، یک تحلیل خطای انسانی به صورت مستقیم ایجاد شده و تحلیل وظیفه و محاسبه احتمال خطای اپراتور برای آن انجام شود. البته خطای انسانی ایجاد شده در این تحلیل نیز می‌تواند بعداً در تحلیل درخت خطا یا درخت رویداد مورد استفاده قرار گیرد. بنابراین، تحلیل خطای انسانی معمولاً به عنوان بخشی از یک تحلیل کلی ایمنی مانند تحلیل ایمنی احتمالاتی یک نیروگاه هسته‌ای انجام می‌شود و نتایج حاصل از تحلیل خطای انسانی در ترکیب و ارتباط با تحلیل قابلیت اعتماد سیستم و خرابی‌های سخت‌افزاری است که قابل تفسیر و استفاده است.

۱-۲-۲- خرابی عامل مشترک

خرابی اجزای مختلف در اثر عامل مشترک، یکی از مهم‌ترین مباحث در ارزیابی قابلیت اطمینان یا عدم دسترسی یک سیستم است. مدل‌سازی یک خرابی با عامل مشترک و حضور آن در ساختار درخت خطا یکی از مهم‌ترین ارکان در تحلیل ایمنی احتمالاتی است. خرابی‌های عامل مشترک، که زیرمجموعه‌ای از کلاس عمومی رویدادهای وابسته است، به صورت خرابی‌های چندگانه اجزا در اثر علت ریشه‌ای مشترک تعریف می‌شوند. مشخصهٔ کلیدی یک رویداد با عامل مشترک این است که دو یا چند جزء باید با یک علت مشترک مورد اصابت قرار گیرند، به طوری که آن علت، نباید خرابی یا عدم دسترسی عملکردی

جزء دیگر باشد. جایگاه مفهوم خرابی عامل مشترک در رویدادهای پایهٔ درخت‌های خطا می‌باشد. خرابی‌های عامل مشترک لحاظ شده در درخت خطا، شامل وابستگی اجزای داخلی سیستم است که اهمیت بالقوّه‌ای برای آنها لحاظ نمی‌شود و مکانیزم‌های آنها به صورت صریح در مدل درخت خطا اشاره نشده است. به عبارت دیگر، خرابی‌های عامل مشترک، یک کلاس مهم از رویدادهای وابسته با لحاظ سهم آنها در عدم دسترسی سیستم است. تحلیل‌های سیستم‌هایی که تنها خرابی‌های مستقل تصادفی را لحاظ می‌کنند، منجر به تخمین ناچیز عدم دسترسی شده و شناخت نادرستی از مزایای افزونگی و تنوع در طراحی سیستم به بار می‌آورد.

۱-۲-۳- عدم قطعیت

تحلیل عدم قطعیت مفهومی است که در تحلیل درخت خطا به کار می‌رود. در تحلیل عدم قطعیت، به‌جای مقدار نقطه‌ای محاسبه شده از تحلیل کمّی درخت خطا، با فرض یک توزیع برای مقدار نرخ خرابی رویدادهای پایه، یک توزیع احتمال برای رویداد رأس درخت خطا محاسبه می‌شود. مبنای این تحلیل شبیه‌سازی به روش مونت کارلو است.

۱-۲-۴- حساسیت

تحلیل حساسیت، تأثیر انتخاب یک مدل یا پارامترهای آن، فرضیات به کار رفته برای یک سد ایمنی، یک پدیده یا مخاطره، عملکرد سدهای ایمنی، شدت مخاطرات، و اهمیت هر متغیر ورودی غیرقطعی را شناسایی می‌کند. فرایند تحلیل حساسیت یک فرایند مستقیم است. اثرات متغیرهای ورودی و فرضیات در تحلیل ایمنی احتمالاتی، با تغییر چندبارهٔ آنها و مشاهدهٔ اثر این تغییرات بر نتایج، اندازه‌گیری می‌شود. این مدل‌ها، متغیرها و فرضیات، که تغییر آنها منجر به بالاترین تغییر در نتایج می‌شوند، به عنوان عوامل «حساس» شناسایی می‌شوند. در این هنگام، برای کاهش عدم قطعیت‌های ناشی از المان‌های حساس در تحلیل ایمنی احتمالاتی باید فرضیات، مدل‌ها، مکانیزم‌های خرابی بیشتر و داده‌های خرابی اضافی بازنگری شوند.

تحلیل حساسیت کمک می‌کند تا تمرکز منابع و توجهات به المان‌هایی از تحلیل ایمنی احتمالاتی معطوف شود که نیاز به توجه و مشخصات بیشتری دارند. یک تحلیل حساسیت خوب، کیفیت و اعتبار نتایج تحلیل ایمنی احتمالاتی را تقویت می‌کند. معمولاً اجزایی از تحلیل ایمنی احتمالاتی که می‌توانند اثرات چندگانه بر نتایج نهایی داشته باشند، شامل پدیده‌های خاص (مانند حفره‌های ناشی از خوردگی در بتن یا فلز، ترک‌های ناشی از خستگی و خرابی‌های عامل مشترک) و فرضیات غیرقطعی، عواملی هستند که نیازمند تحلیل حساسیت می‌باشند.

۱-۲-۵- اهمیت

یکی از جنبه‌های ویژهٔ رویداد پایه، میزان سهم آن رویداد در احتمال رویداد رأس یک درخت خطا است که به آن میزان اهمیت گفته می‌شود. تعیین میزان سهم قابلیت اطمینان یک جزء از سیستم در قابلیت اطمینان کل سیستم، اهمیت آن جزء را تعیین می‌کند. از دید خرابی نیز، احتمال اینکه خرابی یک جزء بتواند منجر به خرابی سیستم شود، میزان اهمیت آن جزء در سیستم را تعیین می‌کند. این نوع از تحلیل، منجر به بهینه‌سازی سرمایه‌گذاری از جنبهٔ ارتقای قابلیت اطمینان سیستم می‌شود. تحلیل اهمیت شامل دو نوع تحلیل اهمیت ساختاری و تحلیل اهمیت احتمالاتی می‌باشد. در تحلیل اهمیت ساختاری، بدون لحاظ داده‌های احتمالاتی، میزان نقش و اهمیت ساختاری یک جزء در سیستم مورد نظر است و در تحلیل اهمیت احتمالاتی، میزان اهمیت جزء با لحاظ داده‌های احتمالاتی (احتمال خرابی) در احتمال خرابی کل سیستم تعیین می‌شود. این مفهوم نیز، در ابزار درخت خطا مطرح می‌شود و در نرم‌افزارهای تحلیل ایمنی احتمالاتی، قابلیت تحلیل اهمیت طراحی شده است.

تحلیل‌های کمّی درخت‌های خطا ابتدا شامل محاسبهٔ احتمال هر مجموعهٔ برشی کمینه و احتمال رویداد رأس است که در آن مجموعه‌های برشی غالب تعیین شده و رویدادهای پایهٔ مهم و مؤثر در رویداد رأس، شناسایی می‌شوند. مطالعات حساسیت و انتشار عدم قطعیت، اطلاعات کلیدی بیشتری فراهم می‌آورند. شناسایی رویدادهای پایهٔ مهم برای اتخاذ تصمیم در تخصیص منابع بسیار مفید است. پایش، نگهداری و جایگزینی می‌تواند بر رویدادهای بحرانی برای مدیریت مؤثر هزینهٔ قابلیت اطمینان یا ریسک، متمرکز شود.

۱-۳- واژه شناسی

مخاطره/خطر (hazard): یک مشخصهٔ ذاتی که پتانسیل منجر شدن به آسیب به جامعه، خواص و یا محیط داشته باشد.

ریسک (risk): ریسک یک کمیت چندعاملی است که خطر، آسیب و احتمال پیامدهای مضر مرتبط با یک رویداد واقعی یا بالقوهٔ مورد نظر را بیان می‌کند. ریسک به کمیت‌هایی مانند احتمال وقوع یک رویداد خاص و اندازه و مشخصات پیامدهای آن وابسته است. به عبارت دیگر، مقیاسی از پیامد یک خطر و فرکانس احتمالی وقوع آن است. ریسک با زبان ریاضی به صورت زیر تعریف می‌شود:

RISK = Consequence * Frequency of Occurrence

ریسک کلی از حاصل‌جمع ریسک‌های انفرادی برای رویدادهای مستقل قابل حصول است.

ایمنی (safety): ایمنی، قضاوتی از قابلیت پذیرش ریسک است. فعالیتی ایمن قلمداد می‌شود که ریسک‌های آن در قیاس با سایر فعالیت‌های روزانه عمومی، قابل قبول ارزیابی شود. هیچ فعالیتی به‌طورکلی عاری از ریسک نیست، ولی می‌توان با استفاده از اقدامات حفاظتی کافی، ریسک را به سطوح قابل قبول کاهش داد. ایمنی به صورت ظرفیت یک واحد در عدم اجازهٔ وقوع آسیب به افراد در شرایط و زمان مشخص تعریف می‌شود. یک سیستم ایمن است، درصورتی‌که هم‌زمان:

- بهره‌برداری اشتباه در آن رخ ندهد و یا پیامد مضر نداشته باشد،
- با استفاده از تجهیزات، مخاطره‌ای وجود نداشته و یا ایجاد نشود.

مهندسی ایمنی و قابلیت اطمینان (Safety Engineering and Reliability): مهندسی ایمنی و قابلیت اطمینان تلاش می‌کند تا خرابی، تعمیر و پیامدهای خرابی سیستم‌ها را به منظور ارتقای عملکرد آنها مطالعه، توصیف، اندازه‌گیری و تحلیل نماید. این کار با افزایش عمر طراحی، حذف یا کاهش احتمال خرابی‌ها و پیامدهای آنها و کاهش زمان غیرفعال بودن یک تأسیسات و درنتیجه افزایش زمان عملکرد در دسترس با کمترین هزینه‌های ممکن در طول عمر انجام می‌شود. قابلیت اطمینان با مفهوم خرابی مرتبط است، درحالی‌که ایمنی با پیامدهای بعد از خرابی مرتبط است.

کیفیت (Quality): سازمان استاندارد بین‌المللی (ISO 3534) کیفیت را به صورت «کفایت اجزا و مشخصات یک محصول یا خدمات مربوط به قابلیت آن محصول برای برطرف کردن نیازمندی‌های تعیین شده و یا ضمنی» تعریف می‌کند. این تعریف مبتنی بر موارد زیر است:

- کیفیت مطلق نیست، بلکه بر اساس نیازمندی‌ها و یا مشخصات تعریف شده قضاوت می‌شود.
- کیفیت یک کمیتِ فیزیکی قابلِ اندازه‌گیری نیست. کیفیت یک تک جزء از محصول نیست، بلکه مجموعهٔ پیچیده‌ای از مشخصات است،
- کیفیت برای یک محصول یا سیستم، به صورت یک کمیت گسستهٔ شامل یکی از دو حالت وجود کیفیت و یا عدم وجود کیفیت نیست، بلکه یک طیف پیوسته بین حالت بسیار خوب و بسیار بد دارد.

مدیریت کیفیت از تضمین کیفیت و کنترل فرایندهای تولید برای حصول کیفیت پایدارتر استفاده می‌کند. روش‌های زیادی برای ارتقای کیفیت وجود دارد که ارتقا در محصولات، فرایند و جامعه را شامل می‌شوند. برخی روش‌های مدیریت کیفیت و

تکنیک‌های ارتقای کیفیت عبارتند از ایزو ۹۰۰۱، مدیریت کیفیت کلی، شش سیگما، گسترش عملکرد کیفی، دایره کیفیت و روش‌های تاگوچی.

قابلیت اطمینان (Reliability): بنیاد مهندسان الکتریکی و الکترونیکی (IEEE) قابلیت اطمینان را به صورت قابلیت یک سیستم و یا جزء برای انجام اقدامات مورد نیاز تحت شرایط تعیین شده برای یک دورهٔ مشخص زمانی، تعریف کرده است. این تعریف چهار مؤلفه دارد:

- قابلیت – به صورت کمّی با احتمال بیان می‌شود و راجع به شانس و یا احتمال اینکه سیستم یا جزء درست کار خواهد کرد، می‌باشد. قابلیت به صورت یک نسبت اعشاری بین صفر و یک اندازه‌گیری می‌شود و معمولاً به صورت درصد بیان می‌شود.
- اقدامات مورد نیاز – عموماً به معنی عمل‌کردن بدون خرابی است. مشخصات الزمات سیستم، معیاری برای اینکه کدام قابلیت اطمینان اندازه‌گیری می‌شود، می‌باشد. برای این امر، یک استاندارد مورد نیاز است که باید شامل معیارهای اندازه‌گیری مؤثر برای مقایسهٔ عملکرد واقعی با استاندارد باشد. اگر عملکرد واقعی در حد مجاز استاندارد قرار گیرد، عملکرد مورد نظر سیستم موفق ارزیابی خواهد شد.
- دورهٔ زمانی مشخص‌شده – هیچ چیز برای همیشه باقی نخواهد ماند و هیچ چیزی برای همیشه به طور مناسب کار نخواهد کرد. بنابراین، برای یک عملکرد مورد نظر یک قالب زمانی نیاز است که معمولاً مدت زمان مأموریت نامیده می‌شود.
- شرایط تعیین‌شده – یک محصول ممکن است عملکرد مورد انتظار خود را در یک سری از شرایط به خوبی انجام دهد و در شرایط دیگر به‌کلی نامناسب انجام دهد. یک بخش طراحی شده به عنوان مثال برای دمای محیط ممکن است برای دماهای بالاتر و یا پایین‌تر به‌کلی نامناسب باشد. شرایط تعیین شده شامل فشار هوا، دما، رطوبت، شوک، ارتعاشات و غیره باشد.

مثالی که حاوی همهٔ چهار مؤلفهٔ فوق است می‌تواند یک سیستم یا جزئی که با احتمال ۹۹ درصد با بیش از ۸۰ درصد ظرفیت نامی، برای ۵۰۰ ساعت بدون خرابی، در دمای محیط ۲۵ تا ۵۰ درجه سانتی‌گراد، با کمتر از ۵۵ درصد رطوبت در محیط بدون گرد و غبار، کار می‌کند، باشد.

قابلیت نگهداری (Maintianability): به قابلیت بازگرداندن سیستم به شرایط عملکردی مشخص‌شده با استفاده از رویه‌ها و منابع مشخص‌شده قابلیت نگهداری می‌گویند. مقیاس کمّی قابلیت نگهداری عبارت است از: احتمال اینکه اقدام نگهداری می‌تواند در بازهٔ زمانی تعیین شده انجام شود. نگهداری اصلاحی پس از وقوع خرابی انجام می‌شود، اما به منظور کاهش احتمال خرابی‌ها و آسیب‌های ناشی از آنها، نگهداری می‌تواند پیش‌گیرانه و یا پیش‌بینانه باشد.

- نگهداری اصلاحی: این نوع نگهداری پس از تشخیص خرابی به منظور بازگردادن سیستم به حالت مورد نیاز عملکردی انجام می‌شود.
- نگهداری پیش‌گیرانه: این نوع نگهداری در بازه‌های زمانی از پیش تعیین‌شده و یا طبق معیارهای مشخص‌شده به منظور کاهش احتمال خرابی و یا نقصان عملکرد انجام می‌شود.
- نگهداری پیش‌بینانه: نگهداری پیش‌بینانه نوعی از نگهداری پیش‌گیرانه است که به صورت پیوسته و یا در بازه‌های زمانی تعیین‌شده توسط پایش شرایط، تشخیص و یا شناسایی رفتار در ساختار، سیستم و یا اجزا انجام می‌شود. نتایج این نوع نگهداری، قابلیت عملکردی کنونی و آینده و برنامهٔ زمانی نگهداری را مشخص می‌کند. نگهداری پیش‌بینانه با عنوان نگهداری مبتنی بر شرایط نیز شناخته می‌شود.

قابلیت دسترسی (Availability): درصد زمانی که یک سیستم برای عمل، در دسترس است را قابلیت دسترسی گویند. به عبارت دیگر، قابلیت دسترسی عبارت است از احتمال اینکه یک محصول یا سیستم در زمان مشخص شده در حال کار است. هنگامی که یک سیستم حفاظتی تست می‌شود، دسترسی به آن در آن زمان متوقف می‌شود.

انواع مختلفی از قابلیت دسترسی وجود دارد. به عنوان مثال، قابلیت دسترسی متوسط، در یک بازهٔ زمانی حقیقی تعریف می‌شود و یا قابلیت دسترسی حالت پایا، حد عملکردی قابلیت دسترسی آنی، هنگامی‌که زمان به بی‌نهایت میل کند، می‌باشد.

در یک سیستم غیرقابل تعمیر، قابلیت دسترسی همان قابلیت اطمینان است. برای سیستم قابل تعمیر، امکان بازگشت سیستم معیوب به شرایط کاری باعث می‌شود اثر خرابی کاهش یابد. در این سیستم قابلیت اطمینان تغییر نمی‌کند، ولی قابلیت دسترسی تغییر خواهد کرد. ساده‌ترین بیان از قابلیت دسترسی به صورت زیر است:

$$A = \frac{\text{بازه زمانی کارکردن سیستم}}{\text{بازه زمانی کارکردن سیستم + بازهٔ زمانی کارنکردن سیستم}}$$

بازهٔ زمانی کارکردن مربوط به قابلیت اطمینان سیستم است، درحالی‌که بازهٔ زمانی کارنکردن مربوط به قابلیت نگهداری سیستم است. بنابراین، قابلیت دسترسی تابعی از قابلیت اطمینان و قابلیت نگهداری است.

رویداد فاجعه‌بار (Catastrophic Incident): رویدادی که شامل یک انتشار سمّی کنترل نشده عظیم، آتش‌سوزی و یا انفجار با اثرات بر جامعه باشد.

شناسایی مخاطرات (Hazards Identification): فرایندی که در آن مخاطرات شناسایی می‌شوند. معمولاً با عنوان تحلیل مخاطرات فرایند (PHA) شناخته می‌شود. ابزارهای تحلیلی ساختاری شامل موارد زیر است:

- تحلیل مخاطره و قابلیت عملکرد (HAZOP)،
- تحلیل «what if»،
- تحلیل مودهای خرابی و اثرات آنها (FMEA)،
- تحلیل پایش‌برگ،
- تحلیل مخاطره اولیه (با عنوان PHA و یا تحلیل ریسک سطح تقسیم‌بندی SLRA نیز به کار می‌رود.)،
- تحلیل «what if» و پایش‌برگ.

در این تقسیم‌بندی، تحلیل‌های درخت خطا و درخت رویداد نیز قابل لحاظ است، اما این دو ابزار، بیشتر از شناسایی مخاطرات، در تحلیل کمّی ریسک به کار می‌روند.

شناسایی مخاطرات بر سناریوها و آزمون‌های ویژه‌ای متمرکز است:

- چگونه این مخاطرات ممکن است رخ دهد؟ علل وقوع چیست؟
- چه ممکن است رخ دهد؟ پیامدها کدامند؟
- در برابر رویداد پایه یا پیامدها، محافظت چگونه انجام می‌شود؟
- اگر محافظت به اندازهٔ کافی نباشد، چه باید کرد؟ اقدامات مورد نیاز کدامند؟

ایمنی ذاتی و عارضی (Intrinsic and Extrinsic Safety): اجزای ایمنی که با طبیعت ذاتی عمل می‌کنند و به فعال‌سازی و یا اقدام انسانی نیاز ندارند، ایمنی ذاتی دارند. اجزای ذاتی کنترل ریسک، غیرفعال (passive) هستند که در برابر مفهوم فعال (active) قرار دارد.

مثال ۱: موجودی یا ذخیره موجودی کاهش یافتهٔ مواد خطرناک، جزء ایمنی ذاتی هستند، که پیامدهای رویدادهای خطرناک را کاهش می‌دهند و مربوط به ایمنی غیرفعال است. مثال دیگر شامل ایجاد فضای افزایش‌یافتهٔ تجهیزات و ایجاد موانع دور مخازن ذخیره است.

مثال ۲: آشکارساز گازهای قابل اشتعال یک جزء ایمنی فعال است که وابسته به اجزای خودکار است و در دستهٔ اجزای ایمنی عارضی قرار دارند.

اغلب تأسیسات نیازمند ترکیبی از اجزای ایمنی ذاتی و عارضی برای رعایت استانداردهای ریسک قابل قبول هستند.

تحلیل ریسک (Risk Analysis): فرایند ارزیابی پیامدها و فرکانس‌های روی دادن فعالیت‌های خطرناک است.

سنجش ریسک (Risk Appraisal): سنجش ریسک، قضاوت کردن قابل پذیرش بودن ریسک‌ها است. معمولاً معیارها با اجماع عام بین تحلیل‌گران ریسک حاصل می‌شوند و از طریق جامعهٔ متخصصین منتشر می‌شود.

ارزیابی ریسک (Risk Assessment): ارزیابی ریسک شامل ترکیب تحلیل ریسک و سنجش ریسک است.

اندازه‌گیری ریسک (Risk Measurement): معمولاً اندازه‌گیری با مقیاس‌های زیر انجام می‌شود:

- میزان مرگ و میر،
- عیب در خاصیت،
- میزان تولید معیوب،
- میزان آسیب محیطی.

مهار ریسک یا کنترل ریسک (Risk Mitigation or Risk Control): کاهش ریسک یک توالی رویدادها با اقدام پیشگیرانه با کاهش احتمال وقوع رویداد، یا اقدام محافظتی با کاهش دامنهٔ پیامدهای رویدادهای مخاطره آمیز را مهار ریسک یا کنترل ریسک گویند. روش‌ها معمولاً به صورت فعال و غیرفعال تقسیم می‌شوند.

نرخ تقاضا (Demand Rate): نرخ فراخوانی فعال‌شدن یک سیستم حفاظتی.

افزونگی (Redundancy): تمهیدات حفاظتی یدکی یا اضافی که درصورت خراب شدن تجهیز اول، عمل می‌کنند.

ارزیابی ریسک احتمالاتی (Probabilistic Risk Assessment) و ارزیابی ایمنی احتمالاتی (Probabilistic Safety Assessment): در ارزیابی ریسک احتمالاتی (PRA) و یا ارزیابی ایمنی احتمالاتی (PSA) هدف ارزش‌یابی ریسک‌های یک سیستم با استفاده از یک روش احتمالاتی است؛ یک رویکرد جامع ساختارمند برای شناسایی سناریوهای خرابی با تشکیل یک ابزار مفهومی و ریاضی برای ارائهٔ تخمین‌های عددی از ریسک که شامل شناسایی رویدادها و ترکیبات آنها که می‌توانند منجر به حوادث وخیم شوند و ارزیابی احتمال وقوع هر ترکیب و ارزش‌گذاری پیامدها است. این دو اصطلاح همزمان برای این مقوله به کار می‌روند. با این تفاوت که PRA دامنه‌ای وسیع‌تر از PSA دارد. در PRA کلیه پدیده‌های همراه با ریسک مورد مطالعه قرار می‌گیرند که شامل صنایع، پدیده‌های طبیعی، مخاطرات زیست محیطی، مسائل بهداشت و سلامت، انواع بیماری‌ها و ... می‌شود، درحالی‌که PSA به تحلیل ایمنی احتمالاتی در سیستم‌ها و تأسیسات صنعتی که حاوی اجزای مرکب با یک مأموریت مشخص است به کار می‌رود. با این بیان، ابزارهایی مانند درخت‌های خطا و رویداد که ابزارهای اصلی PSA هستند برای مقولاتی مانند بهداشت و سلامت چندان به کار نمی‌روند و بیشتر برای تحلیل ایمنی سیستم‌ها و تأسیسات صنعتی مورد استفاده هستند.

۲- تحلیل ریسک

۲-۱- مقدمه

ریسک یک مقیاس نشان‌دهندهٔ زیان بالقوّه در اثر فعالیت‌های انسان یا طبیعت است. زیان‌های بالقوه شامل پیامدهای مضر در قالب فعالیت‌های منجر به آسیب به حیات انسان، اثرات نامناسب بر سلامت، از دست دادن خاصیت و ویرانی در محیط طبیعت است. تحلیل ریسک عبارت است از فرایند تعیین، مدیریت و اطلاع‌رسانی به دیگران در خصوص وجود، ماهیت، دامنه، رواج، عوامل تشکیل دهنده و عدم قطعیت‌های زیان‌های بالقوّه. در سیستم‌های مهندسی (یک سیستم مهندسی به صورت یک مجموعهٔ متشکل از سخت‌افزار، نرم‌افزار و سازمان انسانی تعریف می‌شود)، زیان بالقوّه می‌تواند ناشی از سیستم باشد و به خارج از سیستم سرایت کرده و بر یک یا چند دریافت‌کننده (به عنوان مثال، انسان‌ها، سازمان‌ها، سرمایه‌های اقتصادی و محیط زیست) اثرگذار باشد. همچنین، زیان‌های بالقوّه می‌توانند ناشی از سیستم بوده و تنها به خود آن سیستم آسیب وارد کنند. به عنوان مثال، در یک نیروگاه هسته‌ای زیان بالقوّه می‌تواند منجر به ویرانی نیروگاه در اثر ذوب بخشی از قلب راکتور و یا ایجاد آسیب در اثر انتشار مواد پرتوزا از نیروگاه به محیط زیست شود. حالت اول این مثال، زیان بالقوّه داخلی سیستم است و حالت دوم نشان‌دهندهٔ زیان ناشی از سیستم (نیروگاه هسته‌ای) به محیط زیست است. از دید مهندسی، ریسک و یا زیان بالقوّه با قرار گرفتن دریافت‌کنندگان زیان در معرض مخاطرات مرتبط است و می‌تواند به صورت ترکیبی از احتمال و فرکانس خطر و پیامدهای آن بیان شود. پیامدهایی که لحاظ می‌شوند شامل صدمه یا از دست دادن حیات، هزینه‌های بازسازی، زیان‌های فعالیت‌های اقتصادی، زیان‌های زیست‌محیطی و غیره می‌شوند. در سیستم‌های مهندسی، تحلیل ریسک به منظور تعیین مقیاسی برای زیان‌های بالقوه و مهم‌تر از آن، شناسایی اجزایی از سیستم که سهم بیشتری در این زیان‌ها دارند، انجام می‌شود. این تحلیل می‌تواند به صورت صریح و یا ضمنی انجام شود. در تحلیل صریح، اهداف باید به صورت سطوح ریسک قابل پذیرش[۱] مورد توجه قرار گیرند. اما، معمولاً مهندسان درباره پذیرشِ ریسکِ سیستم‌ها تصمیم نمی‌گیرند. تصمیمات توسط مدیریت‌کنندگان ریسک، سیاست‌گذاران و سیاست‌مدارانی که تحت تأثیر محیط اقتصادی، رسانه‌ها، اعتقادات عمومی و تشکّل‌های غالب هستند، اتخاذ می‌شوند. این جنبهٔ ریسک، همچنین بر اهمیت ارتباطات ریسک بین بخش‌های مختلفِ سهیم، تأکید می‌کند. برای فهم بهتر تحلیل ریسک در فضای سیستم‌های مهندسی پیچیده، نیاز به آشنایی با پیچیدگی طبیعت سیستم است.

[۱] - acceptable risk level

۲-۲- اهمیت تحلیل ریسک

۲-۲-۱- پیچیدگی و مشخصات سیستم‌های مهندسی و مدل‌های آنها

قابلیتِ سازگاری سیستم‌ها با محیط‌های داخلی و خارجی، منجر به تکامل و ظهور سیستم‌هایی می‌شود که به صورت فزاینده‌ای پیچیده، خودکار و هوشمند هستند. مثال‌های فراوان این افزایش پیچیدگی، در سیستم‌های مهندسی شامل سیستم‌های حمل و نقل و انرژی است. در واقع، اگرچه رشد پیچیدگی طی تکامل به صورت فراگیر نیست، اما در جهانِ درهم‌تنیدهٔ پیچیدهٔ ما ظهور و بروز دارد. به عنوان مثال، در نظر گرفتن زیرساخت‌های مهندسیِ به شدت به هم پیوسته، مانند ارتباطات، انرژی، حمل و نقل و منابع آبی، ممکن است این جمع‌بندی را به همراه داشته باشد که ساده‌سازی در یک زمینه ممکن است منجر به افزایش پیچیدگی کل زیرساخت شود. به عنوان مثال، روش‌های ساده‌سازی ارتباطات (مانند ارتباطاتِ سریع‌تر و آسان‌تر) منجر به دسترسیِ بهبودیافته به اطلاعات توسط تروریست‌ها شده که منجر به کاهش امنیت انرژی و منابع آبی می‌شود و نیازمندی‌های متعاقب آن، لایه‌های اضافی حفاظت، ممانعت و مهار است. به طور همزمان با بهبود سطح آموزش جامعه، افزایش سطح دانش و دارایی، استانداردهای بالاتر ایمنی، بهداشت و امنیت برای سیستم‌هایی که پیچیدگی آنها همواره رو به افزایش است، ضروری خواهد بود. در یک جامعه ضروری است که صنعتِ دولتی و خصوصی این نیازهای جامعه را فهمیده و سیاست‌های خود را سازگار با آنها اتخاذ نماید. در سالیان اخیر، تحلیل ریسک به عنوان یک رویکرد قدرتمند در این زمینه و نیز توسعهٔ سیاست صحیح و اتّخاذ استراتژی طراحی، مورد توجه قرار گرفته است.

برای تحلیل هر سیستمِ مهندسیِ پیچیده، یک مدل نیاز است. این مدل باید با مشخصات اولیهٔ سیستمِ مهندسیِ پیچیده سازگار باشد. شاخصه‌های سیستم‌های مهندسی پیچیده عبارتند از: در حال رشد بودن، یکپارچگی، پویایی، بزرگی و هوشمندی. سه شاخصهٔ اول مشخصات اولیه و دو شاخصهٔ بعدی فرعی هستند. مشخصهٔ در حال رشد بودن مستلزم یک مدل ریسکِ دربردارندهٔ بازخوردهای داخلی و خارجی است که امکان توسعه‌های ارتقایی و فرصت‌طلبانه در آن لحاظ شود. همچین عدم قطعیت و ابهام ناشی از مشخصات و خواص اجزای مختلف و روابط آنها در سیستم‌های پیچیده باید لحاظ شوند. لازم به توجه است که در سیستم‌های پیچیده، عدم قطعیتِ تخمینِ عدم قطعیت نیز باید تخمین زده شود.

مدل باید همبستگی اجزای سیستم و نیز یکپارچگی آن را لحاظ کند. بنابراین، پیچیدگیِ همواره رو به افزایش در ساختار، عملکرد و اهداف سیستم باید در مدل تعبیه شود. به‌روزرسانی ارتباطات بین اجزای سیستم از الزامات دیگر مدل است. قابلیت شناسایی ارتباطات مخفی، غیرخطی و غیرقطعی از مشخصات دیگری است که در مدل باید لحاظ شوند. بازخوردِ

مستمر در طول زمان یا همان مشخصهٔ پویایی سیستم باید در مدل لحاظ شود. مدل باید اتصال و یکپارچگیِ زیرسیستم‌های گوناگون اما مرتبط را بدون تحمیل قیدهای اضافه دربرداشته باشد. درنهایت، مدل باید توانایی‌های حصول خواص سیستم مانند خودتنظیمی و قابلیت یادگیری را نشان دهد.

۲-۲-۲- نیاز به تحلیل ریسک

شواهد نشان می‌دهند تا هنگامی که جهان پیرامون ما به سمت پیچیدگی سیر می‌کند، ما، طولانی‌تر، با بهداشت بالاتر و توانمندتر از هر زمان گذشته زندگی می‌کنیم. برخی اقتصاددانان و تحلیل‌گران ریسک مانند مورگان استدلال می‌کنند که امروزه ما بیش از گذشته نگران ریسک هستیم چراکه ما داشته‌های زیادی برای از دست دادن و هزینهٔ بیشتری برای کاهش ریسک داریم. چنین عواملی فشار مضاعف انکارناپذیری بر تولیدکنندگان، سیاست‌گذاران و سازمان‌ها برای فراهم آوردن و اطمینان دادن از اینکه سیستم‌ها، تکنولوژی‌ها و استراتژی‌ها، ایمن، بهداشتی و سازگار با محیط زیست هستند، ایجاد می‌کند.

اثبات و طراحی ایمنی در سیستم‌های پیچیده رویکردهای رسمی تحلیل ریسک را شکل داده است. اگرچه روش‌های رسمی تحلیل ریسک نسبتاً جدید هستند، اما مفهوم مقیاس‌دهی و یا حدس‌زدن ریسک، قرن‌ها سابقه دارد.

۲-۲-۳- ضرورت تحلیل ریسک رسمی برای مدیریت و تنظیم ریسک

همانطور که اشاره شد، سیستم‌های مهندسی به سمت پیچیدگی حرکت می‌کنند و نیاز به تحلیل ریسک بیش از هر زمان است. یک مکانیزم کنترل و ممانعت از ریسک در مدیریت تولید، بهره‌برداری و ساخت و سیستم‌های پیچیده وجود دارد. متأسفانه تصمیمات و قوانین بسیاری مبتنی بر تحلیلِ ریسکِ رسمی نیستند. یعنی قوانین نیز پیچیده هستند. پیچیدگی با چندین عامل ترکیب شده است. مهم‌ترین عاملِ قابلِ توجه، قوانین مبهم، سیاست‌ها و اثرگذاری گروه‌های مصلحت‌سنج است. با وجود مقاصد و نیت‌های خوب، برخی قوانین دولتی ریسک‌های ناحیه‌ای را با هزینه‌های گزاف کنترل می‌کنند. به عنوان مثال قوانین ریسک محلی، منطقه‌ای و ناحیه‌ای ابتدائاً به صورت موضعی کاهش مرگ و میر در اثر سرطان‌ها و حوادث را مورد هدف قرار می‌دهند که این قوانین تأثیر چندانی در کاهش ریسک ندارند.

دیدگاه مرسوم نسبت به قوانین ریسک‌های ایمنی این است که وجود ریسک اجتناب‌ناپذیر است و با به کارگیری تکنولوژی مناسب، می‌توان این ریسک‌ها را حذف کرد. اما در این دیدگاه هزینه‌های کاهش ریسک شناخته نمی‌شود؛ این واقعیت که: یک جامعه بدون ریسک، بسیار پرهزینه و غیرممکن است. روشن است که قوانین به صورت رایگان محقق نمی‌شوند. جامعه متحمّلِ حدّ نهاییِ پرداختِ هزینهٔ این قوانین در قالب قیمت‌های بالاترِ محصولات، مالیات‌های بیشتر، از دست دادن رقابت

جهانی و درآمد کمتر خواهد شد. اثر خالص برخی قوانین پرهزینه، کاهش تولید ناخالص ملی است. بنابراین، تنظیم قوانین باید یک هدف مهم یک جامعه با نظام مالی معقول باشد. روش‌های تحلیل ریسک، نوعی از نتایج برای دست‌یابی این هدف را فراهم می‌آورد. اخیراً قانون‌گذارانِ بسیاری حامی ارتباط بیشتر استفاده از قوانین ریسک توسط آژانس‌های اجرایی شده‌اند.

تحلیل ریسک و بخصوص ارزیابی ریسک احتمالاتی می‌تواند نقش‌های اساسی در طراحی، ساخت، بهره‌برداری، سیاست و تصمیمات تنظیمی بازی کند. توسعه و رشد در زمینه تحلیل ریسک و به خصوص ارزیابی ریسک احتمالاتی نسبت به سه دهه گذشته بسیار زیادتر شده است. یک مزیتِ عالیِ تحلیل ریسک این است که می‌تواند به طور وسیعی اطمینان جامعه در خصوص یک فرایند مهندسی را ارتقا دهد.

۲-۲-۴- انواع ریسک

ریسک می‌تواند به روش‌های مختلفی طبقه‌بندی شود که مبتنی بر نوع مخاطرات است. طبقه‌بندی می‌تواند بر اساس علت ریسک یا پیامدها و یا هر دو انجام شود. همانطور که ذکر شد، اساساً ریسک به صورت زیان بالقوّه تعریف می‌شود. چنین زیانی می‌تواند نهایتاً به صورت یک مقیاسِ اقتصادی اندازه‌گیری شود و به صورت زیانِ اقتصادی بالقوّه دیده شود. اما یک طبقه‌بندیِ صحیح‌تر، مبتنی بر پنج دستهٔ وسیع است که زیان‌های بالقوّه را لحاظ می‌کنند. این دسته‌های ریسک عبارتند از: بهداشت، ایمنی، امنیت، اقتصاد و محیط زیست.

۱. تحلیل ریسک بهداشت شامل تخمین بیماری‌های بالقوّه و زیان‌های مترتّب بر زندگی انسان‌ها، حیوانات و گیاهان می‌شود.
۲. تحلیل ریسک ایمنی شامل تخمین آسیب‌های بالقوّه حاصل از حوادث ناشی از رویدادهای طبیعی (شرایط آب و هوایی، زمین‌لرزه‌ها، آتش‌سوزی و ...) و یا ناشی از محصولات، تکنولوژی‌ها و سیستم‌های ساخته شده توسط انسان (سوانح هواپیما، انفجارات تأسیسات شیمیایی، حوادث نیروگاه‌های هسته‌ای، منقضی شدن عمر و یا خرابی تکنولوژی) می‌شود.
۳. تحلیل ریسک امنیت شامل تخمین دسترسی و آسیب ناشی از جنگ، ترور، اغتشاش، تبهکاری (خرابکاری، سرقت و ...)، دستبرد به اطلاعات (اطلاعات امنیت ملی، مالکیت فکر و ...) می‌شود.
۴. تحلیل ریسک اقتصادی شامل تخمین زیان‌های مالی فردی، سازمانی و اجتماعی مانند نوسانات ارزش پول، نرخ‌های بهره، بازارهای مشترک، زیان‌های پروژه‌ها، ورشکستگی، اختلاس و ...) می‌شود.

۵. تحلیل ریسک محیط زیست شامل تخمین زیان‌های انتشار آلودگی در اکوسیستم (آب، زمین، هوا و اتمسفر) و فضا است.

بین این دسته‌ها ارتباطاتی وجود دارد. به عنوان مثال، ریسک‌های محیط زیست ممکن است منجر به ریسک‌های اقتصادی شوند.

۲-۲-۵- گرایش‌ها در به‌کارگیری روش‌های تحلیل ریسک در مهندسی

یک رویکردِ سنتیِ تحلیل ریسک، طراحی یا تنظیم سیستم‌های ایمنی به صورت محافظه‌کارانه برای اجتناب از ریسک است. این روش‌ها شامل فلسفهٔ دفاع عمقی در صنعت هسته‌ای است که شامل سدهای متعدد ایمنی، محدوده‌های بزرگ ایمنی، کنترل کیفی و بازرسی‌های مکرر است (استراتژی دفاع عمقی و اصول ایمنی در صنعت هسته‌ای در ضمیمهٔ این گزارش بیان شده‌اند). تجربه و تحقیق نشان داده است این فلسفه، از آنجاکه به طور معقولی ایمنی را تضمین می‌کند، اغلب منجر به سیستم‌ها، محصولات و تکنولوژی‌های پرهزینه می‌شود، به طوری‌که جامعه و بازار قادر به برآمدن از عهدهٔ آن نیست. علاوه براین، مطالعات نشان می‌دهند هنگامی که برخی طراحی‌ها و مقررات بر رویکردهای محافظه‌کارانه مبتنی باشد، به ظاهر ریسک سیستم‌ها و محصولات مهندسی پیچیده را کاهش می‌دهد، اما ممکن است این کاهش در اثر هزینهٔ گزاف به دست آید و هنوز ایمنی را تضمین نکند. با درک این مسائل، صنایع و آژانس‌های تعیین ضوابط بر تکنیک‌های رسمی تحلیل ریسک برای ارزیابی اجزای تشکیل دهندهٔ ریسک اعتماد کرده است. به عنوان مثال، کمیتهٔ مقررات هسته‌ای امریکا[۱] در استفاده از تکنیک‌های ریسک در به‌کارگیری و تکمیل مقررات ایجاد شده از روش‌های محافظه‌کارانهٔ دفاع عمقی با نتایج تحلیل ریسک پیشگام است. صنعت هسته‌ای و اخیراً صنایع حمل و نقل، صنایع فضایی و صنایع غذایی استفاده از تحلیل ریسک در بهره‌برداری و اتخاذ تصمیمات سیاستی خود را به میزان بسیار زیادی افزایش داده‌اند.

تحلیل ریسک می‌تواند در کلیهٔ مراحل طراحی، توسعه، ساخت و بهره‌برداری از سیستم‌های مهندسی به کار رود. به عنوان مثال، تحلیل ریسک در مراحل مختلف زیر قابل انجام است.

- طراحی مفهومی: در این مرحله، تحلیل ریسک به مقایسهٔ گزینه‌های طراحی مختلف می‌پردازد.
- طراحی: در این مرحله، تحلیل ریسک به فراهم آوردن موانع ممانعت، کمینه‌سازی و یا حذف آسیب، کمینه‌سازی هزینه در طول عمر، محدوده‌های ریسک تخصیص یافته و اهداف عملکردی می‌پردازد.

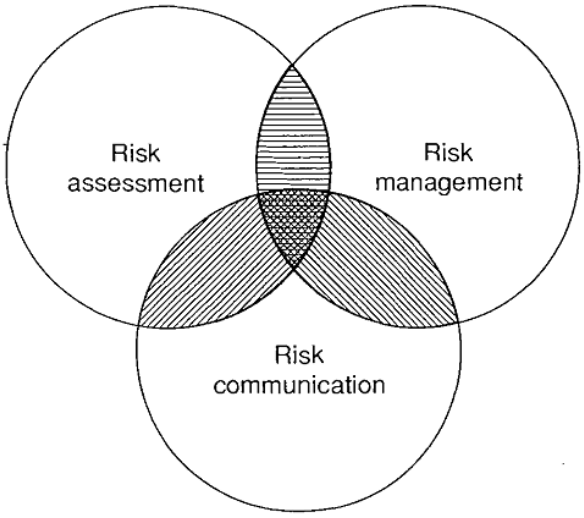
[۱] - NRC

- توسعه: در این مرحله، تحلیل ریسک به شناسایی سیستم‌ها و یا زیرسیستم‌های دارای بیشترین سهم در ایمنی و ریسک، تست ایمنی و ریسک المان‌های خاص از طراحی، تضمین کیفیت و توسعه ضمانت می‌پردازد.
- تنظیم: در این مرحله، تحلیل ریسک در توجه به اهمیت المان‌های سیستم که بیشترین سهم را در ریسک دارند در وضع مقررات، تعیین معیارهای عملکردی و پایش و انجام بازرسی کاربرد دارد.
- بهره‌برداری: در این مرحله، تحلیل ریسک به بهینه‌سازیِ هزینهٔ نگهداری و سایر فعالیت‌های عملکردی، تعریف الزامات نظارت و برنامه زمانی، سیاست‌های جایگزینی و اتخاذ تصمیمات، تخمین و مدیریت افزایش سن و توسعه مقیاس‌های امنیتی می‌پردازد.
- ازکاراندازی: در این مرحله، تحلیل ریسک به ارزیابی ایمنی جایگزین‌های ممکنِ ازکاراندازی، انتخاب صحیح‌ترین روش مصرف و ارزیابی وظایف مسئولیتی بلند مدت می‌پردازد.

۲-۳- اجزا و انواع تحلیل ریسک

معمولاً تحلیل ریسک شامل سه جزء مرکزی ارزیابی ریسک، مدیریت ریسک و ارتباطات ریسک تعریف می‌شود. کنش‌ها و تداخل بین این سه جزء در شکل ۱ نشان داده شده است.

اولین جزء تحلیل ریسک، ارزیابی ریسک است، پردازشی که احتمال یا فرکانس یک زیان حاصل و یا ناشی از یک سیستم مهندسی را تخمین زده و دامنهٔ آن زیان (پیامد) را نیز اندازه‌گیری یا تخمین بزند. مدیریت ریسک فرایندی است که فرکانس (احتمال) دامنهٔ ریسک و اجزای سهیم در ریسک را تخمین، ارزیابی، کمینه و کنترل می‌کند. ارتباطات ریسک فرایندی است که اطلاعات طبیعت ریسک (زیان مورد انتظار) و رویکرد ارزیابی پیامدهای ریسک و گزینه‌های مدیریت ریسک، تبادل و به اشتراک گذاشته شده و بین تصمیم‌گیران به بحث گذاشته می‌شود.



شکل ۱. اجزای تحلیل ریسک

تحلیل ریسک در مورد تخمین پتانسیل و دامنهٔ هر زیان و راه‌های کنترل آن در یک سیستم است. اگر داده‌های پیشینه‌ای کافی در مورد یک زیان وجود داشته باشد، آنگاه می‌توان ریسک را مستقیماً از آمارهای زیان‌های واقعی تعیین کرد. این رویکرد در تصادفات اتومبیل، ریسک‌های سرطان و فرکانس رویدادهای طبیعی خاص مانند سیل‌ها و طوفان‌ها که داده‌های آماری دارند، به کار می‌رود. درصورتی‌که داده‌های کافی در مورد زیان‌های واقعی وجود نداشته باشد، روش دیگری وجود دارد. در این حالت، از مدل‌سازی برای زیان در تحلیل ریسک استفاده می‌شود و زیان بالقوّه (یعنی همان ریسک) تخمین زده می‌شود. در اغلب حالت‌ها، به خصوص برای سیستم‌های مهندسی پیچیده، داده‌های زیان‌ها، کم و یا غیرقابل دسترسی است. بنابراین، تحلیل‌گران باید ریسک را مدل‌سازی و پیش‌بینی کنند. تحلیل‌گرانِ ریسک تلاش می‌کنند که دامنهٔ یک زیان (پیامد) ناشی از سیستم‌های پیچیده را اندازه‌گیری کنند که این امر شامل ارزیابی، کاهش ریسک و سیاست‌های کنترل است. به طورعام، سه نوع تحلیل ریسک عبارتند از: تحلیل ریسک کمّی، کیفی و مرکب. هر سه روش، که هر کدام اهداف، نقاط قوت و ضعف مختلفی دارند، به طور وسیعی استفاده می‌شوند.

۲-۳-۱- تحلیل ریسک کمّی

در تحلیل ریسک کمّی تلاش می‌شود تا ریسک را در قالب احتمالِ (یا فرکانس) یک زیان، تخمین زده شده و این احتمال، برای اتخاذ تصمیمات و به اشتراک‌گذاری نتایج، ارزیابی شود. در این بین، عدم قطعیت مرتبط با تخمین فرکانس (یا احتمال) روی‌دادنِ رویدادهای نامطلوب و دامنهٔ زیان‌ها (پیامدها) با استفاده از مفاهیم احتمال مشخص می‌شوند. هنگامی که شواهد و اطلاعات کمیاب است، عدم قطعیت‌های ناشی از نتایج کمّی نقشی قطعی در به کارگیری نتایج ایفا می‌کنند.

هنگامی که داده‌های میدانی، داده‌های آزمایش‌ها و سایر شواهد برای تخمین احتمال (یا فرکانس) و دامنهٔ زیان‌ها وجود داشته باشد، تحلیل ریسک کمّی رویکردِ پیشنهادی است. به‌کارگیری تحلیل ریسک کمّی روندی رو به رشد دارد که اولاً ناشی از فراهم‌شدن امکان دسترسی به تکنیک‌ها و ابزارهای کمّی است و ثانیاً قابلیت تخمین کمّیِ رویدادها و سناریوهای زیان‌بار در سیستم‌های پیچیده از داده‌های محدود در تحلیل ریسک کمّی وجود دارد. با این حال، استفاده از تحلیل ریسک کمّی به تحلیل‌های ریسک با مقیاس وسیع محدود شده است، چراکه این نوع از تحلیل، پیچیده، زمان‌بر و پرهزینه است.

۲-۳-۲- تحلیل ریسک کیفی

این نوع تحلیل ریسک، احتمالاً پراستفاده‌ترین نوع است؛ فقط به این دلیل که این روش ساده و سریع است. در این نوع تحلیل ریسک، زیان بالقوّه با استفاده از مقیاس‌های مفهومی مانند کم، متوسط و زیاد، به صورت کیفی تخمین زده می‌شوند. در این نوع از تحلیل، یک ماتریس تشکیل می‌شود که ریسک را در قالب فرکانس زیان بر حسب مقادیر بالقوّه آن در مقیاس‌های کیفی مشخص می‌کند. سپس این ماتریس برای سیاست‌گذاری و اتخاذ تصمیمات مدیریت ریسک به کار می‌رود. ازآنجاکه این روش نیاز به ارتباط با داده‌های واقعی و رفتار احتمالاتی چنین داده‌هایی ندارد، بسیار ساده‌تر و آسان‌تر استفاده و فهم می‌شود، ولی باید توجه داشت که این روش به‌غایت ذهنی است.

در واقع می‌توان گفت تحلیل ریسک کیفی، یک روشِ انتخاب برای سیستم‌های بسیار ساده مانند ایمنی یک تک محصول، امنیت فیزیکی ساده و فرایندهای مستقیمِ روبه‌جلو است.

۲-۳-۳- تحلیل ریسک مرکب کمّی و کیفی

تحلیل ریسک می‌تواند مرکب از دو روش کمّی و کیفی باشد. این ترکیب می‌تواند به دو روش انجام شود: فرکانس یا پتانسیل زیان به صورت کیفی تعیین می‌شود، ولی اندازهٔ زیان (پیامد) به صورت کمّی اندازه‌گیری می‌شود و یا برعکس. همچنین، ممکن است هم فرکانس و هم اندازهٔ زیان به صورت کمّی اندازه‌گیری شوند، اما بخش تعیین سیاست و اتخاذ تصمیم در تحلیل ریسک براساس روش‌های کیفی انجام شود، مانند استفاده از مقیاس‌های سیاستی کیفی برای محدوده‌های کمّی زیان. همچنین، ممکن است مقادیر کمّی ریسک با سایر اطلاعات کمّی یا کیفی ریسک برای رسیدن به یک تصمیم، تکمیل شوند. این روش دوم، روش انتخاب در آئین جدید کمیتهٔ هسته‌ای امریکا به نام قانون risk-informed است که در آن، اطلاعات ریسک حاصل از تحلیل ریسک احتمالاتی رسمی با سایر نتایج کمّی و کیفی حاصل از تحلیل‌های ایمنی یقینی و بررسی‌های مهندسی برای اتخاذ تصمیمات و سیاست‌ها ترکیب می‌شوند.

۲-۴- ارزیابی ریسک

ارزیابی ریسک یک تحلیل رسمی و سیستماتیک برای شناسایی یا کمّی‌سازی فرکانس‌ها یا احتمالات و دامنهٔ زیان به دریافت‌کنندگان آن در اثر در معرض مخاطرات (فیزیکی، شیمیایی و یا عوامل میکروبی) قرار گرفتن است که در اثر خرابی‌های ناشی از رویدادهای طبیعی و خرابی‌های سخت‌افزاری و عوامل انسانی حاصل می‌شود.

به طور کلی، ارزیابی ریسک به سه پرسش زیر پاسخ می‌دهد که توسط کاپلان و گاریک مطرح شده‌اند:

- چه چیزی می‌تواند خطرناک باشد؟
- چقدر آن خطر محتمل است؟
- زیان‌های (پیامدهای) آن کدامند؟

پاسخ اولین سؤال منجر به تعیین مجموعه‌ای از سناریوهای نامطلوب (حوادث) می‌شود. سؤال دوم، نیازمند تخمین احتمالات یا فرکانس‌های این سناریوها می‌شود، درحالی‌که سوال سوم دامنهٔ زیان‌های بالقوّه را تخمین می‌زند. پاسخ‌های این پرسش‌های سه‌گانه، توسعهٔ سناریوهای حوادث را به عنوان یک بخش یکپارچهٔ شناسایی و ارزیابی ریسک تشکیل می‌دهد. در واقع سناریوهای ریسک یکی از مهم‌ترین خروجی‌های ارزیابی ریسک هستند.

توسعهٔ سناریوهای ریسک با یک سری «رویداد آغازگر» که سیستم را مختل می‌کنند (رویدادهایی که عملکرد نرمال و یا وضعیت سیستم را تغییر می‌دهند)، آغاز می‌شود. روند تحلیل برای هر رویداد آغازگر، با تعیین رویدادهای بعدی (در قالب سخت‌افزاری، نرم‌افزاری و یا خطاهای انسانی) که ممکن است منجر به پیامدهای نامطلوب شوند، ادامه پیدا می‌کند. احتمال و یا فرکانس هر سناریو نیز با استفاده از روش‌های کمّی و یا کیفی تعیین می‌شود. سپس پیامد مورد انتظار (مقدار زیان) تعیین می‌شود. در پایان، شمار زیادی از چنین سناریوهایی، برای شکل دادن تصویر کامل پروفایل ریسک یک سیستم، کنار هم قرار داده می‌شود.

بنابراین فرایند ارزیابی ریسک، در ابتدا توسعه یک سناریو و محاسبهٔ پیامدهای مورد انتظار هر یک از هر سناریوی ممکن است. از آنجا که فرایند ارزیابی ریسک بر سناریوهایی که منجر به رویدادهای مخاطره‌آمیز می‌شوند، تمرکز دارد، روش عمومی به کار رفته در آن روشی است که شامل شناسایی همهٔ سناریوهای ممکن، محاسبه احتمال مجزای هر یک و تشریح سازگاری پیامدهای ناشی از آنها است. در سیستم‌های مهندسی، توسعهٔ سناریو نیازمند یک سری توضیحات شامل چگونگی مورد تهدید واقع شدن یک سد محدودکنندهٔ یک مخاطره (وقوع رویداد آغازگر)، چگونگی آسیب دیدن سد محدودکنندهٔ مخاطره

و اثرات آن بر بهداشت، ایمنی، محیط و ... می‌باشد. این بدین معنی است که در ارزیابی ریسک، مراحل ۱. شناسایی مخاطرات، ۲. مدیریت ریسک و ۳. ارتباطات ریسک، باید تکمیل شوند.

۲-۴-۱- شناسایی مخاطرات

خطر، موقعیت یا شرایط فیزیکی است که دارای امکان بالقوّه برای یک پیامد نامطلوب (زیان) می‌باشد. در ارزیابی ریسک، باید فرایندهای مورد نظر در تحلیل، به منظور شناسایی مخاطرات نگران‌کننده، مورد پایش قرار گیرند. این مخاطرات را می‌توان به صورت کلی زیر دسته‌بندی کرد:

- شیمیایی (مواد سمّی، عوامل خورنده، دود)،
- زیستی (ویروس‌ها، عوامل میکروبی، آلایندگی‌های زیستی)،
- حرارتی (انفجارها و آتش‌سوزی)،
- مکانیکی (برخورد شیء متحرک، انفجارهای مکانیکی)،
- الکتریکی (میدان‌های مغناطیسی، شوک الکتریکی)
- تشعشع یونیزان (اشعه‌های ایکس، اشعه‌های گاما)،
- تشعشع غیریونیزان (تشعشع امواج مایکرو، اشعه‌های کیهانی)،
- اطلاعات (تبلیغات رسانه‌ای، ویروس رایانه‌ای).

احتمالاً هر یک از این مخاطرات، بخشی از مخاطرات سیستم مورد نظر خواهند بود و سدهای سیستم به عنوان ابزارهایی برای محافظت از سیستم استفاده خواهند شد. این ابزارها که برای جلوگیری از اختلال در سیستم فراهم شده‌اند، خطر را احاطه می‌کنند به نحوی که غیرچالش‌برانگیز باقی بماند. با این حال، در سناریوها رویدادها یا اقداماتی که چنین سدهایی را تهدید و تخریب می‌کنند، فرض شده و پیامد نهایی حاصل از این چالش، تخمین زده می‌شود. بنابراین، توسعهٔ یک سناریو شامل شناسایی مخاطرات، سدها، چالش‌های بالقوّهٔ سدها و میزان مخاطرات است.

۲-۴-۲- شناسایی موانع و سدهای موجود در سیستم

در یک سیستم مهندسی، هر یک از مخاطرات باید برای تعیین همهٔ سدهای فعال و غیرفعال که در معرض خطر هستند و از آن خطر ممانعت به عمل می‌آورند و یا آن را مهار می‌کنند، آزمایش شوند. این سدها ممکن است به صورت فیزیکی خطر را دربر گرفته و ایزوله کنند (سازه‌های غیرفعال مانند دیوارها، لوله‌ها، شیرها، ساختار غلاف سوخت از این نوع هستند)؛ یا

می‌تواند در فاصله‌ای مشخص از چشمهٔ خطر، برای کمینه‌سازی میزان در معرض خطر بودن ایجاد شده باشد؛ یا می‌تواند یک حفاظ مستقیم در برابر خطر برای دریافت‌کنندگان خطر ایجاد نماید (مانند پوشش محافظت‌کننده، سنگر و پناهگاه)؛ و یا ممکن است شرایط در معرض خطر قرارگرفتن را تخفیف دهد (مانند یک واحد سرمایش، یک سیستم اسپری آب، سیستم تخلیه اضطراری).

۲-۴-۳- شناسایی چالش‌های متوجه سدهای ایمنی

شناسایی چالش متوجه هر یک از سدهای مجزا با شناخت الزامات حفظ کارکرد هر یک همراه است. این امر با توسعه یک مدل تحلیلی یا تشریح کیفی الزامات یک سد قابل انجام است. به سادگی می‌توان آنچه برای حفظ یکپارچگی هر سد مورد نیاز است تعیین شود. این الزامات بر اساس حالت‌های تخریب داخلی یا خارجی تحمیل شده و یا دوام یک سد تا حدی که دیگر در برابر بارها و تنش‌های زیر، قابلیت مقاومت نداشته باشد، تعیین می‌شوند.

- تخریب قدرت و یا دوام سد در اثر کاهش ضخامت (به عنوان مثال در اثر تغییر شکل، سایش، خوردگی، پوسیدگی و ...)، و یا تغییر خواص مواد (به عنوان مثال سختی شکست و استحکام تسلیم)،
- افزایش تنش و یا خرابی سد در اثر عوامل داخلی مانند نیروها و یا فشار، و یا نفوذ و یا اعوجاج ناشی از اشیاء و نیروهای خارجی.

مثال‌های فوق از علل تخریب سیستم، اغلب نتایج یک یا چند عامل زیر است:

- درست عمل نکردن تجهیزات فرایند (سیستم خنک‌سازی اضطراری در یک نیروگاه هسته‌ای)،
- مسائل تعامل انسان و ماشین،
- طراحی و نگهداری ضعیف،
- پدیده‌های طبیعی زیان‌بار،
- بسترهای زیان‌آور ساخته شده توسط انسان.

۲-۴-۴- تخمین فرکانس و یا احتمال در معرض مخاطره قرار گرفتن

مرحلهٔ بعدیِ فرایند ارزیابی ریسک، شناسایی سناریوهایی است که در آن ممکن است همهٔ سدهای ایمنی تخریب شده و خطر به دریافت کننده (انسان، محیط، خطوط تولید، سازمان‌ها و ...) برسد و پس از آن، ارائه بهترین تخمین ممکن از احتمال

یا فرکانس هر سناریو است. برای سهولت، سناریوهایی که سطح مشابهی از خطر را با پراکندگی خطر مشابه تحمیل می‌کنند، ممکن است در یک گروه قرار گرفته و احتمالات و یا فرکانس‌های مربوطهٔ آنها تجمیع شود.

۲-۴-۵- ارزش‌گذاری پیامدها

زیان‌های ناشی از در معرض خطر قرار گرفتن، ممکن است به عنوان مثال دربرگیرندهٔ آسیب به مردم، اتلاف دارایی‌ها و یا آلودگی زمین باشد. این زیان‌ها با دانش موجود نسبت به رفتار مخاطرات مربوطه هنگام درمعرض قرارگیری و میزان چنین درمعرض قرارگیری، برای هر سناریو ارزش‌گذاری می‌شوند.

بر اساس طبیعت ذاتی تحلیل ریسک، به نظر می‌رسد که این یک رویکرد عمومی برای درک راه‌های در معرض خطر قرار گرفتن است. این درک برای توسعهٔ سناریوهای قابل حل، بسیار مهم است. حل‌های کمّی و کیفی می‌توانند تخمین‌هایی از مناسب بودن سدها در برابر مخاطرات و روش‌های بهبود مؤثر آن فراهم آورند. این تکنیک که در صنعت هسته‌ای پیشگام است، مبنای شمار زیادی از ارزیابی‌های ریسک مهندسیِ رسمی امروزه است.

۲-۵- مدیریت ریسک

مدیریت ریسک، بر شناسایی، کمّی‌سازی و مشخص کردن عدم قطعیت‌های زیان‌ها تمرکز دارد. در واقع، مدیریت ریسک تلاش برای مدیریت این عدم قطعیت‌ها است. مدیریت ریسک، تمرینی شامل فعالیت‌های هماهنگ‌شده برای ممانعت، کنترل و کمینه‌سازی زیان‌های متحمّل شده در اثر در معرض خطر قرار گرفتن، و نیز وزن‌دهی گزینه‌ها و انتخاب اقدامات مناسب برای لحاظ مقادیر ریسک، قیدهای اقتصادی و فنی و مباحث سیاسی و قانونی است. مدیریت ریسک از شماری از تکنیک‌ها، روش‌ها و ابزارهایی شامل تحلیل سبک و سنگین کردن، تحلیل هزینه-فایده، اثرگذاری ریسک، تحلیل تصمیم چندشاخصه‌ای و تحلیل خرابی پیش‌گویانه (مانند پایش شرایط) بهره می‌برد. تمرکز اولیه در مدیریت ریسک طی سیکل عمر یک سیستم پیچیده شامل اتخاذ تصمیمات پیش‌گویانه برای موارد زیر است:

- ✓ ارزیابی مستمر ریسک (چه موردی می‌تواند اشتباه شود؟)،
- ✓ تصمیم بر اینکه کدام ریسک‌ها برای رسیدگی مهم هستند (اولویت‌بندی ریسک)،
- ✓ به‌کارگیری استراتژی‌هایی برای ممانعت، کنترل و کمینه‌سازی ریسک،
- ✓ ارزیابی مستمر کارایی استراتژی‌ها و بازنگری آنها درصورت نیاز.

مدیریت ریسک، مهم‌ترین و متنوع‌ترین بخش تحلیل ریسک است. مدیریت ریسک خوب، حتی در حضور سیستم‌ها و تکنولوژی‌های با پتانسیل بالای ریسک، می‌تواند در ممانعت، کنترل و یا کمینه‌سازی زیان‌ها بسیار مؤثر باشد. همانگونه که از عنوان مدیریت ریسک پیداست، مدیریت ریسک یک تلاش پیوسته است که از نتایج ارزیابی ریسک آغاز می‌شود. با تغییر محیط داخلی و خارجی سیستم‌های پیچیده، باید ارزیابی ریسک انجام شود. در این حالت نیز مدیریت ریسک با یک تخمین صحیح از ریسک زمانی (آنی و یا متوسط) آغاز می‌شود. با تغییر ترکیب سیستم و سایر عوامل داخلی و خارجی، مؤلفه‌های ریسک نیز تغییر می‌کند. مدیریت ریسک شامل شناسایی مؤلفه‌های اولیه ریسک می‌شود. معمولاً بیش از ۸۰ درصد ریسک، متعلق به کمتر از ۲۰ درصدِ سناریوهای ریسک و یا اجزای سیستم پیچیده است (قانون پارِتو[1]). مدیریت ریسک، شامل شناسایی این ۲۰ درصد مؤلفه‌های ریسک برای کمینه‌سازی آنها است که منجر به حصول بیش‌ترین کاهش ریسک با منابع محدود در دسترس می‌شود. برای انتخاب مؤلفه‌های عمدهٔ ریسک، تکنیک‌های رسمی مانند مقیاس‌های اهمیت به کار می‌روند.

هنگامی‌که مؤلفه‌های عمدهٔ ریسک شناخته شدند، فرایند شناسایی و تحلیل استراتژی‌های ممانعت، کنترل و کمینه‌سازی ریسک شروع می‌شود. کار اولِ شناسایی این است که آیا مؤلفه‌های ریسک به اندازه‌ای مهم هستند که منجر به ریسک کلی و یا منجر به انحراف از حدِ قابلِ قبولِ ریسک شوند. حدود قابل قبول ریسک، به خصوص هنگامی که با ریسک‌های سلامت انسان و محیط مرتبط می‌شوند، به شدت مورد مناقشه قرار گرفته و انتشار آنها بسیار حساسیت‌برانگیز است. با شناسایی طبیعت و اثر مؤلفه‌های قابل توجه ریسک، استراژی‌های جایگزین برای مدیریت آنها باید پیشنهاد شوند. کار بعدی، ارزیابی و انتخاب محتمل‌ترین و مؤثرترین استراتژی برای دفع ریسک (مانند بیمه‌کردن، بازطراحی و ...)، کنترل ریسک (استراتژی‌های تخلیه و فرار، پوشش محافظ و ...) و کمینه‌سازی ریسک (اضافه‌کردن افزونگی، تنوع، موانع در طراحی، بهره‌برداری و نگهداری سیستم) است. فرایند پیداکردن بهترین استراتژی، شامل قضاوت معقولِ ریسک ناشی از تکنیک‌های رسمی مانند هزینه-فایده، اثرگذاری ریسک، تحلیل تصمیم چند منظوره و شمار زیادی از سایر تکنیک‌های بهینه‌سازی است. استراتژی‌ها اغلب در قالب تعیین مسئولیت و تعیین رویکرد مناسب ریسک (تحقیقات بیشتر، پذیرش، مهار و یا پایش) است؛ درصورت مهار ریسک، باید سطح مهار (به عنوان مثال، لیست اقدام و یا نقشه تفصیلی وظایف) و هدف تعریف شود.

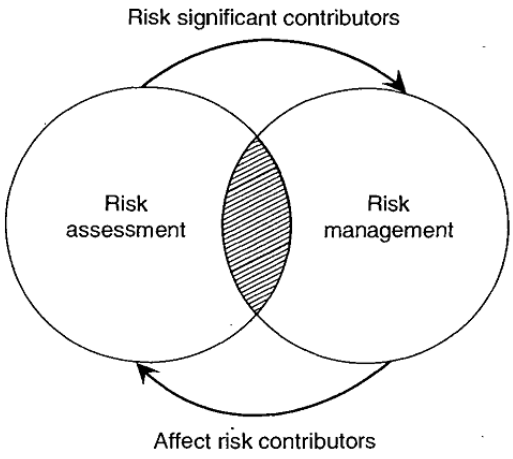
هنگامی‌که بهترین استراتژی انتخاب می‌شود، باید مفاهیمی چون اندازه‌گیری اهمیت، انجام اصلاحات و ویرایش آن هنگام نیاز، در طول زمان پایش شوند. این مشخصه باعث می‌شود مدیریت ریسک یک فرایند پیوسته شود و نه یک تلاش یک‌باره.

[1] - Pareto's Principle

پایش و دنبال‌کردن ریسک شامل به‌روزرسانی، کامپایل کردن، تحلیل کردن و سازماندهی کردن داده‌های ریسک و نیز گزارش‌دهی نتایج و راستی‌آزمایی و اعتبارسنجی اقدامات پیشگیرانه است.

مورگان چهار رویه برای به کارگیری گزینه‌های مدیریت ریسک تعریف می‌کند که شامل قانون آسیب و سایر قوانین عمومی (قوانین مرتبط با کوتاهی و غفلت، مسئولیت، آزار، تخلف و غیره)، بیمه (شخصی یا دولتی برای انتقال ریسک به دیگران)، استانداردهای اختیاری (مانند انجمن ملی حفاظت در برابر آتش‌سوزی) و استانداردها و قوانین دولتیِ اجباری است.

بر اساس مطالب ارائه شده روشن است که ارزیابی و مدیریت ریسک به‌دقت در هم تنیده است. همانطور که در شکل ۲ ارائه شده است، ارزیابی ریسک برای فهم مؤلفه‌های ریسک و اندازه‌گیری تغییرات در چنین مؤلفه‌هایی در طول زمان است. مدیریت ریسک از مؤلفه‌های ریسک برای تعیین استراتژی معقول و نیز به‌کارگیری منابع اندک برای ممانعت، کنترل، کمینه‌سازی و پیمایش مؤلفه‌های عمده استفاده می‌کند.



شکل ۲: رابطهٔ بین ارزیابی ریسک و مدیریت ریسک

هنگامی که یک استراتژی جدید اتخاذ می‌شود، ریسک می‌تواند تغییر کند و ممکن است منجر به مؤلفه‌های جدید و متفاوتی (با اهمیت یکسان، کمتر و یا بیشتر) شود که با تلاش‌های بیشتر در زمینهٔ ارزیابی ریسک، قابل اعتبارسنجی بوده و چرخهٔ همکاری بین ارزیابی و مدیریت ریسک ادامه می‌یابد.

۲-۶- ارتباطات ریسک

ارتباطات ریسک فعالیت انتقال، مبادله و به‌اشتراک‌گذاری اطلاعات، داده‌ها و دانش در مورد ریسک، نتایج تحلیل ریسک و رویکرد مدیریت ریسک بین تصمیم‌گیران، تحلیل‌گران و سایر عوامل دخیل است. اطلاعات می‌تواند مربوط به وجود، قالب،

احتمال، فرکانس، دقت، مقبولیت، کنترل‌پذیری و یا سایر جنبه‌های ریسک باشد. بسته به اینکه چه چیزی و به چه کسی باید تبادل شود، ارتباطات ریسک حاوی اطلاعاتی در موارد زیر است.

۲-۶-۱- نوع ریسک

مشخصات مهم، طبیعت، قالب، اهمّیت و شدت ریسک و اولویت موقعیت آن، در این مقوله قرار می‌گیرند. به‌علاوه، مشخصات دینامیکی و کمّی ریسک باید مشخص شود که شامل رفتار ریسک (افزایشی، کاهشی یا ثابت بودن)، احتمال یا فرکانس در معرض ریسک قرار گرفتن، مقدار در معرض قرارگیری که دربردارندهٔ ریسک قابل توجه است و مشخصات و اندازهٔ جمعیت در معرض ریسک است. در نهایت، دریافت‌کنندگان ویژهٔ ریسک، که بیشترین ریسک را دارند، باید شناسایی شوند.

۲-۶-۲- نوع منافع

اغلب یک پرسش کلیدی در مدیریت ریسک این است که آیا منفعت بیشتر از ریسک است یا خیر؟ اگر ما ریسک را تنها با زیان‌ها (و نه منافع) همراه بدانیم، آنگاه از ریسک بیزار خواهیم شد؛ به این معنی که ما تنها ریسک‌های خود را کنترل و کاهش می‌دهیم. لازم است توجه شود که اقدامات انجام شده برای کاهش ریسک، از این جهت که زیان‌های ممکن را کاهش می‌دهند، می‌توانند گاهی به عنوان منافع لحاظ شوند. ما نیاز به لحاظ مزایای مستقیم یا غیرمستقیم ریسک داریم. این مزایا شامل نوع منافع مانند منافع واقعی یا منافع مورد انتظار است که با ریسک و ذینفعان مستقیم و غیرمستقیم ریسک مرتبط هستند. به‌علاوه، تعادل بین ریسک‌ها و منافع، دامنه و اهمیت منافع، و مقدار کلّی منافع به کل آسیب‌ها باید به صورت کمّی و کیفی روشن شود.

۲-۶-۳- عدم قطعیت در ارزیابی ریسک

هر ارزیابی پیش‌بینانه مبتنی بر یک مدل است که ذاتاً قطعی نیست. علاوه براین، فرایند تهیهٔ چنین مدل‌هایی (برای مثال در تخمین پارامترهای مدل) از داده‌ها و تجربه‌های خام نیز حاوی عدم قطعیت است. ارزیابی ریسک نیز از این امر مستثنی نیست. سوال اغلب این نیست که آیا در یک ارزیابی، استراتژی مدیریت و یا تحلیل، عدم قطعیت وجود دارد یا خیر، بلکه سوال این است که چه میزان عدم قطعیت وجود دارد؟ در شناسایی عدم قطعیت‌ها در ارزیابی ریسک، بحث در مورد روش‌ها، مدل‌ها و تخصص‌های به‌کاررفته در ارزیابی ریسک ضروری است. همچنین توصیف اهمیت هر یک از عدم قطعیت‌ها، ضعف‌ها، عدم دقت‌ها در داده‌های در دسترس ضروری است. یک مشخصهٔ عمومی دیگر هر تحلیل، فرضیات آن است. اساس و حساسیت ریسک و استراتژی‌های مدیریت ریسک (شامل تصمیمات و مقررات) برای تغییر فرضیات نیز باید بررسی شود.

۲-۶-۴- گزینه‌های مدیریت ریسک

یک المان کلیدی هر ارتباط مؤثر، جزئیات نوع گزینه‌های لحاظ شده برای رسیدن به یک استراتژی، سیاست و یا مقررات و نیز اقدامات مدیریت ریسک است. چه اقداماتی، برای کاهش درمعرض ریسک قرار گرفتن در دسترس است؟ به‌علاوه، ارتباطات باید برای قضاوت به منظور انتخاب یک گزینهٔ مدیریت ریسک خاص و اثرگذاری آن گزینه با جزئیات تعیین شود. بر این اساس، گزینه‌های مدیریت ریسک را می‌توان از دید مزایای آنها، مانند مفید بودن و منافع گزینه‌هایی که باید شناسایی شوند، نگریست. ارتباطات هزینهٔ مدیریت ریسک و پرداخت‌کنندهٔ آن (مستقیم یا غیرمستقیم) نیز حیاتی است. در نهایت، ریسک‌هایی که پس از به کارگیری یک گزینهٔ مدیریت ریسک باقی می‌مانند، باید به روشنی تعیین شوند.

۲-۷- المان‌های ارزیابی ریسک

۲-۷-۱- انواع ارزیابی ریسک

در این بخش المان‌های اصلی ارزیابی ریسکِ مهندسی مورد بحث قرار می‌گیرد. روش‌های ارزیابی ریسک توسط دولت‌ها و صنایع برای تخمین ایمنی، قابلیت اطمینان و اثربخشی محصولات، فرایندها و تأسیسات مختلف به کار می‌روند. یک تحلیل ریسک می‌تواند بر اثرات بهداشتی انتشار آلایندگی شیمیایی در محیط متمرکز باشد. این نوع تحلیل ریسک، راجع به ارزیابی ریسک بهداشت است. یک تحلیل ریسک دیگر ممکن است بر اثرات نامناسب اقتصادی، محیطی و بهداشت ناشی از خرابی یک سیستم مهندسی در اثر رویداد طبیعی یا انسانی به همراه خرابی سدهای حفاظتی تمرکز داشته باشد. این نوع از ارزیابی ریسک، از نوع تحلیل ریسک مهندسی است. هنگامی که از هر دو نوع ارزیابی ریسک صحبت می‌شود، تمرکز بر تحلیل ریسک مهندسی و روش‌های ارزیابی ریسک ایمنی است. در یک ارزیابی ریسک مهندسی، تحلیل‌گر فرکانس یک رویداد، سناریویی از رویدادهای متوالی و احتمالات چنین خرابی‌هایی در سیستم مهندسی را در نظر می‌گیرد. ولی در ارزیابی ریسک بهداشت، تحلیل‌گر پیامدهای شرایط انتشار مزمن مقدار مشخصی از مواد خطرناک در محیط را بدون لحاظ مقدار فرکانس یا احتمال انتشار آن، ارزیابی می‌کند.

راه‌های اندازه‌گیری پیامدها نیز در ارزیابی‌های ریسک مهندسی و بهداشت، متفاوت است. در ارزیابی ریسک بهداشت مدلی برای میزان دریافت آلودگی از آلاینده‌ها و مواد سمّی و اثرات آنها (مدل‌های دوز - پاسخ) توسعه می‌یابند و پیامدها عمدتاً در قالب مرگ و میر سرطانی هستند. در ارزیابی ریسک مهندسی، پیامدهای عمومی شامل سلامت و ایمنی کارکنان، زیان‌های

اقتصادی، مرگ و میر سریع و مرگ و میر سرطانی (بلندمدت) در اثر در معرض تشعشع، مواد سمّی یا بیولوژیکی قرارگرفتن، می‌باشد.

مهم‌ترین کاربرد ارزیابی ریسک مهندسی، تعیین مقادیر حدّ پایین ریسک تحت عنوان مرگ و میر یا سایر زیان‌ها نیست، بلکه حصول بینشی از ملاحظات سیستماتیک است. این بینش به ما می‌گوید در یک سیستم چه خطایی ممکن است رخ دهد و کدام بخش از سیستم، مهم‌ترین سهم را در این زیان دارد؟

۲-۷-۲- ریسک و خطر

مفاهیم «خطر» و «ریسک» گاهی به اشتباه به جای یکدیگر به کار می‌روند. در تحلیل ریسک، این دو مفهوم تعریف دقیق و مشخصی دارند. مفهوم خطر به وجود پتانسیل تولید یک پیامد نامطلوب، بدون لحاظ فرکانس یا احتمال آسیب، مربوط است که ماهیت بالقوه دارد. به عنوان مثال، خطر استفاده از توان هسته‌ای عبارت است از انتشار مقادیر زیاد مواد پرتوزا به محیط در اثر وقوع حادثه‌ای که می‌تواند منجر به پیامدهای ممکن نامطلوب، مانند آلودگی زمین، شود. بنابراین، انتشار زیاد مواد رادیواکتیو می‌تواند به عنوان یک «خطرِ» ناشی از یک نیروگاه هسته‌ای لحاظ شود. مفهوم ریسک نه تنها شامل وقوع یک پیامد نامطلوب است، بلکه احتمال وقوع چنین پیامدی را نیز دربر دارد. با این بیان، ممکن است دو نیروگاه «مخاطرات یکسان» و «ریسک‌های متفاوتی» داشته باشند. تفاوت ریسک‌ها ناشی از تفاوت احتمال وقوع مخاطرات است که وابسته به میزان اثرگذاری سدهای ایمنی برای جلوگیری از انتشار مواد رادیواکتیو است.

۲-۷-۳- ارزیابی ریسک مهندسی

ارزیابی ریسک مهندسی شامل پاسخ به پرسش‌های زیر است:

۱. چه اشتباهی ممکن است رخ دهد، که منجر به مواجهه با خطر شود؟
۲. احتمال وقوع آن چقدر است؟
۳. پیامدهای مورد انتظار آن چیست؟

برای پاسخ به سوال اول، لیستی از سناریوهایی رویدادهای منجر به خروجی مورد نظر باید تعریف شوند. برای پاسخ به سوال دوم، احتمال یا فرکانس این سناریوها باید تخمین زده شود و در پاسخ به سوال سوم، پیامد ناشی از هر سناریو باید محاسبه شود. بر اساس این تعریف، ریسک به صورت کمّیِ زیر قابل تعیین است.

$$R = \langle S_i P_i C_i \rangle, i = 1,2,...,n \quad (۱-۲)$$

در این رابطه، S_i یک سناریو از رویدادهایی است که منجر به مواجهه با خطر می‌شود، P_i احتمال سناریوی i و C_i پیامد ناشی از وقوع رویدادهای سناریو (مقیاسی از میزان زیان) است.

یک بیان سادهٔ ریاضی ریسک (زیان مورد انتظار) سازگار با رابطهٔ فوق به صورت زیر است:

ریسک (پیامد به ازای واحد زمان یا مکان) = فرکانس (دفعات وقوع رویداد در واحد زمان یا مکان) × دامنه (پیامد به ازای رویداد)

به عنوان مثال با لحاظ اعداد فرضی، ریسک مرگ و میر سالانه در اثر حوادث اتوموبیل به صورت زیر محاسبه خواهد شد:

$$\left(15\times10^{6}\frac{accident}{year}\right)\left(\frac{1}{300}\frac{fatality}{accident}\right)=50,000\frac{fatality}{year} \quad (۲-۲)$$

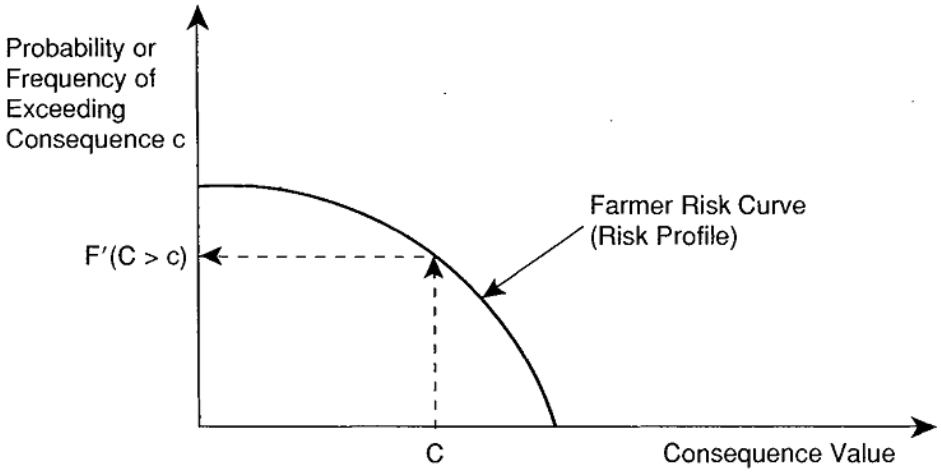
در این مثال، به سادگی با داشتن آمار تصادفات در سال و تعداد مرگ و میر به ازای تصادفات، ریسک (تعداد مرگ و میرهای حوادث اتوموبیل در سال) حاصل می‌شود. اما همیشه محاسبهٔ ریسک به همین سادگی نیست. برای دانستن ریسک حوادث هسته‌ای، انفجارهای گاز طبیعی فشرده و حوادثی از این قبیل، پایگاه دادهٔ آماری وجود ندارد و به جای آن، استفاده از فرمول‌ها کاربردی خواهد بود. برای تخمین فرکانس رویدادهای منجر به مواجهه با خطر (حوادث) و دامنهٔ این پیامدها، به روش دیگری نیاز است؛ یک روش رسمی ساختارمند. این همان چیزی است که ارزیابی ریسک احتمالاتی تلاش می‌کند انجام دهد.

رابطهٔ فوق را می‌توان به صورت کلی زیر نوشت:

$$R = \sum_i f_i c_i \quad (۳-۲)$$

در این رابطه، f_i فرکانس سناریوی i و c_i پیامد این سناریو است.

یک راه برای به دست آوردن مقادیر ریسک نهایی استفاده از منحنی‌های فارمر است. در این روش، پیامد بر حسب توزیع تجمعی فرکانس رویداد (سناریو) رسم می‌شود. این نمودارها اغلب برای نشان دادن پروفایل ریسک سیستم‌های مهندسی بسیار مفید هستند.



شکل ۳: مثالی از پروفایل ریسک

رابطه ارائه شده برای محاسبه ریسک یک نقص جدی دارد. این نقص در مقایسهٔ ریسک‌های پدیده‌های مختلف مشخص می‌شود. برای نشان دادن این مسأله، یک رویداد با فرکانس وقوع $۱۰^{-۶}$ بار در سال و پیامد $۱۰^{۶}$ مرگ به ازای وقوع رویداد و رویداد دیگری با فرکانس وقوع ۰/۱ بار در سال و پیامد ۱۰ مرگ به ازای وقوع رویداد را در نظر بگیرید. براساس رابطهٔ ارائه شده، ریسک هر دو رویداد برابر ۱ مرگ در سال است. در حالی‌که احساس و درکی که از ریسک برای این دو رویداد وجود دارد، با ریسکِ واقعیِ محاسبه شده بسیار متفاوت است. این مسأله به دلیل است که جامعه یا افراد نسبت به رویدادهای با پیامدهای بزرگ، بی‌تفاوت نیستند، بلکه بسیار ضدّ ریسک بوده و از آن بیزارند. برای انعکاس این نوع از بیزاری از ریسک، رابطهٔ ارائه شده برای ریسک باید تغییر کند، به‌گونه‌ای که میزان نفرت از ریسک را لحاظ کند. تعدادی از سایر روابط تابعی بین فرکانس و پیامد در مقالات قابل یافتن است که البته هیچ‌یک هنوز مقبولیّت گسترده‌ای را نداشته است و در ارزیابی ریسک احتمالاتی عموماً محاسبه ریسک از همین رابطهٔ ارائه شده انجام می‌شود. همچنین محاسبهٔ تابع توزیع فرکانس ریسکِ سناریو بر حسب دامنهٔ پیامد آن رایج است. نحوهٔ لحاظ بیزاری از ریسک بیشتر در فرایند تصمیم‌گیری در نظر گرفته می‌شود.

کلید تعیین فرکانس f_i در درک مفهوم احتمال است. دو تعریف کاملاً متفاوت از احتمال وجود دارد. از دید آمار کلاسیک، احتمال به صورت یک ویژگی از یک فرایند یا رویداد است که می‌تواند از شمار داده‌های بی‌نهایت به دست آید. به عنوان مثال، احتمال آمدن یک روی سکه (P_H) به صورت زیر تعریف می‌شود:

$$P_H = \frac{N_H}{N} \qquad N \to \infty \qquad (۴-۲)$$

در این رابطه، N_H تعداد آمدن روی H سکه و N تعداد دفعات آزمایش پرتاب سکه است. کارشناسان آمار روش‌هایی برای تخمین این احتمال (P_H) و میزان اطمینان به آن با تعداد داده‌های کمتر از بی‌نهایت به کار می‌برند. افرادی که این رویکرد را به کار می‌برند، تحت عنوان دیدگاه فرکانسی شناخته می‌شوند و اعتقاد دارند که P_H یک مقدار «دقیق» و «معین» است و تخمین آن فقط از طریق مشاهدات فرایند یا رویداد حاصل می‌شود. بنابراین اگر ۱۰۰ بار سکه را به هوا پرتاب کنیم و ۴۸ بار آن روی H بیاید، دیدگاه فرکانسی می‌گوید که احتمال آمدن روی H در یک سکه برابر ۰/۴۸ است.

دیدگاه دیگر، معروف به دیدگاه ذهنی است که بر اساس آن مقدار P_H در هر زمان دارای یک مقدار است که وابسته به دانش در دسترس در مورد فرایند یا رویداد در آن زمان است. بنابراین، اگر یک سکه پیش از پرتاب به دقت بررسی شده و دریافت شود که یک روی شیر و یک روی خط داشته و به صورت کامل متقارن باشد، یک فرد با رویکرد ذهنی خواهد گفت که احتمال P_H برابر ۰/۵ است. این قضاوت مبتنی بر دانش قبلی از سکه و فرایند پرتاب آن است و منحصر در مشاهدات بخصوصی نمی‌باشد.

حال فرض کنید که سکه ده بار پرتاب شده و ۷ بار شیر و ۳ بار خط آمده باشد. در این حالت، بهترین تخمین از دیدگاه فرکانسی برابر ۰/۷ است. اما فرد ذهن‌گرا این مشاهده را به دانش پیشین خود به‌گونهٔ سازگار و منطقی می‌افزاید. رابطهٔ مشهور تئوری بایز مکانیزم ترکیب مزایای دیدگاه‌های مبتنی بر دانشِ قبلی و مشاهدات واقعی است. در بخش سوم گزارش به ریاضیات احتمالاتی بیشتر پرداخته شده است.

در استفاده از ارزیابی ریسک احتمالاتی در سیستم‌های مهندسی با پیامدهای نامطلوبِ بزرگ و احتمالِ وقوعِ کم باید منطق رویکرد ذهن‌گرا (یا بایزین) به کار رود، چراکه داده‌های کمی برای تعریف‌های دیدگاه فرکانسی وجود خواهد داشت. اگرچه برخی مناقشات هنوز بین این دو دیدگاه فکری وجود دارد، رویکرد بایزین بیشتر مورد پذیرش است.

۲-۷-۴- عملکرد و ارزیابی عملکرد

عملکرد یک سیستم، قابلیتِ سیستم در درک وظایف تعیین شده در همهٔ زمان‌ها است. قابلیتِ سیستم می‌تواند کیفی یا کمّی باشد. کارکردِ کمّی یک مقولهٔ یقینی نیست و یک احتمال برای قابلیتِ درکِ وظایفِ تعیین شده در زمانِ نیاز یا بازهٔ زمانی مطلوب وجود دارد.

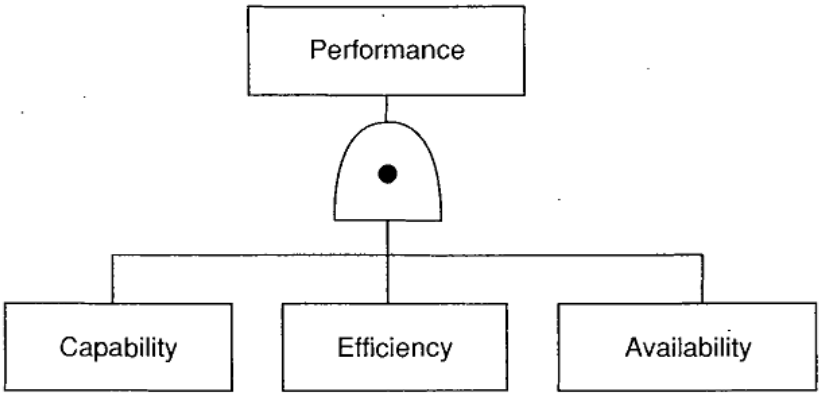
برای بررسی بهتر، عملکرد سیستم به سه مؤلفهٔ قابلیت، کارایی و دسترسی (شکل ۴) تقسیم می‌شود. قابلیت، مقیاس احتمال انجام وظایف سیستم تحت همهٔ شرایط داخلی و خارجی طی زمان مأموریت است. با دانستن اینکه شرایط داخلی و خارجی

و مأموریت‌ها می‌توانند تعداد، اندازهٔ چالش‌ها و ظرفیت سیستم را تحت تأثیر قرار دهند، احتمال اینکه سیستم وظایف خود را انجام دهد بر حسب زمان تغییر می‌کند. به عبارت دیگر احتمال انجام وظایف سیستم وابسته به سطح چالش‌ها (مانند تنش تحمیلی) و ظرفیت (مانند تحمل در برابر خستگی) است.

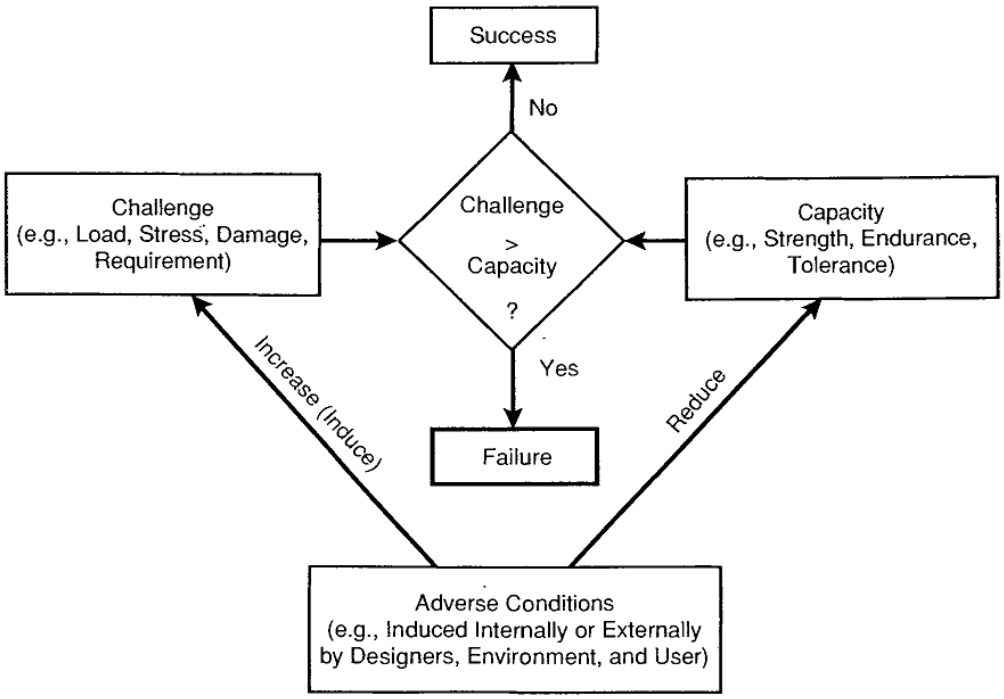
خرابی‌ها نتیجهٔ وجود چالش‌ها و شرایط ایجاد شده در یک سناریوی خاص هستند. هر سیستم، دارای یک ظرفیت درونی برای تحمّل یا مقابله با چنین چالش‌هایی است. این ظرفیت ممکن است با شرایط داخلی یا خارجی خاصی در طول زمان یا دوره‌های کاری مختلف، کاهش یابد. هنگامی که چالش‌ها بر ظرفیت سیستم فائق می‌آیند، خرابی رخ می‌دهد. تعاریف مختلفی برای ظرفیت و چالش در مدل‌های ویژه به کار می‌رود. شکل ۵ المان‌های تشکیل چارچوب مدل‌های خرابی را نشان می‌دهد.

کارایی، مقیاسی از اثربخشی در درک وظایف تعیین شده است که با مقایسهٔ ورودی و خروجی سیستم مشخص می‌شود. به عنوان مثال، سیستمی که بسیار سنگین است، حاصلِ کمی دارد، پرهزینه است، با زحمت کار می‌کند، انرژی بسیار زیاد مصرف می‌کند، یا محیط را آلوده می‌سازد.

قابلیت دسترسی، حالت سیستم را نشان می‌دهد که به صورت احتمالاتی محاسبه می‌شود. در یک بازهٔ زمانی که سیستم در اثر خرابی خاموش است، سیستم قادر به انجام وظیفه مشخص شده نیست و در دسترس نمی‌باشد.



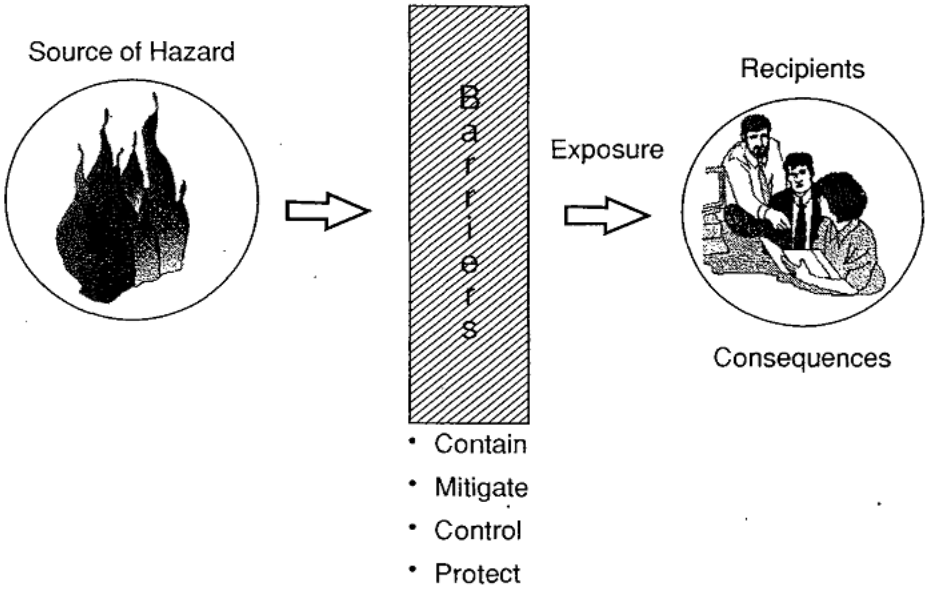
شکل ۴: المان‌های عملکرد: قابلیت، کارآیی، دسترسی



شکل ۵: چارچوب خرابی یا موفقیت یک سیستم

۲-۷-۵- المان‌های ارزیابی ریسک مرسوم

ارزیابی ریسک شامل دو نوع کمّی و کیفی است. در ارزیابی کیفی، پتانسیل و پیامد آسیب‌ها به صورت کیفی با عبارت‌های زیاد، متوسط و کم یا درجه‌های عددی توصیف می‌شود. ارزیابی ریسک کمّی از احتمالات برای اندازه‌گیری پتانسیل آسیب و مقدار واقعی زیان برای حصول پیامد استفاده می‌کند. فرایند ارزیابی ریسک برای هر دو نوع تحلیل، یکسان است. همانطور که در شکل ۶ نشان داده شده است، ارزیابی ریسک شامل شناخت منابع مخاطرات، سدها و موانع در برابر مخاطرات، دریافت کنندگان مخاطرات و پیامدهای دریافتِ مخاطرات است.



شکل ۶: نمای کلی اجزای ارزیابی ریسک

۲-۷-۵-۱- مراحل ارزیابی ریسک

مراحل اصلی که در هر دو نوع ارزیابی ریسک کمّی و کیفی به کار می‌روند، عبارتند از:

شناسایی ریسک - در این مرحله، منابع، مقدار و شدت مخاطراتی که می‌توانند منجر به آسیب به انسان، محیط و جامعه شوند، شناسایی می‌شوند. دو طیف از مخاطرات وجود دارد: مخاطرات با منشأ طبیعی و مخطرات با منشأ مصنوعی. مخاطرات با منشأ طبیعی مانند: سیل، طوفان، رانش زمین، سونامی، اشعه‌های کیهانی، بیماری‌های واگیردار ناشی از باکتری‌ها، ویروس‌ها و قارچ‌های طبیعی. مخاطرات با منشأ مصنوعی مانند: مواد قابل اشتعال مانند هیدروژن، آمونیاک، پروپان، مواد واکنش‌دهنده مانند فلورین، پراکسید هیدروژن، نیتریت‌ها، مواد خورنده مانند اسیدهای قوی، کلرویدهای غیرفلزی، هالوژن‌ها، مواد سمی، مواد پرتوزا و ... .

شناسایی سدهای مقابل ریسک – سدها عمل حفاظت، حذف، خنثی‌سازی، ممانعت، مهار، کنترل یا اخطار انتشار مخاطرات را انجام می‌دهند. دو نوع سد وجود دارد: سدهای فعال و سدهای غیرفعال. سدهای فعال تجهیزات، سیستم‌ها و ابزارهای فیزیکی هستند که برای انجام یکی از اهداف ذکر شده، فعال می‌شوند. سدهای غیرفعال به‌صورت دائمی، به عنوان مثال با استفاده از پدیده‌های طبیعی مانند گردش طبیعی سیال، برای انجام یکی از مقاصد فوق به کار می‌روند.

مثال‌های سدهای فعال عبارتند از: اپراتور (نیروی انسانی کنترل کنندهٔ سیستم)، سیستم‌های خنک‌کننده، سیستم‌های کنترلی، سیستم‌های اخطار، سیستم‌های هوشمند، سیستم‌های تخلیه، سیستم‌های اطفای حریق، خودروهای فضایی، حفاظ‌های انسانی و سیستم‌های پاسخ اضطراری.

مثال‌های سدهای غیرفعال عبارتند از: لوله‌ها، محفظه‌ها و ساختارهای محافظ، مخازن سرمایش ثقلی، پوشش‌های حفاظتی و سیستم گردش طبیعی هوا.

اغلب یک یا چند سد از این سدها باید به صورت مؤثر برای فراهم آوردن حفاظت لازم به کار روند. یک بخش مهم ارزیابی ریسک، بررسی کفایت و شایستگی عملکرد سدها برای مهار خطر می‌باشد.

ارزیابی عملکرد سدها – سدها کامل نیستند و ممکن است موفق به برآمدن از وظیفهٔ تعیین شده نباشند. این امر می‌تواند در اثر خرابی یا ایجاد نقص در اجزای آن سد باشد. به عنوان مثال، مخزن گاز طبیعی یا مواد رادیواکتیو می‌تواند در اثر شرایط زیر خراب شود:

- رسیدن تنش ناشی از گاز به مقاومت استحکام مخزن،
- رسیدن خرابی تجمعی در سد به مقدار نهایی (به عنوان مثال رشد ترک در اثر خستگی)،
- کاهش استحکام سد در اثر عوامل شیمیایی یا مکانیکی منجر به کاهش ضخامت یا تغییر خواص مواد،
- عیب در تجهیزات فرایندی مانند سیستم سرمایش،
- خطاهای انسانی در اثر ضعیف بودن واسط بین سیستم و انسان یا در اثر ارتباطات ضعیف سازمانی،
- نگهداری ضعیف که منجر به بازیابی صحیح ماشین آلات نشود،
- پدیده‌های طبیعی زیان‌بار،
- محیط عملکردی نامناسب.

یک جنبهٔ کلیدی هر ارزیابی ریسک، ارزیابی و توصیف کمّی یا کیفی عملکرد (به عنوان مثال، قابلیت اطمینان و در نتیجه احتمال یا امکان خرابی یک سد) در هر سناریوی حاوی خرابی یک یا چند سد است. محاسبات باید همواره شامل عدم قطعیت‌های مرتبط با مقادیر تخمین‌زده شده باشد. روش‌های بسیاری در ارزیابی ریسک برای محاسبهٔ عملکرد سدها به کار رفته است.

ارزیابی در معرض ریسک قرار گرفتن – در این مرحله تلاش می‌شود میزان و مشخصات (سمیّت، غلظت، دما و ...) حاصل از انتشار مخاطرات ارزیابی شود. در ارزیابی کیفی، این مرحله اغلب با محاسبات ساده یا به‌طور کلی مرتبط با قضاوت متخصّصان انجام می‌شود. در ارزیابی کمّی، مدل‌های خرابی سدها معمولاً توسعه می‌یابند و میزان درمعرض ریسک قرار گرفتن تخمین زده می‌شود. تخمین کمّی همواره شامل توصیف عدم قطعیّت‌های مرتبط با مقادیر ریسک است.

توصیف ریسک – مرحلهٔ نهایی، اندازه‌گیری فرکانس و دامنهٔ پیامدهای درمعرض خطر قرار گرفتن است. در این مرحله ابتدا مسیرهای درمعرض خطر قرار گرفتن و دریافت‌کنندگان شناسایی می‌شوند. سپس رابطه بین میزان درمعرض خطر قرارگیری دریافت‌کنندگان و پیامدها تعیین شود. به عنوان مثال، در مطالعهٔ ریسکِ سرطان انسان در اثر انتشار مواد پرتوزا به محیط ناشی از خرابی چند سد ایمنی در نیروگاه هسته‌ای، دریافت کنندهٔ خطر، انسان و پیامد آن سرطان حاصل از پرتو است. در اینجا، ممکن است از روابط میزان سرطان در اثر درمعرضِ خطرِ تشعشعِ گامای کل بدن (یا مدل پاسخ - دُز) قرار گرفتن، استفاده شود. بر اساس این مدل، میزان تشعشع (نفر-rem) ۱۰۰۰۰ از لحاظ آماری منجر به یک مورد سرطان می‌شود (rem یک واحد بزرگ برای اندازه‌گیری تشعشع یونیزان است). این بدان معنی است که اگر ۱۰۰ نفر هر کدام ۱۰۰ rem یا ۲۰۰ نفر هر کدام ۵۰ rem دریافت کنند، از لحاظ آماری یک مورد سرطان مورد انتظار است. این یک رابطهٔ کمّی احتمالاتی است. روابط دیگرِ کیفی یا از نوع آستانه‌ای (غیراحتمالاتی) نیز ممکن است استفاده شوند. به عنوان مثال، در یک رابطهٔ آستانه‌ای، در معرض اشعه قرار گرفتن یک عضو از بدن به میزان ۱۰۰۰ rem یا بیشتر، معادل از دست رفتن آن عضو لحاظ می‌شود.

پس از تعیین پیامد، مقدار ریسک با استفاده از رابطهٔ معروف ریسک محاسبه می‌شود که حاصل‌ضرب پیامد در فرکانس آن رویداد است. در ادامه مثالی از مراحل ارزیابی ریسک برای مسألهٔ بهداشت ارائه شده است:

- شناسایی خطر: تعیین ماهیت و مقدار آلودگی محیطی که می‌تواند سلامت انسان را به مخاطره اندازد.
- توصیف خطر: ارزش‌یابی رابطهٔ بین میزان درمعرض قرارگیری و میزان شیوع اثرات نامطلوب در انسان. در این مرحله، یک ارزش‌یابی کمّی یا کیفی از طبیعت اثرات نامطلوبِ مرتبط با عوامل بیولوژیکی، شیمیایی و فیزیکی قابلِ حصول است.
- ارزیابی درمعرض خطر قرار گرفتن: تعیین شرایطی که مردم می‌توانند درمعرض آلودگی قرار گیرند و دُزهایی که می‌توانند درنتیجهٔ این اتفاق رخ دهند که شامل ارزش‌یابی کمّی و کیفی میزان ورودی محتمل می‌باشند.

- توصیف ریسک: شرح طبیعت اثرات نامطلوبی که می‌توان آنها را به آلودگی منتسب دانست، تخمین احتمال آنها در جامعه آلوده شده، و ارزش‌یابی قوّت شواهد و عدم قطعیت‌های مرتبط با آنها که شامل یکپارچه‌سازی شناسایی خطر، توصیف خطر و ارزیابی درمعرض آن قرار گرفتن است.

۲-۷-۶- ارزیابی ریسک کیفی

معمولاً انجام تحلیل ریسک کیفی آسان‌تر است چراکه نیازمند جمع‌آوری داده‌های دقیق نیست. در این روش، تخمین‌های درجه‌ای کافی است و اغلب به سرعت تخمین زده می‌شوند. تخمین‌های درجه‌ای احتمال و پیامد کیفی می‌تواند تخمین‌های مفیدی برای ریسک به‌دست آورد. به عنوان مثال، تخمین مقیاس احتمال از کم تا زیاد تعریف می‌شود. دسته‌بندی احتمال کیفی و تعریف‌های مربوط به آنها به صورت زیر است:

۱. مکرر[۱] – اغلب طی عمر یک جزء یا سیستم یا اغلب در عملکرد تعداد زیادی اجزای مشابه به صورت محتمل رخ می‌دهد.
۲. محتمل[۲] – طی عمر یک جزء یا سیستم یا اغلب در عملکرد تعداد زیادی اجزای مشابه چندبار رخ می‌دهد.
۳. گاه و بی‌گاه[۳] – طی عمر یک جزء یا سیستم گاهی رخ می‌دهد یا چندبار در طول عمر شمار زیادی از اجزای مشابه رخ خواهد داد.
۴. احتمال بسیار کم[۴] – طی عمر یک جزء یا سیستم ممکن است گاهی رخ دهد اما محتمل نیست یا به صورت معقولی در طول عمر تعداد زیادی از اجزای مشابه مورد انتظار است.
۵. غیرمحتمل[۵] – طی عمر یک جزء یا سیستم بسیار غیرمحتمل است که رخ دهد به‌گونه‌ای که ممکن است فرض شود وقوع آن تجربه نشده است، یا در طول عمر تعداد زیادی اجزای مشابه وقوع ممکن است اما به صورت غیرمحتمل.
۶. غیرقابل انتظار[۶] – به عنوان رویداد فیزیکی که انتظار وقوع آن طی عمر تأسیسات یا سیستم‌های بزرگ مشابه نمی‌رود.

[۱] - Frequent
[۲] - Probable
[۳] - Occasional
[۴] - Remote
[۵] - Improbable
[۶] - Incredible

به‌طور مشابه، پیامد به صورت روند نزولی قابل تعریف است. در جدول شماره ۱ مثالی از مقادیر ریسک مرتبط با هر دستهٔ فرکانس – پیامد ارائه شده است.

جدول شماره ۱: ماتریس ارزیابی ریسک کیفی

Frequency of Occurrence	Frequency (per Year)	Severity of Consequence			
		Catastrophic	Critical	Marginal	Negligible
Frequent	>1	H	H	H	I
Probable	$1–10^{-1}$	H	H	I	L
Occasional	$10^{-1}–10^{-2}$	H	H	L	L
Remote	$10^{-2}–10^{-4}$	H	H	L	L
Improbable	$10^{-4}–10^{-6}$	H	I	L	T
Incredible	$<10^{-6}$	I	I	T	T

تعریف دسته‌ها و مقادیر به کار رفته در ماتریس فوق تنها جنبهٔ مثال دارند. در ماتریس فوق، H نشان‌دهندهٔ ریسک بالا، I ریسک متوسط، L ریسک پایین و T ریسک ناچیز است. به عنوان مثال، وخامت دسته‌های پیامد به صورت زیر قابل تعریفند:

۱. فاجعه‌انگیز – شامل مرگ و میر بسیار، از دست رفتن سیستم یا تأسیسات، مانند از دست رفتن قابل توجه تولید و منفعت عمومی و وقوع مداخلهٔ سازمانی.
۲. بحرانی – شامل تعداد کمی مجروح، خرابی عمدهٔ سیستم یا سایر رویدادهایی که منجر به از دست رفتن تولید، آسیب به بیش از یک ساختمان یا ناحیه یا قابلیت منجرشدن به پیامدهای فاجعه‌انگیزی تحت شرایط مختلف محیط.
۳. مرزی – جراحت حداقلی، خرابی سیستم حداقلی یا سایر رویدادهایی که به یک ساختمان یا ناحیه محدود می‌شوند.
۴. ناچیز – رویدادی که اغلب قابل صرف‌نظر کردن است.

با ضرب احتمال در پیامد، سطح ریسک به دست می‌آید. در ادامه مثالی برای ارزیابی کیفی ریسک ارائه می‌شود. سیستم اتوبوس‌های گازسوز حاوی اجزا و فعالیت‌های نظیر تأمین گاز طبیعی، ایستگاه فشرده‌سازی و ذخیره، تأسیسات توزیع، اتوبوس گازسوز و تعامل اپراتور با تجهیزات و فعالیت‌های نگهداری است. برای ارزیابی ریسک کیفی مرگ و میر ناشی از آتش‌سوزی و انفجار در این سیستم مراحل زیر انجام می‌شود.

مرحله ۱ – مخاطرات: در این مثال، خطر، آتش‌سوزی گاز متان و انفجار منجر به مرگ و میر مسافران و غیرمسافران است.

مرحله ۲ – سدها: شامل مخزن ذخیره گاز طبیعی، سیستم کنترل فشار، اپراتورها، ابزارهای تشخیص نشت گاز و اخطار و فعالیت‌های نگهداری پیش‌گیرانه می‌باشد.

مرحله ۳ – عملکرد سدها: چندین خرابی برای سدها که منجر به آتش‌سوزی شود، محتمل است. عملکرد سدها در سناریوهای ریسک بحرانی به صورت زیر است:

۱. خرابی‌های داخلی فاجعه‌بار مخزن گاز یا سیستم کنترل، منجر به انتشار آنی گاز در حضور یک منبع اشتعال،
۲. خرابی‌های داخلی خفیف مخزن گاز یا سیستم کنترل، منجر به انتشار تدریجی گاز در حضور یک منبع اشتعال،
۳. ایجاد خطا در مخزن گاز یا سیستم کنترل یا خطای انسانی منجر به انتشار گاز و اشتعال در اثر جرقه‌های بار الکتریسیته ساکن،
۴. ضربهٔ تصادفی به مخزن گاز و سخت‌افزار دیگر با بدنهٔ خارجی (به عنوان مثال در اثر برخورد با وسیله‌های نقلیهٔ دیگر) در حضور یک منبع اشتعال،
۵. خطای اپراتور/راننده منجر به انتشار گاز طبیعی در حضور یک منبع اشتعال.

سناریوهای شامل خرابی سدهای بحرانی در جدول شماره ۲ لیست شده است.

جدول شماره ۲: خرابی سدها و اثرات آنها

دستهٔ خرابی سد	خرابی‌های داخلی سد	خرابی‌های خارجی سد
خرابی مکانیکی	خرابی فشارسنج به یک پرتابه	انفجار سوخت مخزن گاز طبیعی ناشی از خرابی بستن کمپرسور
	آتش‌سوزی ناشی از انتشار گاز از سیستم اطمینان فشار بارهای تناوبی فشار/دما	آسیب پرتابه‌ای از اشیای پرنده هنگام بازکردن مخزن گاز طبیعی
	مخاطرات سقوط مخزن گاز	اشیای پرنده با سرعت بالا در اثر خرابی شلنگ سوخت
	انفجار مخزن سوخت یا سایر آتش‌سوزی‌های ناشی از برخورد وسیلهٔ نقلیه در تصادفات	آتش‌سوزی ناشی از خرابی توزیع کنندهٔ گاز در اثر برخورد وسیلهٔ نقلیه
	آتش‌سوزی وسیلهٔ نقلیه ناشی از نشت سیستم سوخت در اثر طراحی ضعیف یا نصب نادرست	آتش‌سوزی ناشی از خرابی خطوط لولهٔ تغذیه سوخت
	آتش‌سوزی وسیلهٔ نقلیه در اثر نشت آشکارنشدهٔ سیستم سوخت از جزء خراب	آتش‌سوزی طی سوخت‌گیری
	انفجار وسیلهٔ نقلیه ناشی از نشت‌های سیستم سوخت	خرابی پرتابه‌ای از خرابی فاجعه‌بار کمپرسور منجر به خرابی و جراحت/مرگ
	آتش‌سوزی ساختمان از وسیلهٔ نقلیه، پمپ گاز یا نشت‌های مخزن ذخیره	
	انفجار ناشی از خرابی مکانیکی در سیلندر ذخیره گاز در وسیلهٔ نقلیه	

خرابی‌های شیمیایی	انفجار ناشی از خرابی فاجعه‌بار حاصل از خوردگی خارجی مخزن سوخت	آتش‌سوزی در اثر خوردگی خطوط تغذیه گاز منجر به نشت
	انفجار مخزن وسیلهٔ نقلیه در اثر خوردگی داخلی	آتش‌سوزی و انفجار در اثر خودرگی مخازن ذخیره
خرابی‌های الکتریکی	آتش‌سوزی وسیلهٔ نقلیه در اثر خرابی‌های الکتریکی غیرمرتبط به سیستم گاز طبیعی	شوک الکتریکی از منبع تغذیه به ایستگاه‌های کمپرسور سوخت طبیعی
		آتش‌سوزی از بار الکتریکی ساکن طی تخلیهٔ مخزن

جدول شماره ۳: ماتریس سناریوهای انتشار و پراکندگی گاز

مود انتشار گاز طبیعی	حالت احتراق	پیامد مورد انتظار
آنی	سریع	انفجار کروی[1]
	تأخیری	انفجار ابر بخار یا آتش با شعلهٔ ناگهانی
تدریجی	سریع	شعلهٔ جت
	تأخیری	انفجار ابر بخار یا آتش با شعلهٔ ناگهانی

جدول شماره ۴: دسته‌بندی وخامت انفجار آتش‌سوزی

دستهٔ وخامت	توضیح
فاجعه‌آمیز	انتشار گاز طبیعی فشرده شامل آتش‌سوزی یا انفجار فاجعه‌آمیز
بحرانی	انتشار محدود نشدهٔ گاز طبیعی با آتش‌سوزی بحرانی یا پتانسیل انفجار
مرزی	انتشار کم گاز طبیعی با پتانسیل اشتعال یا اثرات آتش‌سوزی مرزی
حداقلی	خرابی با پتانسیل حداقلی آتش‌سوزی و تنها از دست رفتن عملکرد سیستم

جدول شماره ۵: فرکانس مربوط به دسته‌های سناریوهای آتش‌سوزی

دستهٔ فرکانس	توضیح
مکرر	احتمال وقوع در یک سال یا کمتر از یک سال
محتمل	احتمال وقوع در ۱۰ سال یا کمتر
احتمال کم	احتمال وقوع در طول عمر ۲۰ ساله برای یک ایستگاه گاز یا اتوبوس
احتمال بسیار کم	ممکن اما غیرمحتمل طی عمر ۲۰ ساله

[1] - Fireball

مرحله ۴ – در معرض خطر قرارگرفتن

خرابی‌های توضیح داده شده در جدول شماره ۲، می‌تواند منجر به یکی از چهار حالت آتش‌سوزی در جدول شماره ۳ شود. برای هر چهار سناریوی آتش‌سوزی جدول شماره ۳، تخمین اندازه و دمای آتش منجر به ارزیابی نوع درمعرض قرارگیری و احتمال مرگ و میر در اثر آن می‌شود. وخامت هر نوع از درمعرض قرارگیری می‌تواند در یک دسته (جدول شماره ۴) خلاصه شود. بنابراین، هر خرابی جدول شماره ۲ می‌تواند منجر به یکی از حالت‌های لیست شده در جدول شماره ۴ شود.

مرحله ۵ – توصیف ریسک

با لحاظ سناریوهای حاوی خرابی سدهای مهم در جدول شماره ۲، دانستن فرکانس مربوط به وقوع هر سناریو مهم است. جدول شماره ۵ راهنمای به کار رفته برای ارزیابی فرکانس کیفی مربوط به هر سناریوی جدول شماره ۴ را نشان می‌دهد.

پس از تعیین وخامت و فرکانس هر سناریوی خرابی سد در جدول شماره ۲، یک ماتریس ریسک نشان داده شده در جدول شماره ۶ بدست می‌آید. در این ماتریس، هر المان تعداد سناریوهای دارای وخامت و فرکانس مشخص شده را نشان می‌دهد. روشن است که سناریوهایی که ربع بالا و سمت راست ماتریس قرار می‌گیرند، ریسک قابل توجهی دارند و به حفاظت و استراتژی‌های مدیریت ریسک نیاز دارند و سناریوهایی که در ربع پایین و سمت چپ قرار دارند ریسک مهمی ندارند. در مورد سایر سناریوها به ارزیابی‌های بیشتری برای تعیین نیاز یا عدم نیاز به استراتژی‌های مدیریت ریسک اضافی، نیاز است.

جدول شماره ۶: ماتریس ریسک حاوی تعداد سناریوهای دسته‌های مختلف ریسک

	فاجعه‌آمیز	بحرانی	مرزی	حداقلی
مکرر	۰	۰	۰	۴
محتمل	۱	۸	۶	۱۵
احتمال کم	۳	۷	۱۲	۱۹
احتمال بسیار کم	۴	۳	۲	۳

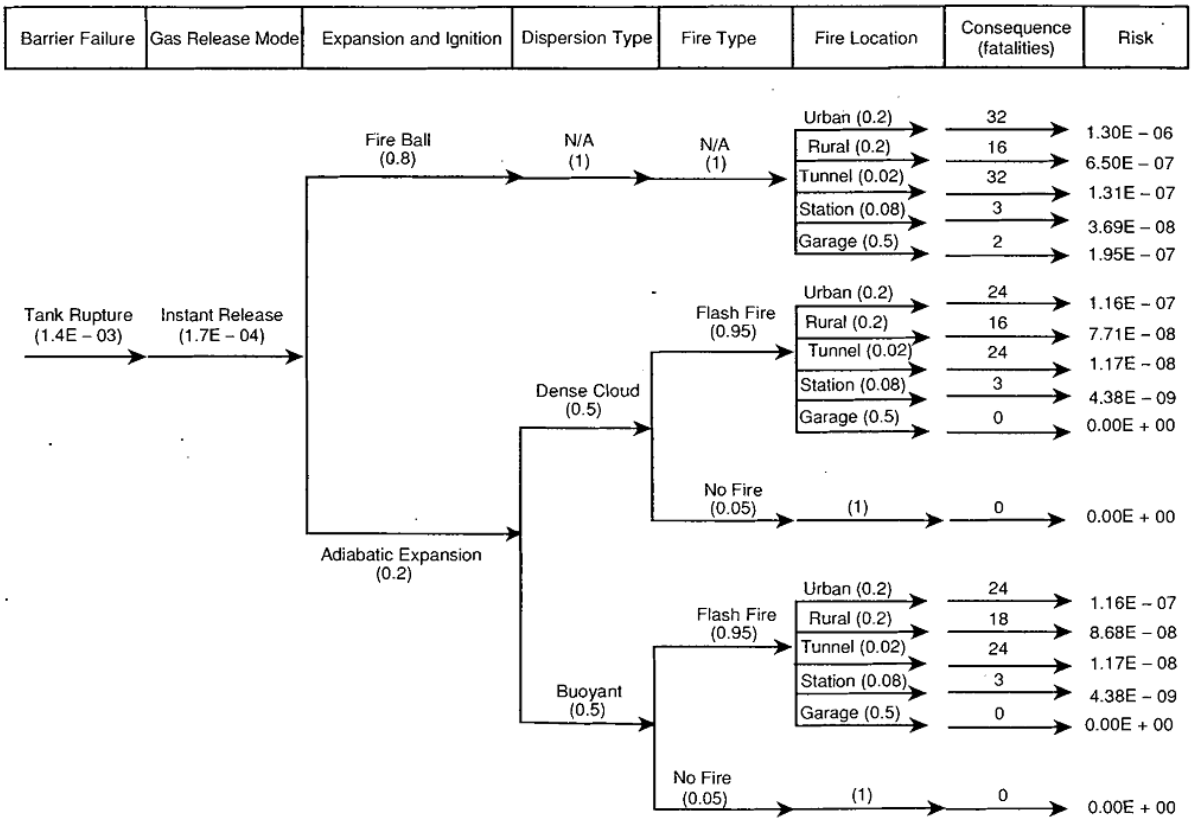
۲-۷-۷- ارزیابی ریسک کمّی

این روش همان مراحل ارزیابی ریسک کیفی را دنبال می‌کند، به جز اینکه در مراحل ۳ تا ۵، عملکرد سدها، مقدار درمعرض قرارگرفتن و پیامدهای آن باید کمّی‌سازی شوند. در این قسمت، ارزیابی ریسک کمّی تنها با یک مثال توضیح داده می‌شود. این مثال همان مثال ارزیابی ریسک کیفی است.

خرابی مخزن گاز طبیعی به عنوان علت اولیه ممکن یک آتش‌سوزی منجر به انتشار گاز و سناریوی آتش‌سوزی مورد نظر است. شکل ۷ سناریوها، فرکانس‌ها و پیامدها را نشان می‌دهد. همچنین سهم ریسک مرزی هر سناریو به همراه مؤلفه‌های ریسک در اثر همهٔ سناریوها محاسبه شده است. ریسک به صورت زیر محاسبه می‌شود:

ریسک = فرکانس یک خرابی سد حفاظتی × احتمال انتشار گاز در اثر خرابی سد حفاظتی × احتمال انبساط و اشتعال گاز منتشر شده × احتمال انتشار آتش در اثر اشتعال گاز × احتمال آتش‌سوزی در اثر انتشار × احتمال وقوع آتش در موقعیت خاص × پیامد

داده‌های جدول شماره ۷ از جمله منابع عمومی خرابی هستند. احتمال اینکه تجهیزات دیگر یا خطای اپراتور، یک سناریوی انتشار گاز را آغاز کند، باید لحاظ شود. زمانی که همهٔ سایر خطاهای ممکن لحاظ شوند، نتایج کلی به صورت جدول شماره ۷ خلاصه می‌شوند.



شکل ۷: سناریوهای شامل خرابی مخزن گاز طبیعی فشرده

جدول شماره ۷: ماتریس ریسک برای همهٔ سناریوهای خرابی اتوبوس‌های سوخت گاز طبیعی (با فرض پیمایش ۱۱۰۰۰ مایل توسط یک اتوبوس در سال)

سناریوهای آتش‌سوزی اتوبوس‌های با سوخت گاز طبیعی	فرکانس وقوع به ازای اتوبوس در سال	ریسک (مرگ و میر به ازای اتوبوس در سال)	ریسک (مرگ و میر به ازای پیمایش ۱۰۰ میلیون مایل)
سخت‌افزار اتوبوس (مانند مخزن گاز)	$۱/۴ \times ۱۰^{-۳}$	$۲/۷ \times ۱۰^{-۶}$	$۲/۸ \times ۱۰^{-۲}$
سخت‌افزار ایستگاه گاز	$۳/۷ \times ۱۰^{-۳}$	$۷/۵ \times ۱۰^{-۶}$	$۷/۸ \times ۱۰^{-۲}$
تخلیه الکترواستاتیکی گاز طبیعی فشرده	$۱/۴ \times ۱۰^{-۵}$	$۳/۷ \times ۱۰^{-۶}$	$۳/۹ \times ۱۰^{-۲}$
اثر خرابی‌های ناشی از برخورد	$۳/۶ \times ۱۰^{-۲}$	$۴/۶ \times ۱۰^{-۶}$	$۴/۸ \times ۱۰^{-۲}$
سخت‌افزار غیرمرتبط با گاز طبیعی فشرده	$۳/۶ \times ۱۰^{-۴}$	$۳/۱ \times ۱۰^{-۶}$	$۳/۲ \times ۱۰^{-۲}$
خطای اپراتور	۴×۱۰^{-۲}	$۳/۵ \times ۱۰^{-۷}$	$۳/۵ \times ۱۰^{-۳}$
ریسک مرگ و میر آتش‌سوزی کلی	–	$۲/۲ \times ۱۰^{-۵}$	$۲/۳ \times ۱۰^{-۱}$

۳- مهندسی قابلیت اطمینان و ایمنی

۳-۱- تاریخچه

مفهوم قابلیت اطمینان و ایمنی تقریباً پس از سایر شاخه‌های مرسوم مهندسی مطرح شد. در گذشته، قابلیت اطمینان و ایمنی با تمرکز بیشتر بر اجزای بحرانی به کار می‌رفته است و بیشتر از آنکه به عنوان یک تکنیک علمی باشد، یک امر تفنّنی بود. در دهۀ ۱۹۳۰ حوادث هواپیما با جمع‌آوری داده‌های خرابی اجزای هواپیماهای مختلف در قالب گزارش‌های آماری ثبت شد. طراحان و سازندگان از این بازخورد برای ارتقای طراحی‌های آینده استفاده کردند. اولین هدف ریسک برای ایمنی هواپیما توسط پوگسلی[۱] در سال ۱۹۳۹ تعریف شد که بر اساس آن، نرخ وقوع حادثه یک هواپیما باید کمتر از 10^{-5} بار در ساعت باشد.

در ابتدا، تکنیک‌های رسمی قابلیت اطمینان طی جنگ جهانی دوم توسعه یافت. اغلب تجهیزات دفاعی در زمان مورد نیاز خراب می‌شدند. دلیل خرابی، سیستم الکترونیکی و به خصوص به دلیل خرابی‌های لولۀ خلأ بود. در دهۀ ۱۹۴۰ تلاش‌های ارتقای قابلیت اطمینان در امریکا با توجه به دو مقیاس انجام شد. یکی افزایش عمر محصولات از طریق طراحی بهتر و دیگری افزایش قابلیت اطمینان از طریق افزایش کیفیت و کنترل کیفی بود.

اولین مدل‌های قابلیت اطمینانِ پیش‌بینانه در آلمان ظاهر شدند. راکت‌های جنگی، قابلیت اطمینان ضعیفی داشتند. این قاعده که استحکام یک زنجیر براساس استحکام ضعیف‌ترین حلقۀ آن تعیین می‌شود، مورد توجه تیم طراح راکت‌ها قرار گرفت، اما خرابی‌ها نه تنها در ضعیف‌ترین بخش‌ها مشاهده شد، بلکه در سایر اجزا نیز قابل رؤیت بود. در نهایت، با یک ریاضی‌دان به نام اریک پرنخا[۲] مشورت شد. او یک رابطه را پیشنهاد داد که بر اساس آن اگر احتمال نجات یک جزء $1/x$ است، احتمال نجات یک سیستم با n جزء از همان نوع $1/x^n$ خواهد بود. درواقع، فرمول مشهور لوسر[۳] برای قابلیت اطمینان سیستم‌های سری (قابلیت اطمینان سیستم سری محصول قابلیت اطمینان اجزای تشکیل‌دهنده است)، از پاسخ پرنخا مشتق شده است.

قابلیت اطمینان به عنوان یک شاخۀ مهندسی در دهه ۱۹۵۰ در امریکا بوجود آمد. قابلیت دسترسی تجهیزات نظامی پایین و هزینه‌ها در اثر نرخ‌های خرابی بالای سیستم‌های الکترونیکی به دلیل پیچیدگی آنها زیاد بود. در سال ۱۹۵۲، وزارت دفاع

[۱] - Pugsley
[۲] -Eric Pernchka
[۳] -Lusser’s formula

و کل صنعت الکترونیک، گروه مشورتی را در زمینه قابلیت اطمینانِ تجهیزات الکترونیکی تشکیل داد. گزارش این گروه تست‌های ارتقای قابلیت اطمینان و تست‌های تشخیصی را پیشنهاد و توصیه کرد که قابلیت اطمینان باید یک بخش یکپارچه از چرخهٔ توسعه باشد. توصیه‌های گروه مشورتی توسط ناسا و وزارت دفاع امریکا پذیرفته شد.

آزمایشگاه‌های واتسون و بِل مفهوم تحلیل درخت خطا را برای ارزیابی ایمنی سیستم‌های کنترل پیشران موشک قاره‌پیما در سال ۱۹۶۱ ارائه کردند. این مفهوم، به صورت وسیعی در همهٔ زمینه‌های مهندسی برای تحلیل ایمنی به کار رفت. روش مود خرابی و تحلیل اثرات (FMEA) نیز در دهه ۱۹۶۰ در زمینهٔ هوانوردی مطرح شد. طی این دهه، رویکردهای احتمالاتی به صورت فزاینده‌ای با طراحی آمیخته شد. در ابتدا، ذات مقررات مرتبط با ایمنی هوانوردی طبیعت یقینی داشتند، ولی به آرامی معیارهای احتمالاتی در طراحی هواپیما وارد شدند. این دوره همچنین شاهد تولّد فعالیت‌های بنیاد مهندسان الکتریکی و الکترونیک (IEEE) در زمینهٔ قابلیت اطمینان بود. ریاضی‌دان‌های برجسته مانند بیرنبام، بروسچن، اساری و ویبال برای توسعهٔ ریاضیات قابلیت اطمینان مشارکت کردند.

در سال ۱۹۷۵ راموسین با یک تیم ۵۰ نفره از مهندسین، مطالعات ارزیابی ریسک نیروگاه‌های هسته‌ای را انجام و گزارش WASH-1400 را منتشر کرد. در بخشی از این مطالعه، روش‌های جدید بسیاری شامل روش‌های درخت رویداد برای ارزیابی سناریوهای حوادث توسعه یافتند. در این مطالعات، شمار زیادی سناریوی حوادث و ریسک کمّی‌شده به صورت احتمال سالیانهٔ ضرر به جامعهٔ مجاور نیروگاه هسته‌ای لحاظ شده است. ریسک محاسبه‌شده در این زمینه، از اثرات شهاب‌سنگ آسمانی کمتر بود. اما گزارش راموسین در ارزیابی انجام شده، در گزارش لوئیس در سال ۱۹۷۷ در زمینهٔ درک عدم قطعیت در داده‌ها، رفتار انسانی، خرابی‌های با عامل مشترک و پیامدها به شدت مورد نقد قرار گرفت.

حادثهٔ تری مایل آیلند در سال ۱۹۷۹ در امریکا به وقوع پیوست و به عنوان اولین حادثهٔ بزرگ هسته‌ای لحاظ شد. متولّیان ایمنی دریافتند که گزارش راموسین، حادثه‌ای با یک سناریوی مشابه با این حادثه شناسایی کرده بود. پس از این حادثه کمیتهٔ ایمنی پیشنهاد کرد که روش‌های تحلیل ریسک احتمالاتی به صورت فزاینده‌ای مورد استفاده قرار گیرد. رویکردها نسبت به روش‌های احتمالاتی تغییر کرد و شمار مطالعات ارزیابی ریسک نیروگاه‌های هسته‌ای در سراسر جهان افزایش یافت.

ارزیابی ریسک در بخش‌های صنعتی دیگر، از جمله تحلیل ریسک در تأسیسات پتروشیمی، نیز انجام می‌گرفت. این تکنیک‌ها به طور وسیعی در میدان‌های مختلفی مانند هوانوردی، شیمی، توان و خطوط ریلی برای تطابق با مقررات و نیز ارتقای طراحی تعمیم یافتند.

در ادامه، در ۲۰ تا ۲۵ سال گذشته، انجمن علمی و فعّال در این زمینه، شاهد افزایش چشم‌گیر توسعه و کاربرد مهندسی قابلیت اطمینان و ایمنی شد به نحوی که بر چالش‌های ایجاد شده از رشد پیچیدگی سیستم‌ها غالب شده و عملاً از مزایای توان محاسباتیِ در دسترس با هزینه معقول بهره‌مند شده است.

بنیاد مهندسان الکتریکی و الکترونیک (IEEE) قابلیت اطمینان را به صورت قابلیت یک سیستم و یا جزء برای انجام اقدامات مورد نیاز تحت شرایط تعیین شده برای یک دورهٔ مشخص زمانی، تعریف کرده است. این تعریف چهار مؤلفه دارد: قابلیت، اقدامات مورد نیاز، دورهٔ زمانی مشخص‌شده و شرایط تعیین‌شده.

۳-۲- نیاز به مهندسی قابلیت اطمینان و ایمنی

خرابی برای هر چیزی در جهانِ واقعی اجتناب‌ناپذیر است و سیستم‌های مهندسی از این امر مستثنی نیستند. اثر خرابی‌ها، از آسیب‌ها و هزینه‌های کم گرفته تا صدمه به فرد، زیان‌های اقتصادی کلان و سلامت متفاوت است. مثال‌های حوادث بزرگ شامل حوادث در نیروگاه‌های هسته‌ای تری مایل آیلند و چرنوبیل، نشت گاز در تأسیسات بهوپال هند و انفجار شاتل فضایی چلنجر است. علل خرابی شامل طراحی نامناسب مهندسی، اشتباهات ساخت، تست‌های غیرکافی، خطاهای انسانی، نگهداری ضعیف، استفاده غیرصحیح و فقدان محافظت در برابر تنش‌های فزاینده است. طراحان، سازندگان و کاربران تلاش می‌کنند تا وقوع خرابی را کمینه سازند. به منظور کمینه‌سازی خرابی‌ها در سیستم‌های مهندسی، فهم دلیل و نحوهٔ وقوع خرابی‌ها ضروری است. همچنین دانستن اینکه هر چند وقت یکبار این خرابی ممکن است رخ دهد نیز ضروری است. قابلیت اطمینان با مفهوم خرابی مرتبط است، درحالی‌که ایمنی با پیامدهای بعد از خرابی مرتبط است. سیستم‌های ایمنی ذاتی کمینه‌بودن پیامدهای خرابی را تضمین می‌کنند. مهندسی ایمنی و قابلیت اطمینان تلاش می‌کند تا خرابی، تعمیر و پیامدهای خرابی سیستم‌ها را به منظور ارتقای عملکرد آنها مطالعه، توصیف، اندازه‌گیری و تحلیل نماید. این کار با افزایش عمر طراحی، حذف یا کاهش احتمال خرابی‌ها و پیامدهای آنها و کاهش زمانِ غیرفعال بودن یک تأسیسات و درنتیجه افزایش زمان عملکرد در دسترس با کمترین هزینه‌های ممکن در طول عمر انجام می‌شود.

نیاز به قابلیت اطمینان و ایمنی بالاتر با عوامل زیر بیشتر درک می‌شود:

- پیچیدگی فزایندهٔ سیستم‌ها،
- رشد شتابان تکنولوژی،
- آگاهی عمومی یا نیازمندی مشتری،

- ایمنی مدرن و قوانین مسئولیت،
- رقابت در بازار،
- خرابی‌های سیستم‌ها در گذشته،
- هزینهٔ خرابی، ویرانی و ضمانت،
- ملاحظات ایمنی با پیامدهای نامطلوب.

قابلیت اطمینان و مهندسی ایمنی، کاربردهای وسیعی در همهٔ زمینه‌های مهندسیِ متداول دارد که مهمترین اجزای آن عبارتند از:

- بررسی طراحی،
- شناسایی اجزای بحرانی،
- مقایسه‌های محیطی،
- نیازمندی‌های افزونگی،
- الزامات مقررات،
- تهیهٔ برنامه‌های نگهداری پیش‌گیرانه،
- مدیریت تعمیر و اجزای یدکی،
- تخمین‌های ماندهٔ عمر و جایگزینی،
- مدیریت ایمنی،
- تحلیل هزینهٔ دورهٔ عمر.

به طور کلی، هدف اصلی مهندسی قابلیت اطمینان، حصول اطمینان از عملکرد موفق سیستم است. اهداف و کاربردهای تفصیلی مهندسی قابلیت اطمینان عبارتند از:

۱- بهبود کیفیت طراحی،
۲- ارتقای کارآیی (قابلیت اعتماد و ایمنی) سیستم موجود (بیشترین کاربرد مهندسی قابلیت اطمینان در این مورد است)،
۳- کاهش هزینه‌های مستقیم و غیرمستقیم (هزینه مستقیم مانند استهلاک سیستم و هزینه غیرمستقیم هزینه‌هایی هستند که به مصرف‌کننده تحمیل می‌شود مانند خسارت‌های وارده به مصرف‌کننده ناشی از قطع برق)،

۴- کاهش مخاطرات،

۵- ارزیابی ایمنی و مخاطرات و مقایسهٔ ریسک ناشی از سیستم‌ها از جمله مقایسهٔ ریسک نیروگاه‌های اتمی با ریسک سایر سیستم‌ها،

۶- ایجاد تغییرات فنی در طرح و بررسی اثر آنها،

۷- افزایش طول عمر سیستم‌ها،

۸- تعمیرات و نگهداری پیش‌گیرانه.

۳-۳- خرابی‌های اجتناب‌ناپذیر

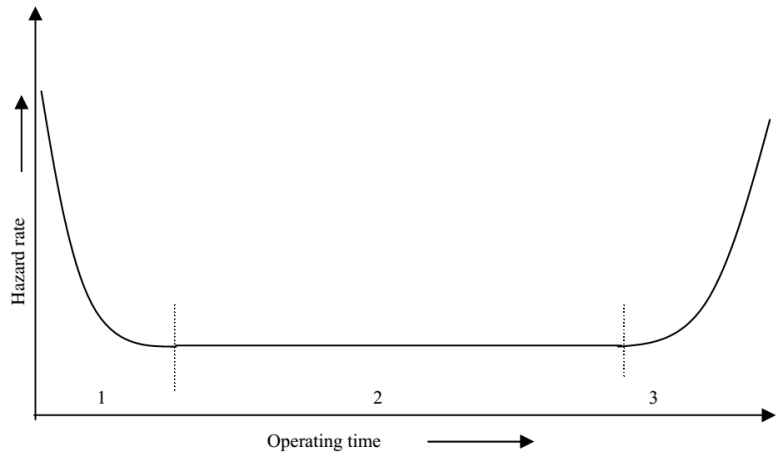
هیچ چیز برای همیشه باقی نخواهد ماند، بنابراین در زمان طولانی عملکرد سیستم، تعمیر و جایگزینی اجزای خراب شده اهمیت فراوانی دارد. علل مختلفی برای خرابی سیستم‌های مهندسی وجود دارد. برخی از آنها عبارتند از:

- خطاهای طراحی،
- ضعف تکنیک‌های ساخت و نقص کنترل کیفی،
- اجزای غیراستاندارد،
- فقدان حفاظت در برابر تنش‌های بیش از حد،
- نگهداری ضعیف،
- پیری و فرسودگی،
- خطاهای انسانی.

سه مرحلهٔ خرابی در طول عمر یک محصول وجود دارد: مرحله زودهنگام، مرحلهٔ بهره‌برداری و مرحلهٔ فرسودگی که در شکل ۸ نشان داده شده است و به نام منحنی عمر و یا منحنی وان حمام (بدلیل شکل آن) شناخته می‌شود.

هنگامی که تجهیز برای اولین‌بار استفاده می‌شود هر جزء ضعیف به زودی خراب می‌شود. بنابراین، نرخ خطر بسیار بالا است. ولی هنگامی که اجزای ضعیف تعویض می‌شوند، نرخ خطر کاهش یافته و ثابت خواهد بود و درنهایت نرخ خطر دوباره با فرسایش اجزا افزایش می‌یابد.

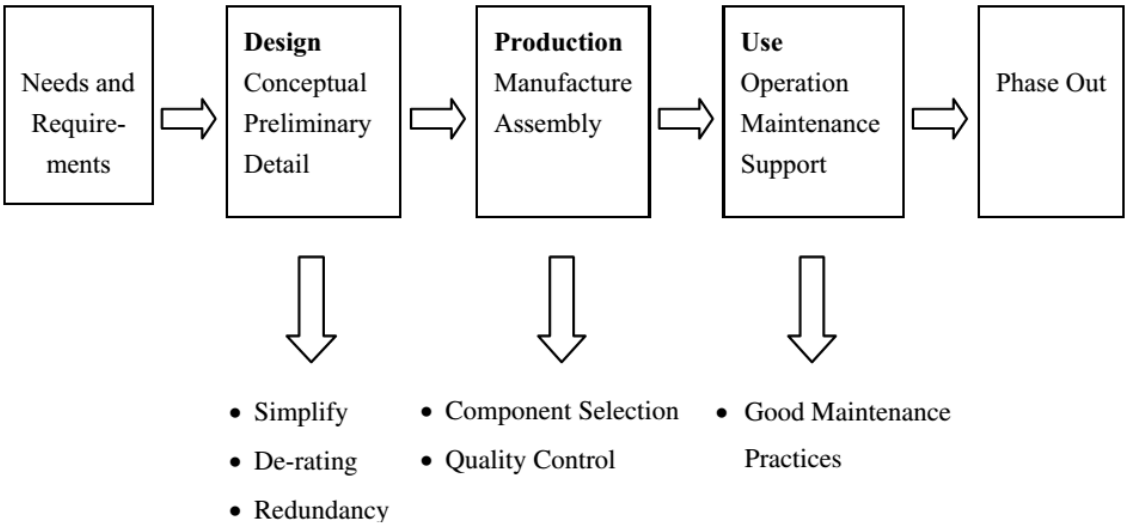
ناحیه ۱ نشان می‌دهد که جزئی استفاده نمی‌شود، مگر اینکه از این دوره جان سالم به در برد. برخی سازندگان مشهور تنها محصولاتی را می‌فروشند که از این دوره جان سالم به در برده‌اند. ناحیه ۲ بازهٔ عمر مفید است که نرخ خطر با خرابی احتمالی معین می‌شود و ثابت است. ناحیه ۳ نشان می‌دهد که جزء باید جایگزین و یا دور انداخته شود.



شکل ۸: منحنی وان حمام

۳-۴- ارتقای قابلیت اطمینان و ایمنی

قابلیت اطمینان یک موضوع مهم است که هر مرحله از طول عمر یک محصول و یا یک سیستم را تحت تأثیر قرار می‌دهد. مراحل مختلف طول عمر یک سیستم در شکل ۹ نشان داده شده است.



شکل ۹: مراحل مختلف در طول عمر یک سیستم

مرحلهٔ اول در ارتقای قابلیت اطمینان، اندازه‌گیری و ارزیابی سطح قابلیت اطمینان کنونی است. شناسایی مؤلفه‌ها و دلایل مهم برای ارتقای قابلیت اطمینان با منابع موجود باید انجام شود. همچنین ارتقای قابلیت اطمینان وابسته به موقعیت زمانی سیستم در طول عمر آن است. به عنوان مثال، اگر سیستم در مرحلهٔ طراحی باشد، تنها با ساده‌سازی طراحی با استفاده از کاهش نرخ و افزونگی، می‌توان قابلیت اطمینان را افزایش داد. با استفاده از اجزای با کیفیت خوب و کنترل کیفی، قابلیت اطمینان می‌تواند در مرحلهٔ تولید ارتقا یابد. داشتن یک برنامهٔ نگهداری خوب، تنها اقدام در مرحلهٔ بهره‌برداری سیستم است.

ایمنی، ترکیبی از قابلیت اطمینان و پیامدها است. جدای از افزایش سطح قابلیت اطمینان برای ارتقای ایمنی، پیامدها باید کاهش یابد. این کار با تدارک سیستم‌های ایمنی و حفاظتی که خرابی‌ها را پیش‌بینی کرده و قرار گرفتن پیامدها در یک سطح قابل قبول را تضمین می‌کنند، حاصل می‌شود.

۳-۵- چالش‌های حاضر و نیازهای خرابی به تمرین مهندسی قابلیت اطمینان و ایمنی

ارزیابی ایمنی و قابلیت اطمینان یک ابزار کارامد برای مدیریت ریسک و تصمیم‌گیری برای طراحی ایمن، اقتصادی و کارامد و عملکرد سیستم‌های مهندسی پیچیده مانند نیروگاه‌های هسته‌ای، تأسیسات شیمی و فرایند، سیستم‌های هوانوردی و تجهیزات دفاعی است. کاربردهای خاص ارزیابی ایمنی و قابلیت اطمینان شامل ارزیابی طراحی برای مقایسه با استانداردها، شناسایی اجزای بحرانی برای قابلیت اطمینان و مدیریت ایمنی، ارزیابی عیب‌یابی و بازه‌های زمانی نگهداری و تخمین عمر باقی‌مانده است. همچنین این ارزیابی به عنوان یک الزام قانونی به کار می‌رود.

درکنار کاربردهای متعدد بالقوّه مطالعات قابلیت اطمینان، محدودیت‌هایی مختص این مقوله نیز وجود دارد. صحت ارزیابی ایمنی و قابلیت اطمینان به شدت از روش به کار رفته، وجود عدم قطعیت‌ها در داده‌ها و مدل‌ها، فرضیات بی‌جهت و وجود نقص در تحلیل، تأثیرپذیر است. از آنجا که در مدل ارزیابی ایمنی تلاش می‌شود واقعیت شبیه‌سازی شود، به کارگیری فرضیات ساده‌کننده و ایده‌آل‌سازی فرایندها و پدیده‌های پیچیده اجتناب‌ناپذیر است. این ساده‌سازی و ایده‌آل‌سازی‌ها، عدم قطعیت تولید خواهد کرد. اگر ارزیابی ایمنی و قابلیت اطمینان به عنوان ابزاری برای فرایند تصمیم‌گیری است، باید اثر این عدم قطعیت‌ها به درستی تعیین شود.

کاربرد نهایی هر مطالعهٔ قابلیت اطمینان کمک به تصمیم‌گیری، ارزیابی طراحی، شناسایی اجزای بحرانی و فعالیت‌های بهره‌برداری و نگهداری است. هنگامی که ارزیابی قابلیت اطمینان طراحی برای مقایسه با استانداردها و اهداف مورد نیاز تعیین شده انجام می‌شود، ابهام تصمیم‌گیرنده این است که آیا مقایسهٔ استاندارد باید با مقدار متوسط و یا با بازه‌های مقداری

انجام شود؟ این مسأله، زمانی مهم می‌شود که بازه‌های مقداری در یک تراز و یا تراز پایین‌تر است. مقدار استاندارد (احتمال خرابی) باید بیشتر از حد بالای تعیین شده در بازه‌های عدم قطعیت طراحی باشد. به طور مشابه، در ارزیابی بازه‌های زمانی بهره‌برداری و نگهداری، عدم قطعیت در داده‌ها و مدل‌ها می‌تواند تصمیم نهایی را تغییر دهد. برخورد صحیح با عدم قطعیت برای کاربردهای عملی نتایج تحلیل قابلیت اطمینان، بسیار ضروری است. صرف نظرکردن از عدم قطعیت‌ها در تحلیل قابلیت اطمینان، ممکن است منجر به تصمیم‌گیری اشتباه شود. لحاظ عدم قطعیت در تحلیل، باعث ارائهٔ راه حل‌های خوش‌بینانه و بدبینانه شده که بینش‌هایی در زمینهٔ تصمیم‌گیری ایجاد می‌کند. حصول اطمینانِ خاطر با سطح قابل قبول در نتایج، تنها از مدیریت صحیح عدم قطعیت بوجود می‌آید.

محققان، دانشگاهیان و مهندسان بسیاری در رشته‌های مختلف در توسعهٔ روش‌های انجام تحلیل عدم قطعیت و به‌کارگیری آنها در رشته‌های خود، تلاش‌های فراوانی انجام داده‌اند. درواقع، تشخیص انواع مختلف عدم قطعیتِ پارامتری، تعیین عدم قطعیتِ اولیه، نحوهٔ عمل عدم قطعیتِ مدل، عدم قطعیت در مدل‌سازیِ وابستگی و لحاظ عدم قطعیت در تصمیم‌گیری هنوز در حال تحقیق و توسعه هستند.

وجود قالب‌های مقرراتی می‌تواند اثر معینی بر به‌کارگیری روش‌های ریسک و قابلیت اطمینان در عمل داشته باشد. این امر در صنایعی نظیر صنعت هوانوردی و هسته‌ای به وضوح مشهود است؛ صنایعی که مطالعات ایمنی و قابلیت اطمینان در آنها مقرراتی اجباری دارد. در این صنایع که الزامات ایمنی یک حالت پیشنهادی (به عنوان مثال، صنایع اتوموبیل، خطوط ریلی، شبکه‌های ارتباطات و بخش ساختمان) دارد، انگیزهٔ کمی برای سرمایه‌گذاری در مطالعات پرهزینهٔ ریسک/ قابلیت اطیمنان وجود دارد. پذیرش مزایای حاصل از هزینه‌های تحمیل شده و زمان مصرف‌شده در تحلیل‌های ریسک/ قابلیت اطمینان مستلزم اقناع مالکان تأسیسات و مدیران سیستم از لحاظ فرهنگ ایمنی است.

برای رسیدن به هدف، دسترسی به کدها، استانداردها و مستندات، داشتن راهنمای خوب برای کاربردهای وسیع‌تر روش‌های قابلیت اطمینان و ریسک و مهندسان ماهر، ضروری است. به عنوان مثال، در حال حاضر هنوز شمار معدودی استاندارد در زمنیهٔ قابلیت اطمینان سازه و تحلیل و تکنیک‌های قابلیت اطمینان سیستمِ توان وجود دارد. علاوه براین، اجرای عملی روش‌های قابلیت اطمینان باید با نرم‌افزاری که به‌صورت معقولی کار با آن آسان است، پشتیبانی شود. چندین ابزار برای کاربردهای استاندارد در دسترس است، درحالی‌که موارد پیچیده از جمله رفتار انسانی، نرم‌افزار و درخت‌های رویداد و خطای دینامیکی نیازمند توسعهٔ بیشتر نرم‌افزارهای شبیه‌سازی یکپارچه هستند.

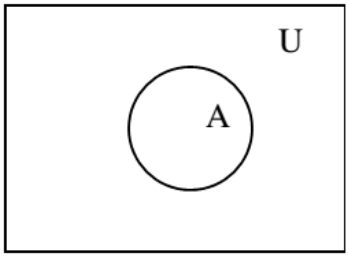
اغلب مطالعات قابلیت اطمینان و ریسک موجود، بر ارزیابی سطح ایمنی و مقایسه آن با استانداردهای صریح یا ضمنی تمرکز دارند. علاوه براین، مطالعات قابلیت اطمینان و ریسک باید به صورت فزاینده در فعالیت‌های بهره‌برداری و نگهداری سیستم‌های مهندسی به کار روند. به عنوان مثال، در نیروگاه هسته‌ای، تعیین بازه‌های زمانی تست نظارتی طی بهره‌برداری و تعیین بازه‌های زمانی بازدید حین بهره‌برداری برای نگهداری، برخی از کاربردهای عملی قابلیت اطمینان و مطالعات ریسک طی فازهای مختلف عملکردی است. در نهایت، فاصلهٔ بین تئوری و عمل با توسعه و به‌کارگیری راه‌حل‌های ممکنِ عملی برای مسائل صنعتی کاهش خواهد یافت.

۳-۶- ریاضیات پایه برای قابلیت اطمینان

به‌منظور جامع بودن گزارش و پرداختن به نیازمندی‌ها و پیش‌نیازهای مطالعات ایمنی احتمالاتی، در این بخش ریاضیات پایهٔ مرتبط با مطالعات مهندسی قابلیت اطمینان و ایمنی ارائه می‌شود. در این بخش، ابتدا مفاهیم پایهٔ تئوری مجموعه‌ها و تئوری احتمالات شرح داده شده، سپس توابع قابلیت اطمینان سیستم‌ها ارائه می‌شود. همچنین توزیع‌های مختلف به کار رفته در مطالعات مهندسی قابلیت اطمینان و ایمنی نیز در این بخش گنجانده شده است.

۳-۶-۱- تئوری مجموعه‌ها

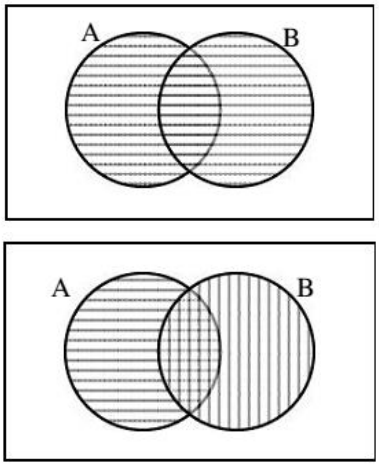
مجموعهٔ کل، حاوی همهٔ اجزای یک محیط است که با U شناخته می‌شود و زیرمجموعه‌ای که در مجموعهٔ کل واقع است به عنوان مجموعه‌ای از برخی اجزای همان محیط می‌باشد. در شکل ۱۰ نمایی از این بیان ارائه شده است که به آن دیاگرام پرکاربرد وِن گفته می‌شود.



شکل ۱۰: دیاگرام وِن برای زیر مجموعهٔ A

اجتماع دو مجموعه A و B از مجموعه کل U، مجموعه‌ای است که حاوی همهٔ اجزای دو مجموعه است به‌گونه‌ای که هر جزء یا در مجموعهٔ A یا در مجموعهٔ B قرار دارد. با این بیان، مشخص است که جزئی که در هر دو مجموعه قرار دارد نیز

عضوی از اجتماع دو مجموعه است. اشتراک دو مجموعه A و B مجموعه‌ای از اجزایی است که هم در A و هم در B قرار دارند. (شکل ۱۱)



شکل ۱۱: دیاگرام وِن برای اجتماع و اشتراک دو مجموعهٔ A و B

برخی قوانین مهم تئوری مجموعه‌ها در جدول شماره ۸ ارائه شده است.

جدول شماره ۸: قوانین تئوری مجموعه‌ها

نام	شرح
قانون اتحاد	$A\cup\varnothing=A;A\cup U=U$ $A\cap\varnothing=\varnothing;A\cap U=A$
قانون عدم تغییر	$A\cup A=A$ $A\cap A=A$
قانون جابجایی	$A\cup B=B\cup A$ $A\cap B=B\cap A$
قانون شرکت‌پذیری	$A\cup(B\cup C)=(A\cup B)\cup C$ $A\cap(B\cap C)=(A\cap B)\cap C$
قانون توزیع‌پذیری	$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$ $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$
قانون متمم‌گیری	$A\cup\overline{A}=U$ $A\cap\overline{A}=\varnothing$ $\overline{\overline{A}}=A$
قانون دمورگان	$\overline{(A\cup B)}=\overline{A}\cap\overline{B}$ $\overline{(A\cap B)}=\overline{A}\cup\overline{B}$

۳-۶-۲- جبر بولی

اجزا و سیستم‌ها می‌توانند دو حالت عملکردی موفق یا ناموفق داشته باشند. این مشخصه باعث شده است که مطالعات مهندسی قابلیت اطمینان و ایمنی با جبر بولی گره خورده و کاربرد وسیعی برای جبر بولی ایجاد شود. با فرض اینکه کمیت X نشان دهندهٔ حالت یک جزء یا سیستم باشد و مقدار ۱ نشان دهندهٔ حالت موفقیت و مقدار صفر نشان دهندهٔ حالت خرابی آن جزء یا سیستم است، احتمال اینکه مقدار X برابر یک باشد P(X=1)، قابلیت اطمینان آن جزء یا سیستم نامیده می‌شود. بر اساس این فرض، حالت دودویی جبر بولی به راحتی قابل استفاده است. در جبر بولی همهٔ متغیرها باید تنها دارای یکی از دو مقدار باشند: یا صفر یا یک. سه عملگر بولی وجود دارد که نام‌های آنها OR، AND و NOT می‌باشد. این عملگرها به ترتیب با علامت‌های « + »، « . » و « ¯ » شناخته می‌شوند. شماری از قوانین کاربردی و مفید جبر بولی در جدول شماره ۹ لیست شده‌اند. در این جدول، x_1، x_2 و x_3 متغیرهای مجموعهٔ X هستند.

جدول شماره ۹: قوانین جبر بولی

نام قانون	رابطه
اتحاد	$x+0=x$ $x.1=x$
عدم تغییر	$x+x=x$ $x.x=x$
متمم	$\overline{0}=1$ $\overline{1}=0$ $\overline{\overline{x}}=x$
جذب	$x_1+x_1.x_2=x_1$ $x_1.(x_1+x_2)=x_1$
شرکت‌پذیری	$x_1+(x_2+x_3)=(x_1+x_2)+x_3$ $x_1.(x_2.x_3)=(x_1.x_2).x_3$
دمورگان	$\overline{(x_1+x_2)}=\overline{x}_1.\overline{x}_2$ $\overline{(x_1.x_2)}=\overline{x}_1+\overline{x}_2$

یک تابع $f(x_1,x_2,x_3,...,x_n)$ با n متغیر را در نظر بگیرید که با عملگرهای بولی ترکیب شده‌اند. تابع f با توجه به مقادیر متغیرهای پایهٔ $x_1,x_2,x_3,...,x_n$، برابر یک یا صفر خواهد بود. از آنجا که n متغیر وجود دارد و هریک می‌تواند مقدار صفر یا یک داشته باشد، تعداد 2^n ترکیب از متغیرها باید لحاظ شود تا مقدار تابع تعیین شود. جدول‌های بررسی مقدار تابع برای همهٔ این ترکیب‌ها استفاده می‌شوند. بررسی عبارت بولی زیر در جدول شماره ۱۰ ارائه شده است.

$$f(x_1, x_2, x_3) = x_1.x_2 + x_2.x_3 + x_1.x_3 \quad (۱-۳)$$

جدول شماره ۱۰: جدول بررسی عبارت بولی

x_1	x_2	x_3	f
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

در محاسبات قابلیت اطمینان، ضروری است که به منظور حذف تکرار المان‌های یکسان، عبارت بولی کمینه شود. فرض منطقی همهٔ روش‌های کمینه‌سازی در مجموعه‌های قوانین جبر بولی در جدول شماره ۹ ارائه شده است. حجم کار درگیر در کمینه‌سازی با افزایش تعداد متغیرها، افزایش می‌یابد. روش‌های هندسی و نقشهٔ مشهور کارنوف[۱] تنها برای شش متغیر کاربردی هستند. امروزه الگوریتم‌های رایانه‌ای پیچیده برای محاسبات شمار زیادی از متغیرها در دسترس است.

۳-۶-۳- مفاهیم تئوری احتمالات

عبارت «آزمایش» در احتمالات و آمار برای شرح هر فرایندِ مشاهده‌ای که دادهٔ خام ایجاد می‌کند، به کار می‌رود. یک آزمایش درصورتی‌که تکرارپذیر بوده و در اثر تکرار بسیار زیاد حالت‌های وقوعِ معین داشته باشد، از نوع «آزمایش تصادفی» خواهد بود. برخی از مثال‌های آزمایش تصادفی شامل پرتاب یک سکه، یک تاس و زمان‌های خرابی تجهیزات مهندسی است. مجموعهٔ همهٔ خروجی‌های ممکنِ یک آزمایش تصادفی با عنوان «فضای نمونه‌گیری» و با عبارت S شناخته می‌شود. فضای نمونه‌گیری آزمایش تصادفی پرتاب یک تاس عبارت است از: {۱، ۲، ۳، ۴، ۵ و ۶}. درحالت تست عمرِ تجهیزات مهندسی، فضای نمونه‌گیری از صفر تا بی‌نهایت خواهد بود. هر زیرمجموعه‌ای از فضای نمونه‌گیری با عنوان یک رویداد E است. اگر خروجی آزمایش تصادفی در رویداد E قرار داشته باشد، آنگاه می‌توان گفت رویداد E واقع شده است. در اینجا احتمالات به منظور کمّی‌سازی احتمال یا شانس اینکه یک خروجی مشخص از آزمایش تصادفی رخ خواهد داد، به‌کار می‌رود. احتمالات با هر رویداد E از فضای نمونه‌گیری S وابسته به شانس وقوع است که از اطلاعات یا داده‌های دردسترس حاصل می‌شود.

[۱] -Karnaugh's map

مفهوم احتمال یک رویداد مشخص، معانی و تفاسیر مختلفی دارد. همان‌طور که پیش‌تر اشاره شد، اساساً سه تفسیر از احتمال وجود دارد: تفسیر کلاسیک، تفسیر فرکانسِ نسبی و تفسیر ذهنی.

تفسیر کلاسیک از احتمال مبتنی بر مفهوم خروجی‌های محتمل برابر است و اساساً در حیطهٔ بازی‌های شانس از دیرباز در تئوری احتمال توسعه یافته است. در اینجا احتمال یک رویداد E برابر تعداد خروجی‌های شامل وقوع آن رویداد (n) تقسیم بر کل تعداد خروجی‌های ممکن (N) است. این تفسیر، ساده و از لحاظ شهودی جذاب است و به کارگیری آن آسان است، ولی کاربرد آن محدود به قید خروجی‌های محتملِ برابر است؛ یعنی تنها مواردی که احتمال خروجی‌های آن یکسان و برابر است، مشمول این تفسیر می‌شوند.

$$P(E) = \frac{n}{N} \qquad (۲-۳)$$

در تفسیر فرکانسِ نسبی، احتمال یک رویداد به صورت نسبت دفعات وقوع رویداد در آزمایش‌های بلندمدتِ یکسان تعریف می‌شود. اصولاً به نظر می‌رسد این تفسیر کاملاً معقول است. در عمل، این تفسیر نیازمند داده‌های وسیعی است، که در بسیاری از حالت‌ها به سادگی قابل دسترسی نیستند و در حالت‌های دیگر ممکن است این پرسش ایجاد شود که چه آزمایشی‌هایی می‌توانند یکسان باشند؟ از لحاظ ریاضی تفسیر فرکانس از احتمال به صورت زیر است:

$$P(E) = \lim_{N\to\infty} \frac{n}{N} \qquad (۳-۳)$$

در تفسیر ذهنی، احتمال جنبهٔ اعتقادی پیدا می‌کند و شامل مقایسه‌های خاص در زمرهٔ بخت‌آزمایی است. یک احتمال ذهنی، احتمال وابسته به یک شخص خاص است. افراد متفاوت می‌توانند احتمالات متفاوتی برای یک رویداد مشابه داشته باشند. این واقعیت که تفسیر احتمال ذهنی می‌تواند بر اساس قوانین معمول ریاضیات احتمالات تدوین شود، شفاف نیست، ولی می‌توان نشان داد که از قوانین بدیهی تبعیت می‌کنند. علی‌رغم چنین تفسیری، یک اجماع عمومی وجود دارد مبنی بر اینکه ریاضیات احتمالاتی در همهٔ حالت‌ها یکسان است.

۳-۶-۳-۱- ویژگی‌های احتمال

احتمال عددی است که به هر تعداد از یک مجموعه از رویدادها از یک آزمایش تصادفی که شرایط زیر را داشته باشند، تخصیص داده می‌شود. اگر S فضای نمونه‌گیری و E هر رویداد در آزمایش تصادفی باشد:

جدول شماره ۱۱: ویژگی‌های احتمال

ویژگی اول	$P(S)=1$
ویژگی دوم	$0 \le P(E) \le 1$
ویژگی سوم - برای دو رویداد که اشتراکشان تهی است، خواهیم داشت:	$P(E_1 \cup E_2) = P(E_1) + P(E_2)$

ویژگی اول پیامدی از این حقیقت است که در هر بار انجام آزمایش، از فضای نمونه‌گیری بالاخره یک خروجی به دست خواهد آمد. ویژگی دوم معادل الزام تفسیر فرکانس نسبی از احتمال است که بر اساس آن، مقدار احتمال باید بین صفر باشد. ویژگی سوم، بیان می‌کند که اگر دو رویداد خروجی مشترکی نداشته باشند، فرکانس نسبی آنها جمع فرکانس نسبی هر یک از دو رویداد است.

۳-۶-۳-۲- جبر تئوری احتمال

۳-۶-۳-۲-۱- رویدادهای مستقل و غیرقابل جمع

دو رویداد مستقل هستند اگر وقوع یکی، احتمال وقوع دیگری را متأثر نسازد. اگر وقوع یک رویداد هیچ‌گونه اطلاعاتی در مورد وقوع رویداد دیگر تولید نکند، آنگاه می‌توان گفت این دو رویداد از لحاظ آماری مستقل هستند. به عنوان مثال، در یک تأسیسات فرایندی، خرابی یک پمپ، یک شیر را تحت تأثیر قرار نمی‌دهد و باعث خرابی آن نمی‌شود.

اگر وقوع یک رویداد مانع وقوع رویداد دیگر شود، این دو رویداد غیرقابل جمع خواهند بود. غیرقابل جمع به معنای عدم امکان وقوع همزمان هر دو رویداد است. در این حالت این دو رویداد قطعاً از لحاظ آماری از یکدیگر مستقل خواهند بود. رویدادهای موفقیت و شکست هر جزء غیرقابل جمع هستند. در یک زمان، عملکرد موفق یک پمپ به معنی عدم وقوع رویداد خرابی پمپ است.

۳-۶-۳-۲-۲- احتمال شرطی

مفهوم احتمال شرطی در کلّ تئوری احتمالات بسیار مهم است. برای دو رویداد A و B، احتمال A به شرط اینکه رویداد B رخ داده باشد، را احتمال شرطی گویند و به صورت زیر به دست می‌آید.

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} \qquad (۴-۳)$$

به طور مشابه، داریم:

$$P(B \mid A) = \frac{P(A \cap B)}{P(A)} \qquad (۵-۳)$$

۳-۶-۳-۲-۳- احتمال فصل مشترک رویدادها

از رابطهٔ (۳-۵) می‌توان نوشت:

$$P(A \cap B) = P(A) \times P(B \mid A) \qquad (۶-۳)$$

اگر A و B رویدادهای مستقل باشند، آنگاه احتمال شرطی $P(B \mid A)$ برابر $P(B)$ است، چراکه وقوع رویداد A هیچ تأثیری بر وقوع رویداد B ندارد. در این صورت، رابطه (۳-۶) به صورت زیر ساده می‌شود:

$$P(A \cap B) = P(A) \times P(B) \qquad (۷-۳)$$

بنابراین، هنگامی که دو رویداد A و B مستقل باشند، احتمال اینکه این دو رویداد باهم روی دهند به سادگی برابر حاصل ضرب احتمال وقوع مستقل دو رویداد است. به طور عمومی احتمال وقوع همزمان n رویداد مستقل به صورت زیر محاسبه می‌شود:

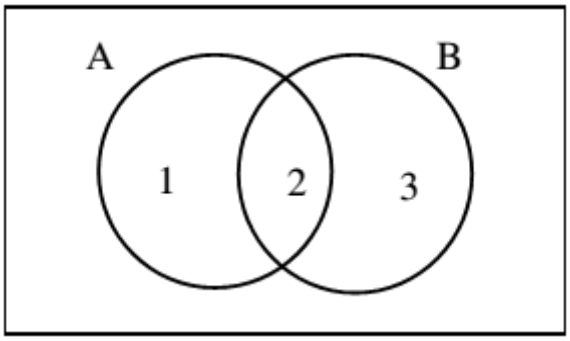
$$P(E_1 \cap E_2 \cap \ldots \cap E_n) = P(E_1) \times P(E_2 \mid E_1) \times P(E_3 \mid E_1 \cap E_2) \times \ldots \times P(E_n \mid E_1 \cap E_2 \cap \ldots \cap E_{n-1}) \qquad (۸-۳)$$

اگر همهٔ رویدادها مستقل باشند، آنگاه احتمال وقوع همهٔ آنها برابر حاصلضرب احتمالات تک تک آنهاست.

$$P(E_1 \cap E_2 \cap \ldots \cap E_n) = P(E_1) \times P(E_2) \times P(E_3) \times \ldots \times P(E_n) \qquad (۹-۳)$$

۳-۶-۳-۲-۴- احتمال اجتماع رویدادها

A و B دو رویداد هستند که در دیاگرام وِن نشان داده شده است. در این شکل نواحی ۱، ۲ و ۳ هیچ‌گونه اشتراکی با هم ندارند و به قولی غیرقابل جمع هستند. برای این شکل روابط زیر صادق است:



شکل ۱۲: دیاگرام وِن اجتماع

$$\begin{aligned} &P(A\cup B)=P(1)+P(2)+P(3),\\ &P(A)=P(1)+P(2),\\ &P(B)=P(2)+P(3). \end{aligned} \qquad (۱۰-۳)$$

$$\begin{aligned} &P(A\cup B)=P(A)+P(B)-P(2),\\ &P(2)=P(A\cap B),\\ &P(A\cup B)=P(A)+P(B)-P(A\cap B). \end{aligned} \qquad (۱۱-۳)$$

رابطه فوق را می‌توان برای n رویداد به صورت زیر توسعه داد.

$$\begin{aligned} &P(E_1\cup E_2\cup\ldots\cup E_n)=\\ &P(E_1)+P(E_2)+\ldots+P(E_n)\\ &-\left[P(E_1\cap E_2)+P(E_2\cap E_3)+\ldots+P(E_{n-1}\cap E_n)\right]\\ &+\left[P(E_1\cap E_2\cap E_3)+P(E_2\cap E_3\cap E_4)+\ldots+P(E_{n-2}\cap E_{n-1}\cap E_n)\right]-\\ &\vdots\\ &(-1)^{n+1}P(E_1\cap E_2\cap\ldots\cap E_n). \end{aligned} \qquad (۱۲-۳)$$

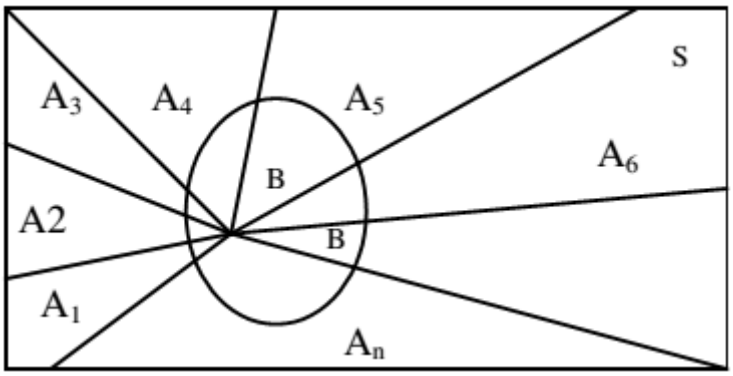
۳-۶-۳-۲-۵- تئوری احتمال کلی

اگر رویدادهای غیرقابل جمعِ $A_1,A_2,\ldots A_n$ تشکیل دهندهٔ یک فضای نمونه‌گیری باشند و $P(A_i)$ احتمال وقوع رویداد A_i باشد. برای یک رویداد دلخواه B می‌توان نوشت:

$$B=B\cap S=B\cap(A_1\cup A_2\cup\ldots\cup A_n)=(B\cap A_1)\cup(B\cap A_2)\cup\ldots\cup(B\cap A_n) \qquad (۱۳-۳)$$

رویدادهای $(B\cap A_1),(B\cap A_2),\ldots,(B\cap A_n)$ غیرقابل جمع هستند. بنابراین خواهیم داشت:

$$P(B)=\sum_i P(B\cap A_i)=\sum_i P(A_i)P(B\mid A_i). \qquad (۱۴-۳)$$



شکل ۱۳: فضای نمونهٔ شامل n رویداد غیرقابل جمع

۳-۶-۳-۲-۶- تئوری بایز

بر اساس تعریف احتمال شرطی و با استفاده از دو رابطهٔ (۳-۴) و (۳-۵)، می‌توان احتمال وقوع رویداد A به شرط وقوع رویداد B را به صورت رابطه زیر نوشت:

$$P(A|B)=\frac{P(A)\times P(B|A)}{P(B)} \qquad (۱۵-۳)$$

این یک نتیجهٔ مفید است. اگر P(B) با استفاده از رابطهٔ تئوری احتمال کلی (۳-۱۴) نوشته شود، رابطهٔ زیر که با نام تئوری بایز شناخته می‌شود، به دست خواهد آمد.

$$P(A_i|B)=\frac{P(A_i)\times P(B|A_i)}{\sum_i P(A_i)P(B|A_i)} \qquad (۱۶-۳)$$

تئوری بایز راهی برای بدست آوردن احتمالاتِ پسین $P(A_i|B)$ بر حسب احتمالات پیشین $P(A_i)$ و احتمالات شرطی $P(B|A_i)$ ارائه می‌کند. این تئوری برای به‌روزرسانی داده‌های خرابی بسیار مفید است؛ چراکه براساس تجربیات بهره‌برداری، شواهد بیشتری از آن در دسترس است.

۳-۶-۳-۳- متغیرهای تصادفی و توزیع‌های احتمال

ارائهٔ خروجی یک آزمایش تصادفی با یک عدد ساده ضروری است. در برخی حالت‌ها، توضیح خروجی‌ها کافی است، ولی در برخی حالت‌های دیگر، به‌کارگیری یک عدد برای هر خروجی در فضای نمونه‌گیری مفید است؛ چراکه خروجی یک آزمایش و مقدارِ نتیجهٔ متغیر پیش از انجام مشخص نیست. به همین دلیل، متغیرهای تصادفی برای به‌کارگیری یک عدد برای خروجی یک آزمایش تصادفی استفاده می‌شود. متغیر تصادفی تابعی است که یک عدد حقیقی به هر خروجی در فضای نمونه‌گیری یک آزمایش تصادفی تخصیص می‌دهد.

متغیرهای تصادفی را می‌توان به دو گروه متغیر تصادفی گسسته و پیوسته تقسیم کرد. متغیر تصادفی، گسسته است اگر فضای نمونه‌گیری آن قابل شمارش باشد. اگر تعداد اجزای فضای نمونه‌گیری بی‌نهایت بوده و فضای نمونه‌گیری پیوسته باشد، متغیر تصادفی در چنین فضایی پیوسته خواهد بود. اگر داده قابل شمارش باشد، با متغیر تصادفی گسسته ارائه می‌شود و اگر داده یک کمیت قابل اندازه‌گیری باشد، با یک متغیر تصادفی پیوسته ارائه می‌شود.

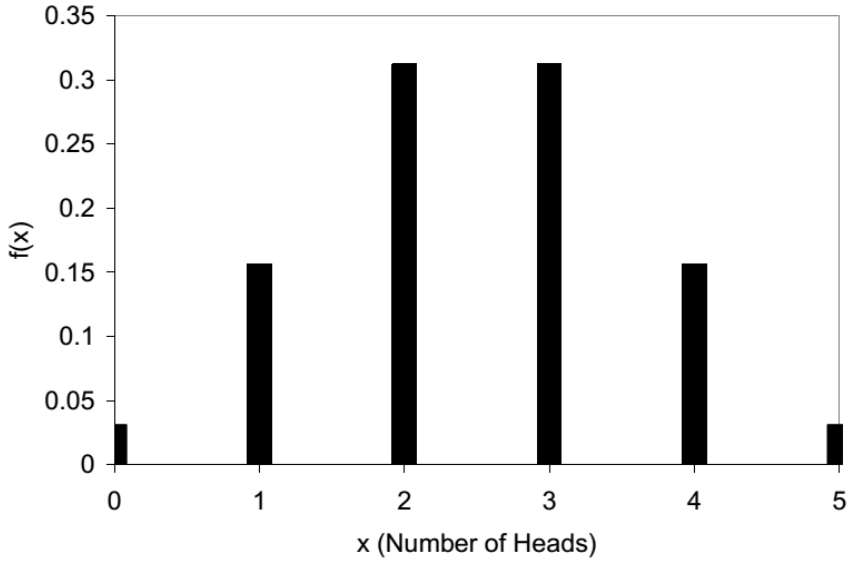
۳-۶-۳-۳-۱- توزیع احتمال گسسته

توزیع احتمالِ یک متغیر تصادفی X بیانی از احتمالات مرتبط با مقادیر ممکن X است. توزیع متغیرهای تصادفی گسسته، اغلب با تنها یک لیست از مقادیر ممکن به همراه احتمال هر یک مشخص می‌شود. در برخی حالت‌ها مرسوم است که احتمال به صورت یک فرمول بیان شود.

X یک متغیر تصادفی گسسته است که در فضای نمونه‌گیری $S=\{x_1,x_2,...,x_n\}$ تعریف شده است. به هر مقدار از S یک مقدار احتمال می‌توان تخصیص داد که با $f(x)$ نشان داده می‌شود. برای یک متغیر تصادفی گسسته X، یک توزیع احتمال تابعی به صورت زیر است:

$$\begin{aligned} &f(x_i)\geq 0,\\ &\sum_{i=1}^{n} f(x_i)=1,\\ &f(x_i)=P(X=x_i). \end{aligned} \qquad (۱۷-۳)$$

توزیع احتمال با عنوان تابع جرم احتمال نیز شناخته می‌شود. برخی نمونه‌های توزیع احتمال توزیع‌های دودویی، پواسون و هندسی هستند. تصویر یک توزیع احتمال گسسته مانند نمودارهای نواری یا هیستوگرام است. به عنوان مثال در پنج‌بار پرتاب یک سکه، که X نشان دهندهٔ تعداد دفعات آمدن روی خط سکه است، تابع جرمی احتمال در شکل ۱۴ نشان داده شده است. بر اساس این شکل، احتمال اینکه از پنج بار پرتاب سکه، ۳بار روی خط سکه بیاید، برابر ۰/۳ است و احتمال اینکه هر ۵ بار روی خط سکه بیاید، کمتر از ۰/۰۵ است.

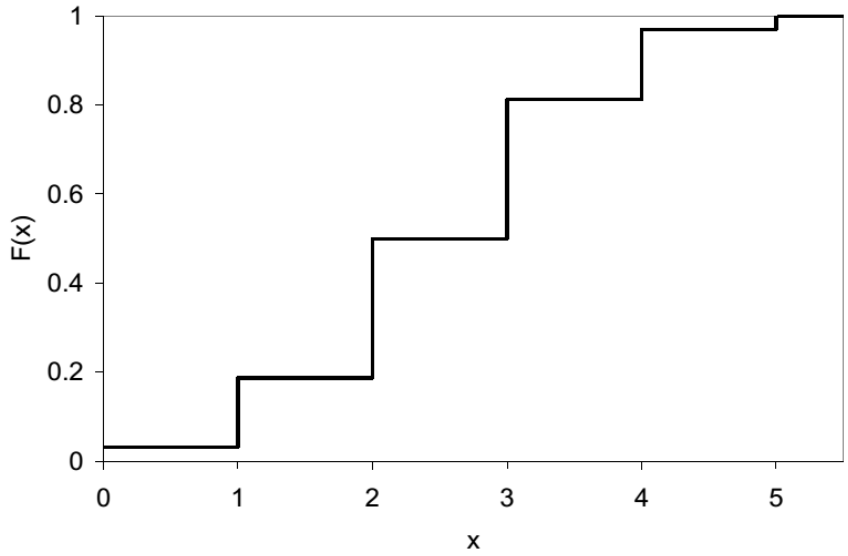


شکل ۱۴: یک تابع جرمی احتمال گسسته

تابع توزیع تجمعی (CDF) یک متغیر تصادفی گسستهٔ X با F(x) نشان داده می‌شود که دو ویژگی زیر را دارد. تابع توزیع تجمعی مثال فوق در شکل ۱۵ آمده است.

$$F(x) = P(X \le x) = \sum_{x_i \le x} f(x_i),$$
$$0 \le F(x) \le 1,$$
$$if\ (x \le y) then (F(x) \le F(y)).$$

(۱۸-۳)



شکل ۱۵: تابع توزیع احتمال تجمعی

۳-۶-۳-۳-۲- توزیع احتمال پیوسته

از آنجایی که تعداد اجزای فضای نمونه‌گیری برای یک متغیر تصادفی پیوسته X، نامحدود هستند، احتمال فرض دقیق هر یک از مقادیر ممکن، صفر است. توابع چگالی معمولاً در مهندسی برای بیان سیستم‌های فیزیکی به کار می‌روند. به‌طور مشابه، یک تابع چگالی احتمال $f(x)$ برای بیان توزیع احتمال یک متغیر تصادفی پیوسته X استفاده می‌شود. احتمال اینکه X بین a و b باشد، با انتگرال‌گیری از $f(x)$ از a تا b تعیین می‌شود. برای یک متغیر تصادفی پیوسته X، یک تابع چگالی احتمال (PDF) تابعی با شرایط زیر است:

$$\begin{aligned} &f(x) \geq 0, \\ &\int_{-\infty}^{+\infty} f(x) = 1, \\ &P(a \leq X \leq b) = \int_{a}^{b} f(x). \end{aligned} \qquad (۱۹-۳)$$

تابع توزیع تجمعی یک متغیر تصادفی پیوسته به صورت زیر است:

$$F(x) = P(X \leq x) = \int_{-\infty}^{x} f(\theta) d\theta. \qquad (۲۰-۳)$$

تابع چگالی احتمال یک متغیر تصادفی پیوسته می‌تواند با مشتق‌گیری از تابع توزیع تجمعی به دست آید.

$$\begin{aligned} &\frac{d}{dx} \int_{-\infty}^{x} f(\theta) d\theta = f(x), \\ &f(x) = \frac{dF(x)}{dx}. \end{aligned} \qquad (۲۱-۳)$$

۳-۶-۳-۳-۳- ویژگی‌های متغیرهای تصادفی

به منظور ارائه تابع توزیع احتمال یک متغیر تصادفی، برخی مقادیر مشخصه مانند مقدار مورد انتظار (متوسط) و میزان انحراف از مقدار متوسط (واریانس) نیز به طور وسیعی استفاده می‌شوند. مقدار مورد انتظار یا مقدار متوسط، تمایل مرکزی یک تابع توزیع را نشان می‌دهد و به صورت زیر محاسبه می‌شود.

$$mean = E(x) = \begin{cases} \sum_{i} x_i f(x_i) & for \quad discrete, \\ \int_{-\infty}^{+\infty} x f(x) dx & for \quad continous. \end{cases} \qquad (۲۲-۳)$$

در رابطه فوق، مقیاسی از انتشار یا انحراف توزیع احتمال با واریانس نشان داده می‌شود. این کمّیت همچنین با ممان مرکزی یا ممان دوم مقدار متوسط شناخته می‌شود و به صورت زیر محاسبه می‌شود.

$$Variance = E((x-mean)^2) = \begin{cases} \sum_{x} (x-mean)^2 f(x) & for \quad discrete, \\ \int_{-\infty}^{+\infty} (x-mean)^2 f(x) dx & for \quad continous. \end{cases} \qquad (۲۳-۳)$$

۳-۶-۴- توابع قابلیت اطمینان و مخاطرات

۳-۶-۴-۱- تابع موفقیت یا تابع قابلیت اطمینان

T یک متغیر تصادفی است که زمان خرابی یک جزء یا سیستم را نشان می‌دهد. قابلیت اطمینان عبارت است از احتمال اینکه آن سیستم وظیفهٔ مورد انتظار را تحت شرایط تعیین شدهٔ محیطی در بازهٔ زمانی مشخص انجام دهد. از لحاظ ریاضی، قابلیت اطمینان را می‌توان به صورت احتمال اینکه مدت زمان سپری شده تا خرابی جزء یا سیستم، بزرگتر یا مساوی زمان تعیین شده t باشد، تعریف کرد.

$$R(t) = P(T \geq t) \qquad (۲۴-۳)$$

۳-۶-۴-۲- تابع خرابی

از آنجا که قابلیت اطمینان، عملکردِ بدون خرابی را مشخص می‌کند، می‌توان آن را احتمال موفقیت در نظر گرفت. برعکس، احتمال عملکرد غیرموفق سیستم پیش از زمان t، احتمال خرابی یا عدم اطمینان نامیده می‌شود. از لحاظ ریاضی احتمال خرابی احتمال آن است که زمان خرابی سیستم پیش از زمان تعیین شده t رخ دهد.

$$\bar{R}(t) = P(T < t) \qquad (۲۵-۳)$$

در تطابق با تئوری احتمالات، $\bar{R}(t)$ همان توزیع احتمال تجمعی (CDF) متغیر تصادفی T است.

$$F(t) = \bar{R}(t) = P(T < t) \qquad (۲۶-۳)$$

بر اساس ویژگی اول احتمالات، احتمال یک فضای نمونه‌گیری برابر ۱ است و در فضای نمونه‌گیری برای متغیر تصادفی پیوسته T مقداری بین صفر تا بی‌نهایت وجود دارد.

فضای نمونه‌گیری می‌تواند دو بخش غیرقابل جمع را تشکیل دهد: بخشی که در آن سیستم موفق است و بخش دیگر که در آن سیستم خراب است. با توجه به ویژگی سوم احتمالات، می‌توان نوشت:

$$P(S) = P(0 < T < \infty) = P(T < t \cup T \geq t) = P(T < t) + P(T \geq t) = 1,$$
$$F(t) + R(t) = 1. \qquad (۲۷-۳)$$

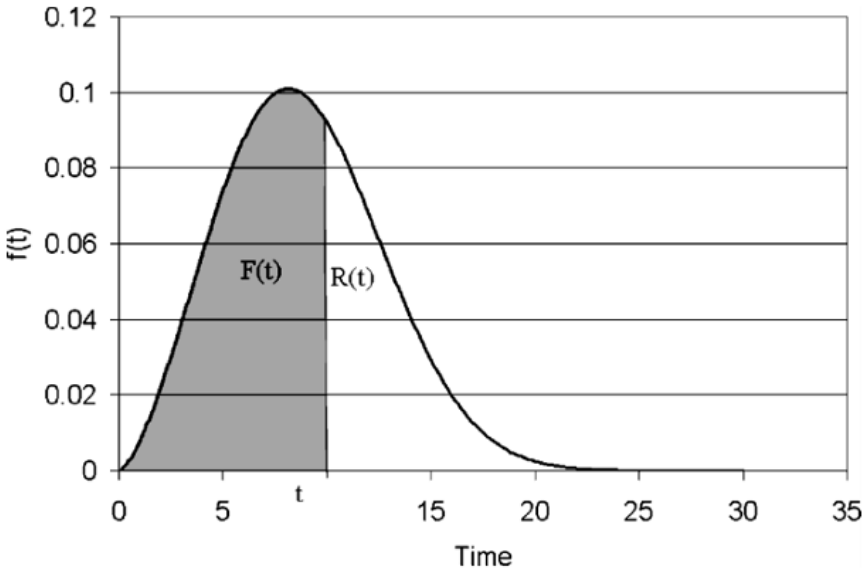
۳-۶-۴-۳- تابع چگالی احتمال خرابی

تابع چگالی احتمال خرابی به صورت زیر تعریف می‌شود:

$$f(t) = \lim_{\Delta t \to 0} \frac{F(t+\Delta t) - F(t)}{\Delta t} = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt} \qquad (۲۸-۳)$$

با داشتن تابع چگالی احتمال خرابی $f(t)$ ، می‌توان تابع خرابی (تابع توزیع احتمال تجمعی) و تابع قابلیت اطمینان را از روابط زیر به دست آورد.

$$F(t) = \int_0^t f(t)dt,$$
$$R(t) = \int_t^\infty f(t)dt. \qquad (۲۹-۳)$$



شکل ۱۶: تابع چگالی احتمال، تابع خرابی و تابع موفقیت

۳-۶-۴-۴- تابع چگالی احتمال خرابی شرطی یا نرخ خرابی

احتمال شرطی خرابی در یک بازهٔ زمانی بین t و $t+\Delta t$، به این شرط که سیستم تا زمان t سالم بماند، به صورت زیر است.

$$P(t \le T \le t+\Delta t \,|\, T \ge t) = \frac{R(t) - R(t+\Delta t)}{R(t)}. \qquad (۳۰-۳)$$

با تقسیم عبارت فوق بر Δt، احتمال شرطی خرابی به ازای واحد زمان که همان نرخ خرابی است، بدست می‌آید.

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{R(t) - R(t+\Delta t)}{R(t)\Delta t} = -\frac{dR(t)}{dt}\frac{1}{R(t)} = \frac{f(t)}{R(t)}. \qquad (۳۱-۳)$$

این تابع، نرخ خطر آنی یا تابع نرخ خرابی نامیده می‌شود. از رابطه فوق می‌توان قابلیت اطمینان یا احتمال موفقیت را به صورت زیر به دست آورد.

$$R(t) = \exp\left[-\int_0^t \lambda(\theta)d\theta\right]. \qquad (۳۲-۳)$$

۳-۶-۴-۵- تابع قابلیت نگهداری

این تابع به صورت احتمال اینکه سیستم در بازهٔ زمانی صفر تا t تعمیر شود، تعریف می‌شود و بدین معنی است که سیستم در زمان صفر خراب شده است. اگر Y متغیر تصادفی باشد که بازهٔ خراب شدن (یا بازهٔ تعمیر) سیستم باشد، و M تابع توزیع باشد، با فرض اینکه M تابع پیوسته است، داریم:

$$M(t) = P(Y \le t),$$
$$m(t) = \frac{dM(t)}{dt}. \qquad (۳۳-۳)$$

تابع نرخ تعمیر به صورت زیر به دست می‌آید.

$$\mu(t) = \lim_{\Delta t \to 0} \frac{P(t \le T \le t + \Delta t \mid T \ge t)}{\Delta t}. \qquad (۳۴-۳)$$

۳-۶-۴-۶- تابع زمان متوسط

این تابع نقش بسیار مهمی در ارتباط با قابلیت اطمینان بازی می‌کند، چراکه شامل شاخص‌های مقایسهٔ قابلیت اطمینان سیستم‌ها است. تابع زمان متوسط خرابی به صورت زیر است.

$$MTTF = \int_0^t t dF(t) = \int_0^t t f(t) dt \qquad (۳۵-۳)$$

تابع زمان متوسط تعمیر به صورت زیر است:

$$MTTR = \int_0^t t dM(t) = \int_0^t t m(t) dt \qquad (۳۶-۳)$$

۳-۶-۵- انواع توابع توزیع

در این بخش مهم‌ترین توزیع‌های احتمال به کار رفته در مطالعات قابلیت اطمینان و ایمنی ارائه می‌شود. این توابع به دو گروه گسسته و پیوسته تقسیم می‌شوند.

۳-۶-۵-۱- توابع توزیع گسسته

۳-۶-۵-۱-۱- تابع توزیع دودویی

یک آزمایش که تنها دو خروجی موفقیت و شکست دارد را در نظر بگیرید. متغیر تصادفی X در این آزمایش می‌تواند مقدار موفقیت (X=1) یا شکست (X=0) داشته باشد. متغیر تصادفی X یک متغیر تصادفی دودویی است، اگر تابع جرمی احتمال به صورت زیر باشد:

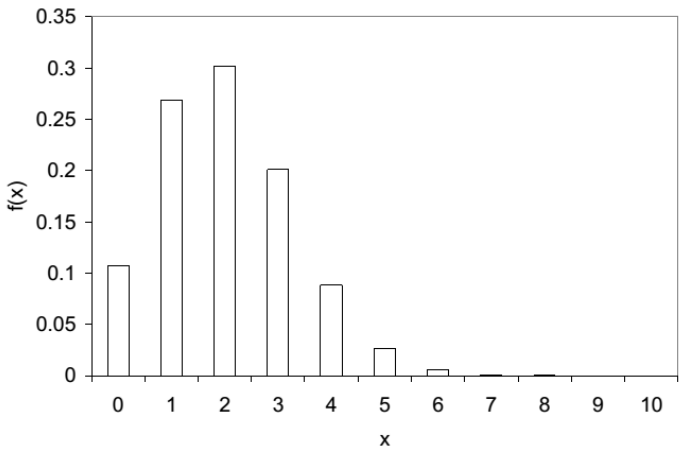
$$P(X=1)=p,\quad P(X=0)=1-p. \tag{۳۷-۳}$$

در این رابطه p احتمال موفق بودن نتیجه آزمایش است. حال اگر n بار آزمایش به صورت مستقل انجام شود، نتیجه هر بار آزمایش با احتمال p، حالت موفق و با احتمال 1-p، حالت شکست خواهد بود. اگر X نشان‌دهندهٔ تعداد موفقیت‌های واقع در n بار انجام آزمایش باشد، X متغیر تصادفی دودویی با پارامترهای n و p نامیده می‌شود. تابع جرمی احتمال متغیر تصادفی دودویی و تابع توزیع احتمال تجمعی به صورت زیر به دست می‌آیند:

$$P(X=i)=\binom{n}{i}p^i(1-p)^{n-i}\qquad i=0,1,2,\ldots,n \tag{۳۸-۳}$$

$$P(X\le i)=\sum_{j=0}^{i}\binom{n}{j}p^j(1-p)^{n-j} \tag{۳۹-۳}$$

تابع جرمی احتمال یک متغیر تصادفی دودویی با پارامترهای ۱۰ و ۰/۲ برای n و p در شکل ۱۷ نشان داده شده است.



شکل ۱۷: تابع جرمی احتمال دودویی

مقدار میانگین و واریانس تابع توزیع دودویی به صورت زیر محاسبه می‌شود:

$$E(x) = np,$$
$$Variance = npq. \quad (۴۰-۳)$$

مثالی برای توزیع دودویی: بر اساس تجربه معلوم شده است که ۴ درصد هارد دیسک تولید شده توسط یک سازنده معیوب هستند. بیش از ۵۰ هارد دیسک آزمایش شدند. احتمال اینکه هیچ مورد خرابی یافت نشود و احتمال اینکه همهٔ هاردها خراب باشند چقدر است؟

$$p(X=0) = \binom{50}{0}(0.04)^0(0.96)^{50} = 0.1299 \quad (۴۱-۳)$$

$$p(X=50) = \binom{50}{50}(0.04)^{50}(0.96)^0 = 1.2676e-70 \quad (۴۲-۳)$$

به عنوان مثال دیگر، به‌منظور تضمین قابلیت اطمینان بالاتر، افزونگی سه‌گانه (که نهایتاً به دو مورد از سه مورد نیاز است) در تجهیزات سیستم‌های نیروگاه هسته‌ای لحاظ شده است. احتمال خرابی هر یک براساس تجربه ۰/۰۱ است. احتمال موفقیت کل سیستم چقدر است؟

جدول شماره ۱۲: محاسبات حل مسأله

	Probability
i	$P(X=0) = \binom{3}{0}(0.99)^0(0.01)^3 = 1e-6$
ii	$P(X=1) = \binom{3}{1}(0.99)^1(0.01)^2 = 2.9e-4$
iii	$P(X=2) = \binom{3}{2}(0.99)^2(0.01)^1 = 2.9e-2$
iv	$P(X=3) = \binom{3}{3}(0.99)^3(0.01)^0 = 0.97$

احتمال خرابی سیستم که مجموع موارد i و ii است، برابر $۲/۹۸ \times ۱۰^{-۴}$ و احتمال موفقیت سیستم که مجموع موارد iii و iv است، برابر ۰/۹۹۹۷۰۲ است.

۳-۶-۵-۱-۲- تابع توزیع پواسون

توزیع پواسون برای مدل‌سازی رویدادهایی که وقوع گسسته و بازه‌های پیوسته دارند، مناسب است. برای یک آزمایش که از نوع پواسون است، شرایط زیر حاکم است:

۱. احتمال وقوع یک رویداد در زمان Δt برابر $\lambda\Delta t$ است که λ ثابت است.

۲. احتمال وقوع بیش از یک بار در بازهٔ Δt، ناچیز است.

۳. هر وقوع از سایر وقوع‌ها مستقل است.

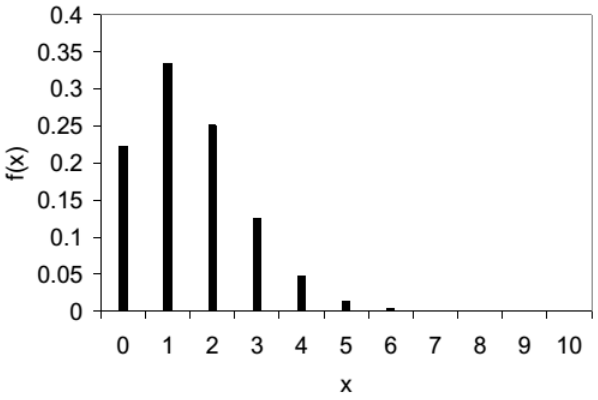
اگر احتمال توزیع متغیر تصادفی X از رابطه زیر تبعیت کند، آن متغیر توزیع پواسون خواهد داشت.

$$f(x)=\frac{e^{-\lambda t}(\lambda t)^{x}}{x!}, x=0,1,2,... \qquad (۴۳-۳)$$

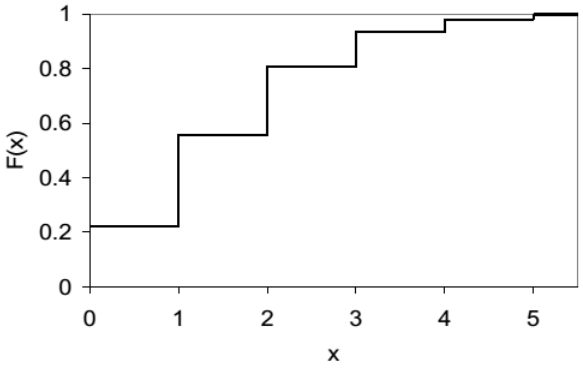
λ نرخ وقوع متوسط نام دارد و x تعداد وقوع رویداد پواسون است. تابع تجمعی احتمال به صورت زیر است:

$$F(x)=\sum_{i=0}^{x} f(X=i). \qquad (۴۴-۳)$$

تابع جرمی احتمال و تابع تجمعی برای λ برابر ۱/۵ بار در سال و t برابر ۱ سال در شکل ۱۸ نشان داده شده است. مقدار متوسط و واریانس توزیع پواسون هر دو برابر با λt است.



(a)



(b)

شکل ۱۸: تابع جرمی احتمال و تابع توزیع تجمعی

به عنوان مثال، اگر نرخ خرابی یک جزء برابر دو بار در سال باشد، احتمال اینکه در طول دو سال خرابی رخ ندهد، به صورت زیر محاسبه می‌شود. در این حالت، x برابر صفر است.

$$f(x=0)=\frac{e^{-\lambda t}(\lambda t)^{x}}{x!}=\frac{e^{-2\times 2}(2\times 2)^{0}}{0!}=0.0183 \qquad (۴۵-۳)$$

اگر احتمال وقوع نزدیک صفر بوده و اندازهٔ فضای نمونه بسیار بزرگ باشد، توزیع پواسون مشابه توزیع دودویی می‌شود.

۳-۶-۵-۱-۳- توزیع هندسی

در توزیع دودویی، تعداد آزمایش‌ها ثابت است و تعداد دفعات موفّقیّت، یک متغیّر تصادفی است. توزیع هندسی هنگامی به‌کار می‌رود که تعدادِ دفعات آزمایش تا حصول اولین موفقیت مورد نظر باشد. متغیر تصادفی در این توزیع، تعداد دفعات آزمایش برای اولین موفقیت است. تابع جرمی احتمال توزیع هندسی به صورت زیر است که در آن p احتمال موفقیت در یک آزمایش است. مقدار متوسط و واریانس برای این توزیع نیز در این روابط ارائه شده‌اند.

$$f(x) = P(x;p) = p(1-p)^{x-1}, x = 1,2,3,\ldots,n,$$
$$E(x) = \frac{1}{p},$$
$$V(x) = \frac{1-p}{p^2}. \quad (۴۶-۳)$$

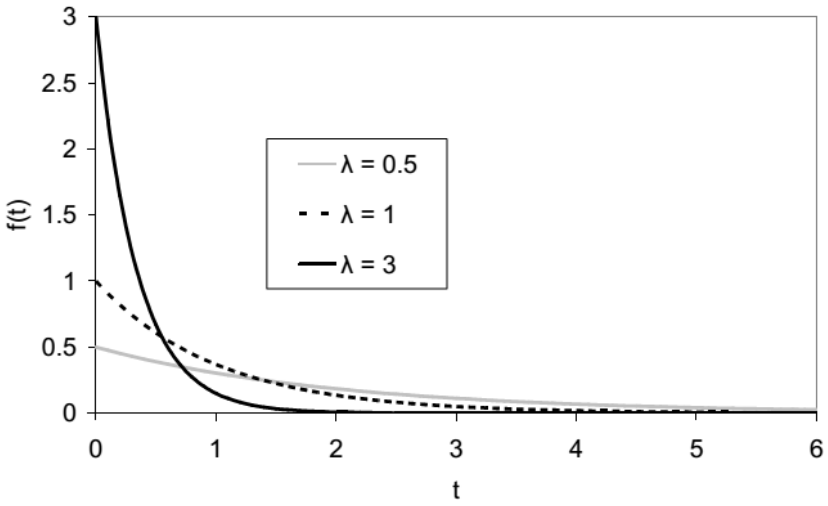
۳-۶-۵-۲- توابع توزیع پیوسته

۳-۶-۵-۲-۱- توزیع نمایی

توزیع نمایی پرکاربردترین توزیع در ارزیابی ریسک و قابلیت اطمینان است و تنها توزیعی است که نرخ مخاطره ثابت داشته و برای مدل‌سازی عمر مفید سیستم‌های مهندسی بسیاری به کار می‌رود. توزیع نمایی به توزیع پواسون که گسسته است، بسیار نزدیک است. اگر دفعات خرابی به ازای واحد زمان توزیع پواسون داشته باشد، آنگاه زمان بین خرابی‌ها از توزیع نمایی پیروی می‌کند. تابع توزیع احتمال (PDF) توزیع نمایی به صورت زیر است.

$$f(t) = \lambda e^{-\lambda t} \quad for \quad 0 \le t \le \infty,$$
$$f(t) = 0 \quad for \quad t < 0. \quad (۴۷-۳)$$

تابع توزیع احتمال نمایی برای مقادیر مختلف λ در شکل ۱۹ نشان داده شده است.



شکل ۱۹: تابع توزیع احتمال نمایی

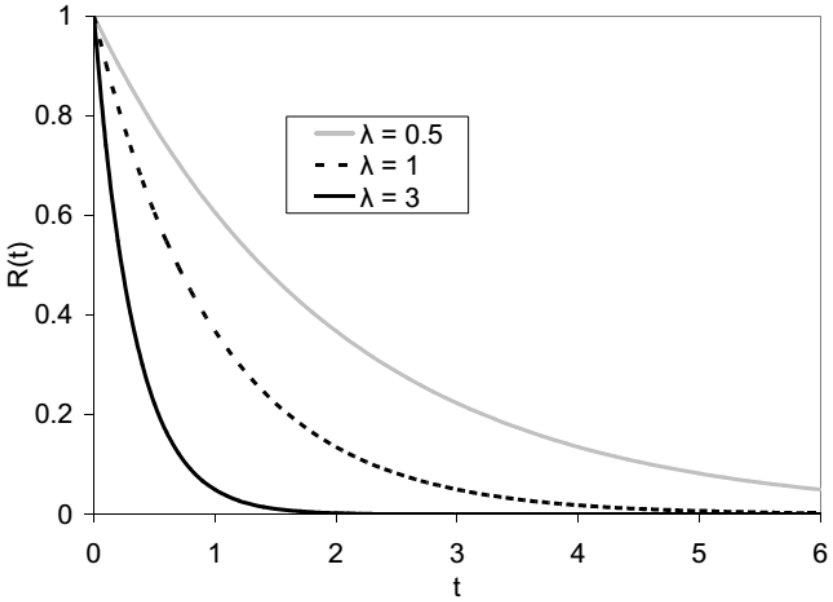
تابع تجمعی توزیع احتمال نمایی به صورت زیر است.

$$F(t)=\int_0^t f(t)dt=\int_0^t \lambda e^{-\lambda t}dt=\lambda\left[\frac{e^{-\lambda t}}{-\lambda}-\frac{1}{-\lambda}\right]=1-e^{-\lambda t}. \quad (۴۸-۳)$$

تابع قابلیت اطمینان متمم تابع توزیع تجمعی است.

$$R(t)=1-F(t)=e^{-\lambda t}. \quad (۴۹-۳)$$

تابع قابلیت اطمینان توزیع نمایی در شکل ۲۰ برای مقادیر مختلف λ ارائه شده است.



شکل ۲۰: تابع قابلیت اطمینان توزیع نمایی

تابع خطر، نسبت تابع توزیع احتمال (PDF) به تابع قابلیت اطمینان است که پیش از این با عنوان نرخ خرابی معرفی شده است.

$$h(t)=\frac{f(t)}{R(t)}=\frac{\lambda e^{-\lambda t}}{e^{-\lambda t}}=\lambda. \quad (۵۰-۳)$$

تابع خطر نمایی یا نرخ خرابی، ثابت λ است و نشان‌دهندهٔ مشخصهٔ عدم وابستگی به زمان در توزیع نمایی است. براساس این مشخصه، احتمال خرابی در بازهٔ زمانی مشخص، صرف‌نظر از نقطهٔ شروع آن بازهٔ زمانی، یکسان است. مقدار میانگین و واریانس توزیع نمایی به صورت زیر است.

$$E(t)=\int_0^\infty tf(t)dt=\int_0^\infty t\lambda e^{-\lambda t}dt=\frac{1}{\lambda} \quad (۵۱-۳)$$

$$V(t)=E(T^2)-(mean)^2=\frac{1}{\lambda^2} \quad (۵۲-۳)$$

مثال: زمان خرابی (T) یک مدار الکتریکی از یک توزیع نمایی نرخ خرابی λ برابر $۱۰^{-۴}$ بار در ساعت پیروی می‌کند. احتمال اینکه ۱. پیش از ۱۰۰۰ ساعت خراب شود، ۲. تا ۱۰۰۰۰ ساعت سالم بماند و ۳. بین ۱۰۰۰ ساعت و ۱۰۰۰۰ ساعت خراب شود، چقدر است؟ مقدار میانگین و زمان متوسط خرابی چقدر است؟

$$\begin{aligned}&1.P(T<1000)=F(T=1000)=1-e^{-0.0001\times1000}=0.09516.\\&2.P(T>10000)=R(T=10000)=e^{-0.0001\times10000}=0.3678.\\&3.P(1000<T<10000)=F(10000)-F(1000)=[1-R(10000)]-F(1000)=0.537.\\&4.Mean=1/\lambda=10000\,h.\end{aligned} \quad (۵۳-۳)$$

زمان متوسط تا خرابی زمانی است که ۵۰ درصد خرابی رخ دهد، یعنی تابع خرابی برابر ۰/۵ باشد. در این صورت زمان متوسط به صورت زیر بدست می‌آید.

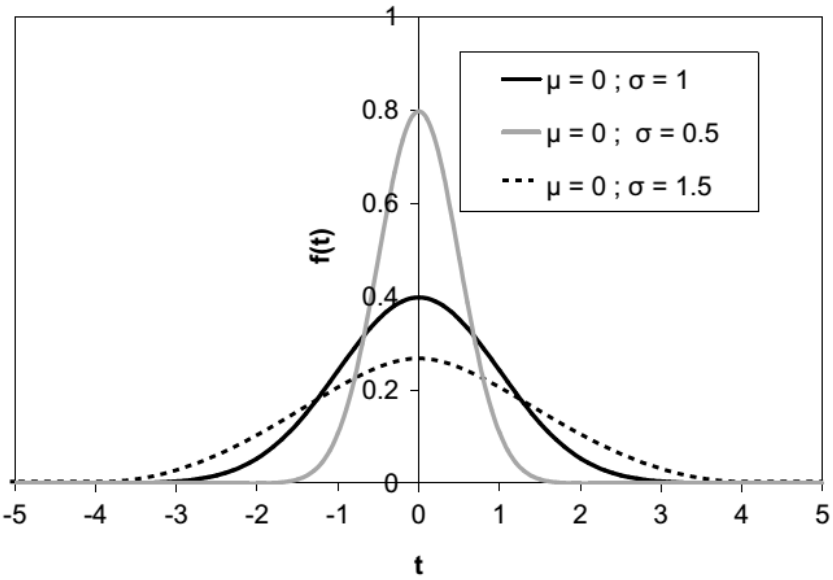
$$R(T)=e^{-0.0001t}=0.5\Rightarrow t=\frac{-\ln(0.5)}{0.0001}=6931.47h. \quad (۵۴-۳)$$

۳-۶-۵-۲-۲- توزیع نرمال

توزیع نرمال پرکاربردترین و مهم‌ترین توزیع در همهٔ زمینه‌های آماری و احتمالاتی است. نام دیگر این توزیع، توزیع گوسی است و جزء اولین توزیع‌ها است که در سال ۱۷۳۳ مطرح شده است. توزیع نرمال اغلب در مسائل کاربردی رخ می‌دهد، زیرا متوسط شمار زیادی از متغیرهای تصادفی مستقلِ آماری به یک توزیع نرمال همگرا می‌شود که با نام تئوری حد وسط شناخته می‌شود. توزیع نرمال می‌تواند برای نواحی فرسایش منحنی وان حمام که شامل خستگی و افزایش سن است، به کار رود. همچنین در مدل‌های تنش – استحکام در مطالعات قابلیت اطمینان قابل استفاده است. تابع توزیع (PDF) نرمال به صورت زیر است.

$$f(t)=\frac{e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2}}{\sigma\sqrt{2\pi}},-\infty\le t\le\infty. \quad (۵۵-۳)$$

در این رابطه، μ و σ پارامترهای توزیع هستند. این توزیع به شکل زنگوله‌ای است که حول مقدار میانگین متقارن است و گسترش توزیع با σ تعیین می‌شود. در شکل ۲۱ این توزیع نشان داده شده است.

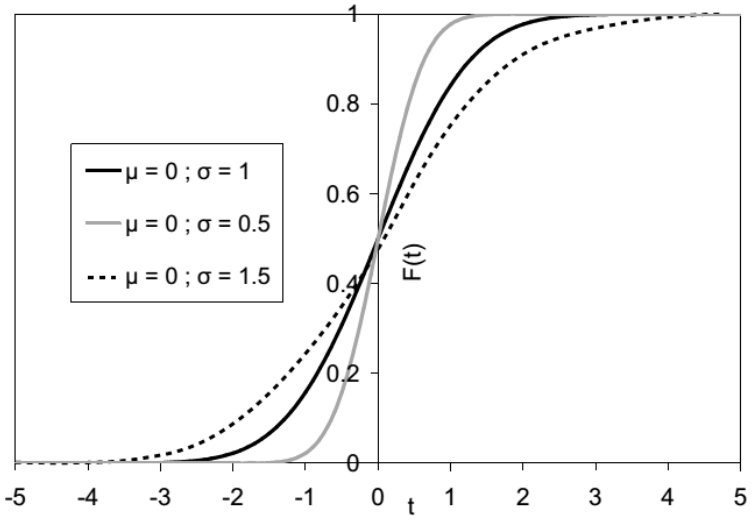


شکل ۲۱: تابع توزیع نرمال

از آنجا که محدودهٔ متغیر تصادفی از منفی بی‌نهایت تا مثبت بی‌نهایت است، توزیع نرمال یک توزیع قابلیت اطمینان صحیح نیست. ولی اگر مقدار میانگین μ، مثبت و بزرگتر از σ باشد، احتمال اینکه متغیر تصادفی T مقدار منفی داشته باشد، قابل صرف‌نظر کردن است و توزیع نرمال می‌تواند تخمین معقولی برای یک فرایند خرابی باشد. تابع قابلیت اطمینان نرمال و تابع تجمعی به صورت زیر است:

$$R(t)=\int_{t}^{\infty}\frac{e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2}}{\sigma\sqrt{2\pi}}dt,$$
$$F(t)=\int_{-\infty}^{t}\frac{e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2}}{\sigma\sqrt{2\pi}}dt. \qquad (۵۶-۳)$$

از آنجا که انتگرال‌های فوق حل تحلیل ندارند، تابع توزیع قابلیت اطمینان و تابع تجمعی آن اغلب به صورت تابعی از توزیع نرمال استاندارد با $\sigma=1$ و $\mu=0$ بیان می‌شوند (شکل ۲۱ و شکل ۲۲).



شکل ۲۲: تابع تجمعی توزیع نرمال

با عبارت زیر، توزیع نرمال استاندارد حاصل می‌شود.

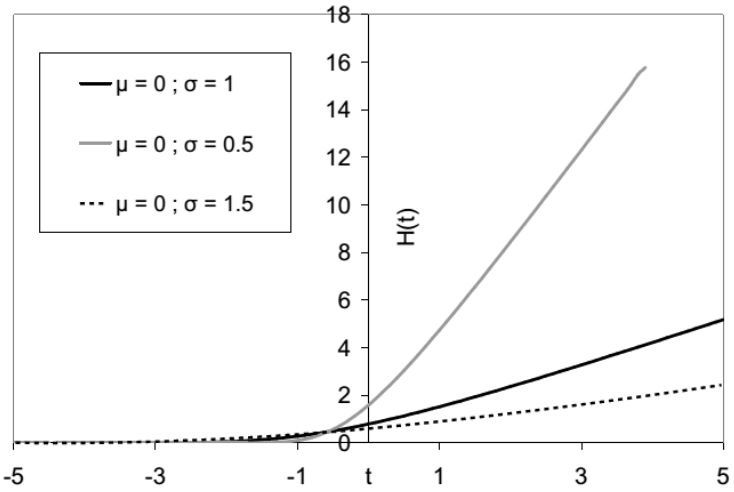
$$z = \frac{t-\mu}{\sigma} \qquad (۵۷-۳)$$

تابع تجمعی توزیع نرمال به صورت زیر بر حسب z بدست می‌آید.

$$\phi(z) = \int_{-\infty}^{z} \frac{e^{-\frac{z^2}{2}}}{\sqrt{2\pi}} dz. \qquad (۵۸-۳)$$

این تابع به صورت جدولی برای توزیع نرمال استاندارد ارائه می‌شود و بر اساس آن، احتمال تجمعی هر توزیع نرمال به دست می‌آید. تابع خطر یا نرخ خرابی برای توزیع نرمال به صورت زیر به دست می‌آید. این تابع در شکل ۲۳ نشان داده شده است.

$$h(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1-\phi(z)}. \qquad (۵۹-۳)$$



شکل ۲۳: تابع نرخ خرابی نرمال

تابع خطر یا نرخ خرابی توزیع نرمال یک روند صعودی دارد و برای مدل‌سازی افزایش سن اجزا مناسب است.

مثال: زمان‌های خرابی ثبت شده از تست‌های عمر یک جزء سیستم مهندسی برابر با ۸۵۰، ۸۹۰، ۹۲۱، ۹۵۵، ۹۸۰، ۱۰۲۵، ۱۰۳۶، ۱۰۴۷، ۱۰۶۵ و ۱۱۲۰ است. با فرض اینکه توزیع نرمال برقرار است، نرخ خرابی آنی در ۱۰۰۰ ساعت چقدر است؟

در این مثال: n=۱۰ و t=۱۰۰۰ است. مقدار متوسط و انحراف از معیار به صورت زیر محاسبه می‌شود.

$$Mean = \bar{x} = \frac{\sum x_i}{n} = \frac{9889}{10} = 988.9 \qquad (۶۰-۳)$$

$$\sigma = \sqrt{\frac{n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2}{n(n-1)}} = 84.8455 \qquad (۶۱-۳)$$

نرخ خرابی آنی از تابع خطر به صورت زیر به دست می‌آید.

$$h(t) = \frac{f(t)}{R(t)} = \frac{f(1000)}{R(1000)} = \frac{f(t)}{1-\phi(z)} = \frac{0.0046619}{1-0.552} = 0.0104 \qquad (۶۲-۳)$$

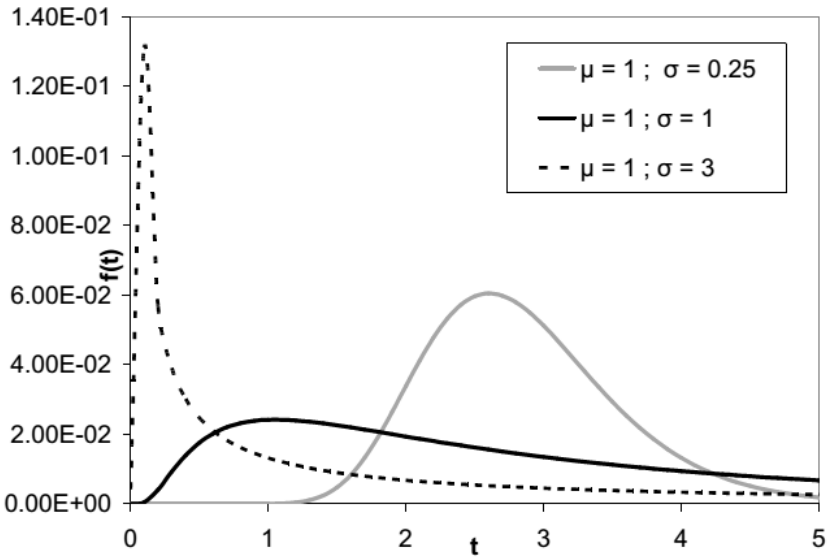
۳-۶-۵-۲-۳- تابع توزیع لوگ‌نرمال

اگر لگاریتم طبیعیِ متغیر تصادفیِ مثبتِ پیوستهٔ T دارای توزیع نرمال باشد، به توزیع آن متغیر تصادفی توزیع لوگ‌نرمال گفته می‌شود. توزیع لوگ‌نرمال می‌تواند برای مدل‌سازی سیکل‌های خرابی فلزات، عمر ترانزیستورها و یاتاقان‌ها و زمان‌های

تعمیر استفاده شود. این توزیع اغلب در تست عمر هنگامی که شمار زیادی از متغیرهای تصادفی مستقل آماری در هم ضرب می‌شوند ظاهر می‌شود. تابع توزیع احتمال PDF لوگ‌نرمال به صورت زیر است:

$$f(t)=\frac{e^{-\frac{1}{2}\left(\frac{\ln t-\mu}{\sigma}\right)^2}}{\sigma t\sqrt{2\pi}},0<t. \qquad (۶۳-۳)$$

در این رابطه، μ و σ پارامتر موقعیت و پارامتر شکل‌دهی هستند. شکل این توزیع بر اساس مقدار σ تغییر می‌کند.



شکل ۲۴: تابع توزیع لوگ‌نرمال

تابع قابلیت اطمینان و تابع تجمعی احتمال لوگ‌نرمال به صورت زیر بدست می‌آیند.

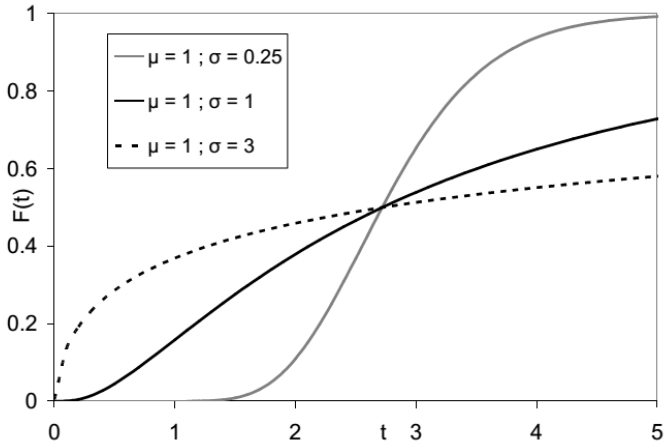
$$R(t)=1-\Phi\left[\frac{\ln t-\mu}{\sigma}\right] \qquad (۶۴-۳)$$

$$F(t)=\Phi\left[\frac{\ln t-\mu}{\sigma}\right] \qquad (۶۵-۳)$$

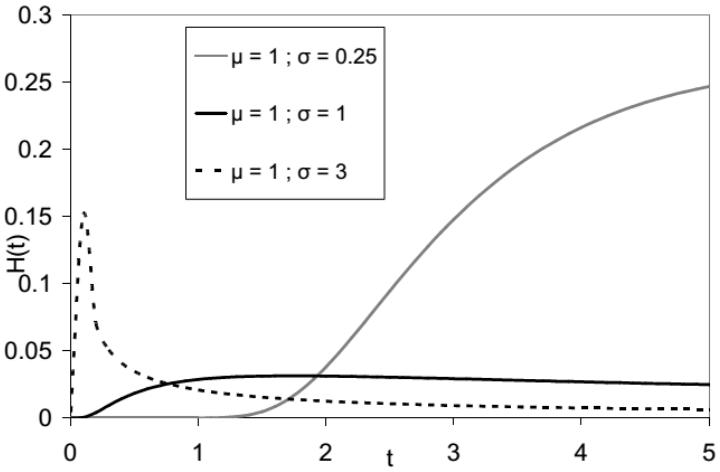
توابع توزیع خرابی لوگ‌نرمال و توابع خطر لوگ‌نرمال در شکل ۲۵ و شکل ۲۶ نشان داده شده است. مقدار میانگین این توزیع و واریانس به صورت زیر محاسبه می‌شود.

$$E(t)=e^{\mu+\frac{\sigma^2}{2}} \qquad (۶۶-۳)$$

$$V(t) = e^{(2\mu+\sigma^2)}(e^{\sigma^2} - 1) \quad (۶۷-۳)$$



شکل ۲۵: تابع توزیع تجمعی لوگنرمال



شکل ۲۶: تابع خطر لوگنرمال

به عنوان مثال، مقدار میانگین و واریانس زمان خرابی برای سیستمی که زمان خرابی آن توزیع لوگ‌نرمال با μ برابر ۵ سال و σ=۰/۸ دارد، به صورت زیر محاسبه می‌شود.

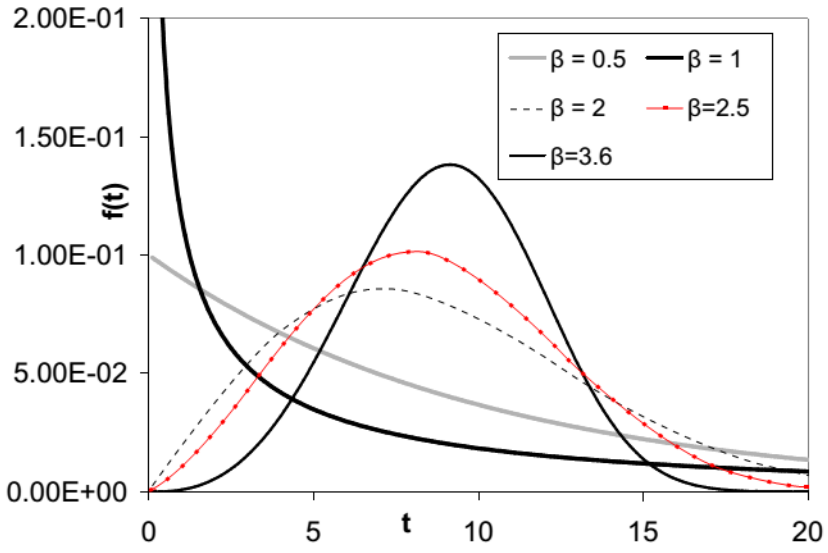
$$E(t) = e^{\mu+\frac{\sigma^2}{2}} = e^{5+\frac{0.8^2}{2}} = 204.3839 \quad (۶۸-۳)$$

$$V(t) = e^{(2\mu+\sigma^2)}(e^{\sigma^2} - 1) = e^{10+0.8^2} \times (e^{0.8^2} - 1) = 37448.49 \quad (۶۹-۳)$$

۳-۶-۵-۲-۴- توزیع وایبال

توزیع وایبال در سال ۱۹۳۳ معرفی شد. این توزیع به دلیل انعطافی که در مدل‌سازی شکل‌های توزیع مختلف دارد، کاربرد وسیعی در محاسبات قابلیت اطمینان دارد. این توزیع می‌تواند برای زمان خرابی لامپ‌ها، رله‌ها، خازن‌ها، ترانزیستورهای ژرمانیوم، یاتاقان‌های کروی، تایرهای خودروها و موتورهای خاص به کار رود. این توزیع علاوه بر اینکه در تحلیل عدم قطعیت پرکاربردترین توزیع است، در دسته‌بندی انواع خرابی، عیب‌یابی، نگهداری پیش‌گیرانه برنامه‌ای و فعالیت‌های بازرسی مفید است. تابع توزیع PDF وایبال به صورت زیر است.

$$f(t)=\frac{\beta}{\alpha}\left(\frac{t}{\alpha}\right)^{\beta-1}e^{-\left(\frac{t}{\alpha}\right)^{\beta}},\quad 0<t. \tag{۳-۷۰}$$



شکل ۲۷: تابع توزیع وایبال

پارامترهای α و β به عنوان پارامتر مقیاس (یا عمر مشخصه) و پارامتر شکل‌دهی شناخته می‌شوند. یک مشخصهٔ مهم توزیع وایبال این است که با افزایش پارامتر β، مقدار میانگین توزیع به α و واریانس به صفر میل می‌کند. این رفتار در شکل ۲۷ قابل مشاهده است. در این شکل، مقدار α برای تمام حالت‌ها برابر ۱۰ فرض شده است. نکته قابل توجه دیگر در این شکل این است که هر منحنی تقریباً مطابق یک تابع توزیع دیگر است. به دلیل این انعطاف‌پذیری، توزیع وایبال مدل مناسبی برای تطابق با داده‌های خرابی حاصل از تجربیات فراهم می‌آورد. در جدول شماره ۱۳ این رفتار خلاصه شده است.

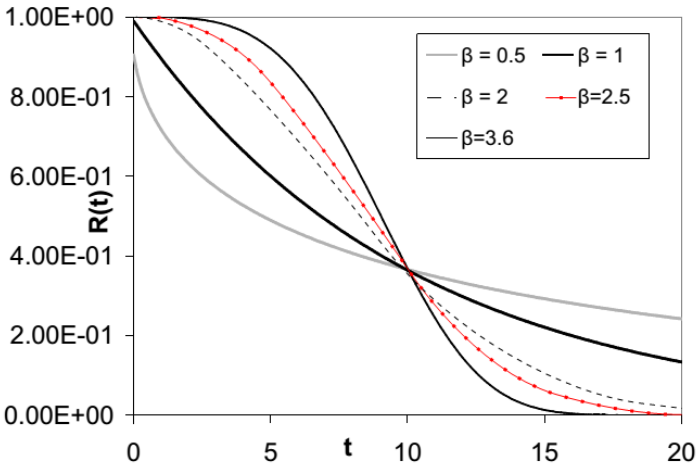
جدول شماره ۱۳: توزیع‌های مبتنی بر مقادیر مختلف β

مقدار β	توزیع
۱	مطابق توزیع نمایی
۲	مطابق توزیع رایلی
۲/۵	مشابه توزیع لوگنرمال
۳/۶	مشابه توزیع نرمال

تابع قابلیت اطمینان و تابع توزیع تجمعی وایبال به صورت زیر می‌باشند.

$$R(t) = e^{-\left(\frac{t}{\alpha}\right)^{\beta}} \qquad (۷۱-۳)$$

$$F(t) = 1 - e^{-\left(\frac{t}{\alpha}\right)^{\beta}} \qquad (۷۲-۳)$$



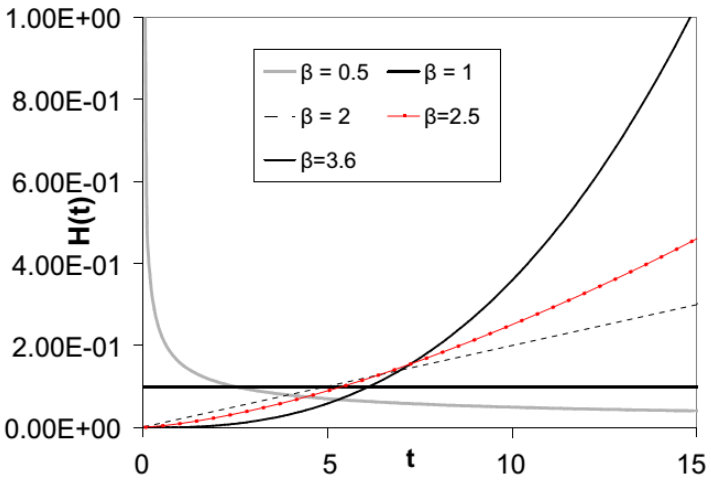
شکل ۲۸: تابع قابلیت اطمینان توزیع وایبال

تابع خطر یا نرخ خرابی در توزیع وایبال به صورت زیر است.

$$f(t) = \frac{\beta t^{\beta-1}}{\alpha^{\beta}} \qquad (۷۳-۳)$$

تأثیر پارامتر β بر تابع خطر در شکل ۲۹ مشهود است. هر سه ناحیهٔ منحنی وان حمام با تغییر β قابل ارائه هستند.

- $\beta<1$ منجر به کاهش نرخ خرابی می‌شود (ناحیه ابتدایی سیستم)،
- $\beta=1$ منجر به نرخ خرابی ثابت می‌شود (ناحیه عمر مفید سیستم)،
- $\beta>1$ منجر به افزایش نرخ خرابی می‌شود (ناحیه پیری سیستم).



شکل ۲۹: تابع خطر یا نرخ خرابی در توزیع وایبال

مقدار میانگین و واریانس به صورت زیر به دست می‌آیند. در این روابط، $\Gamma(x)$ به تابع گاما معروف است.

$$E(T)=\alpha\Gamma\left(1+\frac{1}{\beta}\right),$$
$$\Gamma(x)=\int_0^{\infty} y^{x-1}e^{-y}dy. \qquad (۷۴-۳)$$

$$V(T)=\alpha^2\left[\Gamma(1+\frac{2}{\beta})-\Gamma^2(1+\frac{1}{\beta})\right]. \qquad (۷۵-۳)$$

مثال: زمان خرابی یک جزء دارای توزیع وایبال با پارامتر شکل‌دهی β برابر ۱/۵ و پارامتر مقیاس α برابر ۱۰۰۰۰ ساعت است. اگر حداقل قابلیت اطمینان برای این جزء ۰/۹۵ باشد، چه زمانی باید این جزء تعویض شود؟

از تابع قابلیت اطمینان وایبال داریم:

$$R(t)=e^{-\left(\frac{t}{\alpha}\right)^{\beta}} \Rightarrow 0.95=e^{-\left(\frac{t}{10000}\right)^{1.5}} \Rightarrow \ln\frac{1}{0.95}=\left(\frac{t}{10000}\right)^{1.5} \Rightarrow \log 0.051293=1.5\log\frac{t}{10000} \qquad (۷۶-۳)$$
$$\Rightarrow t=1380.38h.$$

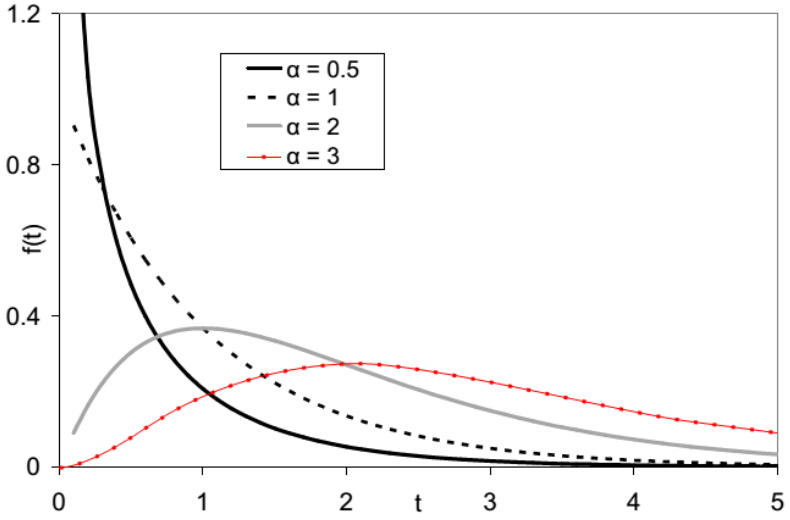
۳-۶-۵-۲-۵- تابع توزیع گاما

همانطور که از نام این توزیع مشخص است، تابع توزیع گاما نامش را از تابع معروف گاما گرفته است. این توزیع شبیه توزیع وایبال است که در آن با تغییر پارامتر توزیع، محدودهٔ وسیعی از سایر توزیع‌ها به دست می‌آیند. توزیع گاما اغلب برای مدل‌سازی عمر سیستم‌ها به کار می‌رود. اگر یک رویداد پس از n رویداد متوالی با توزیع نمایی رخ دهد، متغیر تصادفی

حاصل، از یک توزیع گاما تبعیت می‌کند. مثال کاربرد این توزیع شامل زمان خرابی سیستمِ شامل n جزء مستقل، با n-1 جزء استندبای است، زمان بین اقدامات نگهداری برای یک سیستم که نیازمند نگهداری پس از تعداد دفعات ثابت کار کردن است و یا زمان خرابی سیستمی که پس از n بار شوک، خراب می‌شود. تابع توزیع احتمال گاما به صورت زیر است:

$$f(t)=\Gamma(t;\alpha,\beta)=\frac{\beta^{\alpha}}{\Gamma(\alpha)}t^{\alpha-1}e^{-\beta t},\qquad t\geq 0 \tag{۷۷-۳}$$

α و β پارامترهای توزیع هستند. اگر $\beta=1$ باشد، تابع چگالی گامای استاندارد به دست می‌آید. با تغییر پارامتر α، توزیع‌های مختلف بدست می‌آیند.



شکل ۳۰: تابع توزیع گاما

جدول شماره ۱۴: توزیع گاما با مقادیر مختلف α

مقدار α	نام توزیع
۱	نمایی
عدد صحیح	ارلنگین
۲	مربع - Chi
بزرگتر از ۲	نرمال

تابع توزیع تجمعی برای متغیر تصادفی T با توزیع گاما به صورت زیر است. این تابع حل تحلیلی ندارد و به صورت جدول‌های توزیع گامای استاندارد ارائه می‌شود.

$$F(t)=P(T<t)=\int_{0}^{t}\frac{\beta^{\alpha}}{\Gamma(\alpha)}t^{\alpha-1}e^{-\beta t}dt \tag{۷۸-۳}$$

مقدار میانگین و واریانس توزیع گاما به صورت زیر است.

$$E(T)=\frac{\alpha}{\beta} \qquad (۷۹-۳)$$

$$V(T)=\frac{\alpha}{\beta^2} \qquad (۸۰-۳)$$

خلاصه کاربردهای توابع توزیع اشاره شده در این بخش، در جدول شماره ۱۵ ارائه شده است.

جدول شماره ۱۵: خلاصهٔ زمینه‌های کاربردی توابع توزیع

تابع توزیع	زمینه‌های کاربردی در مطالعات قابلیت اطمینان
پواسون	برای مدل‌سازی نرخ‌های وقوع خرابی‌ها از نوع تعداد بر ساعت یا تعداد خرابی به ازای تعداد اجزا به کار می‌رود.
دودویی	برای مدل‌سازی خرابی K جزء از M جزء یا خرابی در افزونگی مانند افزونگی سه‌گانه در سیستم کنترل و ابزاردقیق
نمایی	برای مدل‌سازی عمر مفید بسیاری از اجزا و توزیع عمر سیستم‌های پیچیدهٔ غیرقابل تعمیر
لوگ‌نرمال	برای مدل‌سازی چرخه‌های خرابی فلزات، عمر ترانزیستورها، عمر یاتاقان‌ها، توزیع اندازی شکست‌های لوله، مدل‌سازی زمان تعمیر به کار می‌رود. این توزیع، به عنوان توزیع پارامتر اولیه در تحلیل بایِز به کار می‌رود.
نرمال	برای مدل‌سازی رشد تلورانس‌ها، تحلیل مقاومت در برابر بار (تنش- استحکام) و توزیع عمر اجزای با تنش بالا
گاما	برای مدل‌سازی زمان خرابی سیستم دارای واحد استندبای و زمان بین تعمیرات به کار می‌رود. این توزیع، به عنوان توزیع پارامتر اولیه در تحلیل بایِز به کار می‌رود.
وایبال	برای $\beta>1$ اغلب در کاربردهایی مانند زمان خرابی اجزای در معرض سایش و یا خستگی (لامپ‌ها، رله‌ها، اجزای مکانیکی) و نیز برای بازرسی‌های دوره‌ای و اقدامات نگهداری پیشگیرانه به کار می‌رود.

۳-۷- تحلیل داده‌های خرابی

اعتبار هر مطالعهٔ قابلیت اطمینان و ایمنی وابسته به کیفیت داده‌های به کار رفته است. این بخش مربوط به رفتار داده‌های خرابی و به کاربردن آنها در مطالعات قابلیت اطمینان و ایمنی است. توسعهٔ مدل‌های قابلیت اطمینان سیستم و معیارهای مختلف آن، یک کاربرد برای تئوری احتمالات است، درحالی‌که تحلیل داده‌های خرابی یک مقولهٔ آماری است. اهداف تحلیل داده‌های خرابی، حصول توابع قابلیت اطمینان و نرخ خطر است که با دو رویکرد به دست می‌آیند. رویکرد اول توسعهٔ توابع تجربی برای قابلیت اطمینان و نرخِ خطر مستقیماً از داده‌های خرابی است. این رویکرد با عنوان «روش‌های غیرپارامتری» یا روش‌های تجربی شناخته می‌شود. رویکرد دوم، شامل شناسایی یک توزیع تئوری تقریبی، تخمین پارامترهای توزیع و انجام تست میزان انطباق با داده‌ها است. این رویکرد با نام «روش پارامتری» شناخته می‌شود.

۳-۷-۱- روش‌های غیرپارامتری

در این روش‌ها، توزیع‌های قابلیت اطمینان تجربی مستقیماً از داده‌های خرابی حاصل می‌شوند. منابع داده‌های خرابی عموماً شامل (۱) تجربهٔ میدانی یا عملکردی و یا (۲) خرابی‌های تولیدشده از تست‌های قابلیت اطمینان هستند. روش‌های غیرپارامتری برای تحلیل داده‌های اولیه برای انتخاب توزیع مناسب، مفید هستند. همچنین هنگامی‌که توزیع پارامتری مناسبی برای داده‌ها یافت نشود، این روش کاربردی است.

تست‌های عمر در یک واحد مشخص تحت شرایط یکسان برای تعداد N واحد که خرابی‌های واحدها از یکدیگر مستقل هستند را در نظر بگیرید. در بازه‌های مشخص زمانی، تعداد واحدهای خراب مشاهده می‌شوند. فرض می‌شود که تست تازمانی که همهٔ واحدها خراب شوند، ادامه می‌یابد. اطلاعات حاصل از این تست به این صورت تحلیل می‌شوند: از تعریف کلاسیک احتمال، احتمال وقوع یک رویداد A به صورت زیر است:

$$P(A)=\frac{n_s}{N}=\frac{n_s}{n_s+n_f} \qquad (۸۱-۳)$$

n_s تعداد دفعات خروجی مطلوب، n_f تعداد دفعات خروجی نامطلوب و N تعداد کل دفعات آزمایش‌ها است. هنگامی‌که N تعداد واحد آزمایش شوند، می‌توان فرض کرد تعداد $n_s(t)$ واحد تا زمان t سالم می‌ماند و تعداد $n_f(t)$ واحد تا زمان t خراب می‌شوند. با استفاده از رابطهٔ فوق، قابلیت اطمینان یک واحد به صورت زیر قابل بیان است.

$$R(t)=\frac{n_s(t)}{N}=\frac{n_s(t)}{n_s(t)+n_f(t)} \qquad (۸۲-۳)$$

در این تعریف از قابلیت اطمینان فرض می‌شود که آزمایش یا تست برای تعداد زیادی از واحدهای یکسان انجام شده است. احتمال خرابی واحد تا زمان t به صورت تابع توزیع تجمعی است.

$$Q(t)\equiv F(t)=\frac{n_f(t)}{N} \qquad (۸۳-۳)$$

مشتق تابع توزیع تجمعیِ یک متغیر تصادفی پیوسته، تابع توزیع احتمال است. در مطالعات قابلیت اطمینان، تابع چگالی خرابیِ مرتبط با زمان خرابی یک واحد می‌تواند به صورت زیر تعریف شود.

$$f(t) \equiv \frac{dF(t)}{dt} = \frac{1}{N}\frac{dn_f(t)}{dt} \qquad (۸۴-۳)$$

تابع نرخ خطر یا نرخ خرابی با تقسیم $f(t)$ بر $R(t)$ به دست می‌آید.

$$h(t) = \frac{1}{n_s(t)}\frac{dn_f(t)}{dt} \qquad (۸۵-۳)$$

بر اساس اطلاعات اولیهٔ مدل خرابی می‌توان توابع پیوسته تکه‌ای برای بازه‌های زمانی رسم کرد. هرچه بازه‌های زمانی کوچکتر باشند، نتایج دقیق‌تری حاصل می‌شوند، اگرچه هزینهٔ محاسباتی افزایش می‌یابد. اگر N کل تعداد خرابی‌ها باشد، تعداد بهینهٔ بازه‌های زمانی از رابطه زیر بدست می‌آید.

$$n = 1 + 3.3\log_{10}^{(N)} \qquad (۸۶-۳)$$

مثال: به منظور تضمین روشنایی صحیح در اتاق‌های کنترل، قابلیت اطمینان بالایی برای لامپ‌های الکتریکی لازم است. زمان‌های خرابی بر حسب ساعت برای تعداد ۳۰ لامپ از یک اتاق کنترل در جدول شماره ۱۶ ارائه شده است. توابع چگالی خرابی، قابلیت اطمینان و نرخ خطر را محاسبه کنید.

جدول شماره ۱۶: داده‌های خرابی

لامپ	زمان خرابی	لامپ	زمان خرابی	لامپ	زمان خرابی
۱	۵۴۹۵/۰۵	۱۱	۳۵۱۱/۴۲	۲۱	۴۰۳۷/۱۱
۲	۸۸۱۷/۸۱	۱۲	۶۸۹۳/۸۱	۲۲	۷۹/۹۳۳
۳	۵۳۹/۶۶	۱۳	۱۸۵۳/۸۳	۲۳	۱۴۸۵/۶۶
۴	۲۲۵۳/۰۲	۱۴	۳۴۵۸/۴	۲۴	۴۱۵۸/۱۱
۵	۱۸۸۸۷	۱۵	۷۷۱۰/۷۸	۲۵	۶۵۱۳/۴۳
۶	۲۴۳۵/۶۲	۱۶	۳۲۴/۶۱	۲۶	۸۳۶۷/۹۲
۷	۹۹/۳۳	۱۷	۸۶۶/۶۹	۲۷	۱۹۱۲/۲۴
۸	۳۷۱۶/۲۴	۱۸	۶۳۱۱/۴۷	۲۸	۱۳۵۷۶/۹۷
۹	۱۲۱۵۵/۵۶	۱۹	۳۰۹۵/۶۲	۲۹	۱۸۴۳/۳۸
۱۰	۵۵۲/۷۵	۲۰	۹۲۷/۴۱	۳۰	۴۶۵۳/۹۹

تعداد بازه‌های بهینه برای این داده‌ها برابر است با:

$$n = 1 + 3.3\log_{10}^{(30)} = 5.87 \qquad (۸۷-۳)$$

به منظور گروه‌بندی زمان‌های خرابی در بازه‌های مختلف، داده‌ها در یک روند صعودی مرتب می‌شوند. جدول شماره ۱۷ داده‌ها را بر حسب روند صعودی زمان‌های خربی نشان می‌دهد. زمان خرابی کمینه و بیشینه برابر ۹۹/۳۳ و ۱۸۸۸۷ است.

جدول شماره ۱۷: داده‌های خرابی

لامپ	زمان خرابی	لامپ	زمان خرابی	لامپ	زمان خرابی
۱	۹۹/۳۳	۱۱	۱۹۱۲/۲۴	۲۱	۵۴۹۵/۰۵
۲	۳۲۴/۶۱	۱۲	۲۲۵۳/۰۲	۲۲	۶۳۱۱/۴۷
۳	۵۳۹/۶۶	۱۳	۲۴۳۵/۶۲	۲۳	۶۵۱۳/۴۳
۴	۵۵۲/۷۵	۱۴	۳۰۹۵/۶۲	۲۴	۶۸۹۳/۸۱
۵	۸۶۶/۶۹	۱۵	۳۴۵۸/۴	۲۵	۷۷۱۰/۷۸
۶	۹۲۷/۴۱	۱۶	۳۵۱۱/۴۲	۲۶	۸۳۶۷/۹۲
۷	۹۳۳/۷۹	۱۷	۳۷۱۶/۲۴	۲۷	۸۸۱۷/۷۱
۸	۱۴۸۵/۶۶	۱۸	۴۰۳۷/۱۱	۲۸	۱۲۱۵۵/۵۶
۹	۱۸۴۳/۳۸	۱۹	۴۱۵۸/۱۱	۲۹	۱۳۵۷۶/۹۷
۱۰	۱۸۵۳/۸۳	۲۰	۴۶۵۳/۹۹	۳۰	۱۸۸۸۷

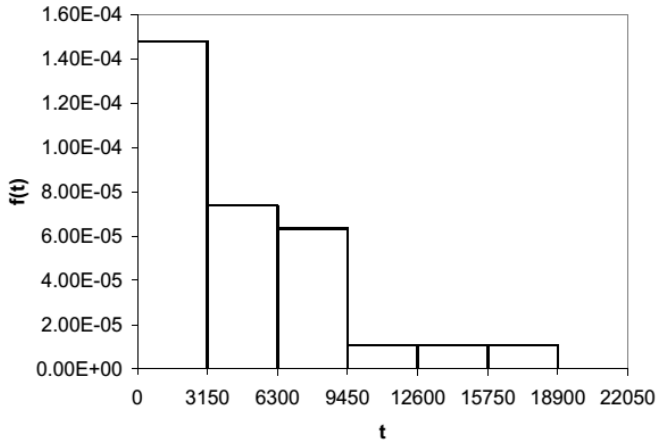
اندازهٔ بازهٔ زمانی به صورت زیر است:

$$\Delta t_i = \frac{18887 - 99.33}{6} = 3131.27 \approx 3150 \qquad (۸۸-۳)$$

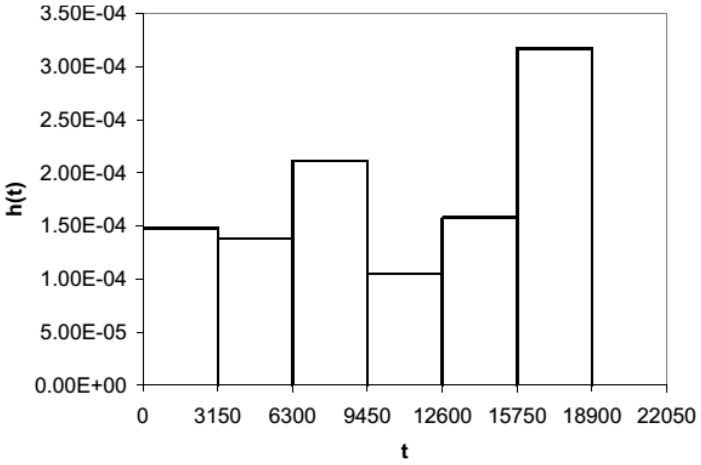
حال می‌توان جدول حاوی بازه‌های زمانی و مقادیر مربوط به توابع $R(t)$، $F(t)$، $f(t)$ و $h(t)$ را بدست آورد. $n_s(t_i)$ تعداد لامپ‌های سالم در ابتدای بازه و $n_f(t_i)$ تعداد خرابی‌ها طی بازهٔ tام است.

جدول شماره ۱۸: جدول محاسبات

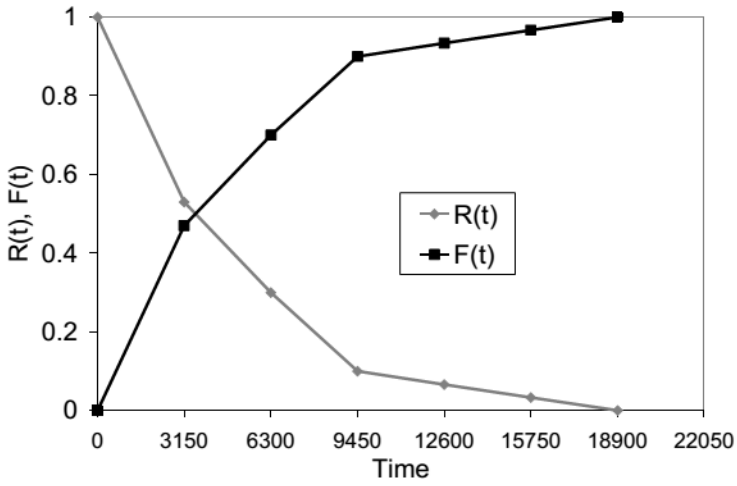
بازه	$n_s(t_i)$	$n_f(t_i)$	$R(t_i)$	$F(t_i)$	$f(t_i)=\frac{n_f(t_i)}{N\Delta t_i}$	$h(t_i)=\frac{n_f(t_i)}{n_s(t_i)\Delta t_i}$
۳۱۵۰-۰	۳۰	۱۴	۱	۰	۱/۴۸×۱۰$^{-۴}$	۱/۴۸×۱۰$^{-۴}$
۶۳۰۰-۳۱۵۱	۱۶	۷	۰/۵۳	۰/۴۷	۷/۴×۱۰$^{-۵}$	۱/۳۸×۱۰$^{-۴}$
۹۴۵۰-۶۳۰۱	۹	۶	۰/۳	۰/۷	۶/۳۵×۱۰$^{-۵}$	۲/۱۱×۱۰$^{-۴}$
۱۲۶۰۰-۹۴۵۱	۳	۱	۰/۱	۰/۹	۱/۰۶×۱۰$^{-۵}$	۱/۰۵×۱۰$^{-۴}$
۱۵۷۵۰-۱۲۶۰۱	۲	۱	۰/۰۶۶	۰/۹۳۴	۱/۰۶×۱۰$^{-۵}$	۱/۵۸×۱۰$^{-۴}$
۱۸۹۰۰-۱۵۷۵۱	۱	۱	۰/۰۳۳	۰/۹۶۷	۱/۰۶×۱۰$^{-۵}$	۳/۱۷×۱۰$^{-۴}$



شکل ۳۱: تابع چگالی خرابی



شکل ۳۲: تابع نرخ خطر



شکل ۳۳: تابع قابلیت اطمینان و تابع توزیع تجمعی

۳-۷-۲- روش‌های پارامتری

در روش‌های پارامتری، توزیع‌های پارامتری از داده‌های خرابی به‌دست می‌آید. روش دوم و توصیه شده برای تحلیل داده‌های خرابی، برازش یک توزیع مانند توزیع نمایی، وایبال یا نرمال است. از آنجا که توزیع‌های تئوری هر یک دارای پارامترهایی هستند، این روش‌ها با عنوان روش‌های پارامتری شناخته می‌شوند. روش‌های غیرپارامتری در قیاس با روش‌های پارامتری محدودیت‌های عملی دارند.

از آنجا که روش‌های غیرپارامتری مبتنی بر داده‌های نمونه هستند، اطلاعات خارج از محدودهٔ داده‌ها قابل تحلیل نیستند. برون‌یابی داده‌ها در یک توزیع تئوری قابل انجام است. دغدغهٔ اصلی تعیین طبیعت احتمالاتی فرایند خرابی مورد نظر است. ممکن است داده‌های خرابی موجود زیرمجموعه‌ای از مجموعهٔ زمان‌های خرابی باشد. فرایند خرابی اغلب نتیجهٔ برخی پدیده‌های فیزیکی است که می‌تواند با یک توزیع مناسب همراه باشد. به کارگیری یک مدل تئوری، تحلیلِ پیچیده را آسان می‌کند. در روش پارامتری، برازش یک توزیعِ تئوری، شامل سه مرحله است:

۱. شناسایی توزیع‌های مناسب

در روش‌های غیرپارامتری، نحوهٔ به دست‌آوردن توزیع تجربی یا هیستوگرام‌ها از داده‌های خرابیِ پایه روشن شد. این تمرین به حدس زدن یک توزیع خرابی که می‌تواند احتمالاً برای مدل‌سازی داده‌های خرابی به‌کاررود کمک می‌نماید. نمودارهای احتمالات، روشی برای ارزش‌یابی برازش یک توزیع برای یک سری از داده‌ها فراهم می‌آورند. یک نمودار احتمال، تصویری است که در آن توزیع تجمعی احتمال به‌صورت یک خط پیوسته است. در مقایسه با نمودارهای هیستوگرام، نمودارهای احتمال، کاربرد آسان‌تری دارند و روش تحلیل، تفسیر و تخمین سریع‌تری برای پارامترهای مرتبط با مدل فراهم می‌کنند. در این مرحله، یک توزیع برای مجموعهٔ داده‌ها شناسایی می‌شود، به این صورت که برای داده‌های موجود یک نمودار خطّی تخمین زده می‌شود.

۲. تخمین پارامترهای توزیع

تخمین پارامترهای توزیع با رسم نمودار احتمال بهترین روش نیست، به خصوص در تست‌های برازش خوب که مبتنی بر تخمین احتمال بیشینه برای پارامترهای توزیع هستند. معیارهای بسیاری بر اساس روش به کار رفته برای تخمین وجود دارد. این روش‌ها شامل روش ویز، روش تخمین مربعات کمینه و روش تخمین احتمال کمینه هستند. روش تخمین احتمال کمینه، حداکثر انعطاف را داشته و بیشترین استفاده را دارد.

۳. انجام تست برازش خوب[۱]

در این مرحله یک تست آماری برای میزان مناسب بودن برازش انجام می‌شود. هدف این تست راستی‌آزمایی تطابق داده‌های مشاهده شده با یک مدل مورد نظر است.

۳-۸- مدل‌های قابلیت اطمینان

در هر تحلیل کمّی از خرابی یک سیستم، باید یک مدل قابلیت اطمینان انتخاب شود. یک مدل قابلیت اطمینان، یک سری از روابط ریاضی است که چگونگی محاسبهٔ مشخصه‌های قابلیت اطمینان اجزای سیستم را تعیین می‌کند. مشخصه‌های قابلیت اطمینان زیر در مدل‌های قابلیت اطمینان محاسبه می‌شوند:

- عدم دسترسی در زمان t، $Q(t)$
- احتمال یا عدم دسترسی میانگین حالت پایای بلند مدت، Q
- شدت خرابی غیرمشروط در زمان t، $W(t)$

هر مدلِ قابلیت اطمینان دارای یک یا چند پارامتر است. این مدل‌ها حاوی یک یا چند پارامتر اختیاری هستند. پارامترهای به کار رفته در این مدل‌ها در جدول شماره ۱۹ ارائه شده است.

جدول شماره ۱۹: پارامترهای مدل‌های خرابی

پارامتر	توضیح
q	احتمال خرابی به ازای نیاز (فراخوانی)
λ	نرخ خرابی
f	فرکانس
μ	نرخ تعمیر
TR	زمان تعمیر (MTTR)
TI	بازه تست
TF	زمان اولین تست
TM	زمان مأموریت

[۱] -goodness-of-fit test

۳-۸-۱- مدل جزء قابل تعمیر

این مدل برای یک جزء عادی قابل تعمیر به کار می‌رود که در آن توزیع‌های نمایی برای فرایند خرابی و فرایند تعمیر فرض می‌شود. یعنی هر دو نرخ خرابی و نرخ تعمیر ثابت هستند. این مدل دارای پارامترهای الزامی و اختیاری زیر است.

- پارامترهای الزامی: $\lambda, \mu(r, TR)$
- پارامترهای اختیاری: q

عدم دسترسی برای این نوع از اجزا که تنها شامل پارامترهای لازم است، به صورت زیر محاسبه می‌شود.

$$Q(t) = \frac{\lambda}{\lambda + \mu}\left[1 - e^{-(\lambda+\mu)t}\right] \qquad (۸۹-۳)$$

این روش، یک روش مرسومِ به‌کاررفته در اغلب تحلیل‌های قابلیت اطمینان است. رفتار نوعی این است که عدم دسترسی در زمان صفر شروع می‌شود و به سرعت تا یک مقدار مجانبیِ حالت پایا رشد می‌کند. پارامتر اختیاری q به این معنی است که جزء در زمان صفر هنگامی که وارد فرایند تعمیر خرابی می‌شود، در دسترس نیست. این حالت در اغلب شرایط استفاده نمی‌شود. رابطهٔ عدم دسترسی با لحاظ پارامتر اختیاری به صورت زیر است:

$$Q(t) = q.e^{-(\lambda+\mu)t} + \frac{\lambda}{\lambda + \mu}\left[1 - e^{-(\lambda+\mu)t}\right] \qquad (۹۰-۳)$$

اگر q بزرگتر از صفر باشد، عدم دسترسی از مقدار q شروع شده و بر حسب مقدار μ به صورت مجانبی به مقدار صفر نزدیک می‌شود. این حالت می‌تواند برای مدل‌های اجزایی که دارای احتمال خرابی اولیه q در زمان صفر بوده و پس از آن یک نرخ خرابی ثابت λ دارند، استفاده شود. هر دو نوع خرابی می‌توانند با یک نرخ تعمیر ثابت μ تعمیر شوند. عدم دسترسی بلند مدت برای این مدلِ قابلیت اطمینان به صورت زیر است:

$$Q = \frac{\lambda}{\lambda + \mu} \qquad (۹۱-۳)$$

اگر این مقدار با رابطهٔ (۳-۹۰) مقایسه شود، مشاهده می‌شود که این حالت زمانی حاصل می‌شود که هر دو ترم اول و دوم این رابطه به مقدار مجانبی خود برسند. این یک تقریب مناسب برای عدم دسترسی برای این نوع از اجزا در بسیاری از شرایط

است، چراکه فرایندهای مرتبط با ترم اول و دوم معمولاً به سرعت به مقدار مجانبی خود می‌رسند. شدت خرابی غیرمشروط برای این نوع مدل به صورت زیر محاسبه می‌شود.

$$W(t) = \lambda(1 - Q(t)) \qquad (۹۲-۳)$$

رفتار نرمال $W(t)$ برای q برابر صفر این است که از مقدار λ شروع شده و سپس به آرامی به یک مقدار مجانبی کاهش می‌یابد. اگر مقدار عدم دسترسی کوچک باشد، به صورت تقریبی $W(t)$ برابر نرخ خرابی خواهد بود.

۳-۸-۲- مدل جزء بازرسی‌شدهٔ متناوب

این مدل پیچیده‌ترین مدل قابلیت اطمینان است. در ساده‌ترین حالت، که تنها نرخ خرابی و بازهٔ زمانی بازرسی (یا تست) مشخص است، این مدل به مدل مرسوم تبدیل می‌شود. این مدل دارای پارامترهای الزامی و اختیاری زیر است:

- پارامترهای الزامی: $\lambda, TI\,(r, TI)$
- پارامترهای اختیاری: q, TF, TR

در این مدل برای فرایند خرابی یک توزیع نمایی (با نرخ خرابی ثابت)، یک بازهٔ زمانی بازرسی (تست) ثابت با زمان اولین تست اختیاری (TF) و یک زمان تعمیر ثابت (TR) فرض می‌شود.

برای ساده‌سازی فهم این مدل، ابتدا باید تنها پارامترهای لازم یعنی نرخ خرابی و بازهٔ زمانی بازرسی به کار روند. در این صورت عدم دسترسی از رابطه زیر به دست می‌آید.

$$Q(t) = 1 - e^{-\lambda(t - T_i)}, \qquad T_i = 0, TI, 2TI, \ldots \qquad (۹۳-۳)$$

اگر پارامتر زمان اولین تست، TF، معلوم باشد، مدل یکسان است، به جز اینکه نقاط زمانی برای بازرسی به اندازهٔ مقدار TF منتقل می‌شوند. یعنی $T_i = 0, TF, TF + TI, TF + 2TI, \ldots$

مقدار میانگین عدم دسترسی با انتگرال‌گیری از رابطه (۳-۹۳) در کل دورهٔ بازرسی به دست می‌آید.

$$Q_{mean} = \frac{1}{TI}\int_0^{TI} Q(t)dt = 1 - \frac{1}{\lambda TI}(1 - e^{-\lambda TI}) \qquad (۹۴-۳)$$

در این مدل فرض شده است زمان تعمیر قابل صرف‌نظرکردن است ($TR = 0$). اگر این فرض معتبر نباشد، می‌توان پارامتر اختیاری TR را به رابطه افزود تا محاسبات شامل سهم عدم دسترسی ناشی از تعمیر شود. در این حالت، فرضیات زیر برقرار هستند:

- اگر در بازرسی، جزء مورد نظر خراب باشد، فرض می‌شود که تعمیر مستقیماً پس از بازرسی انجام می‌شود،
- مدت زمان تعمیر یک مدت ثابت است.

عدم دسترسی برای این نوع از اجزا از روابط زیر محاسبه می‌شوند:

$$Q(t) = 1 - e^{-\lambda t}, \; for \quad t < TF \tag{۹۵-۳}$$

$$Q(t) = Q(TI) = 1 - e^{-\lambda TI}, \; for \quad t = TF + nTI \tag{۹۶-۳}$$

$$Q(t) = Q(TI) + (1 - Q(TI))(1 - e^{-\lambda (t - TI)}), \; for \quad TI < t < TI + TR \tag{۹۷-۳}$$

$$Q(t) = 1 - e^{-\lambda (t - TI)}, \; for \quad TI + TR < t < 2TI \tag{۹۸-۳}$$

عدم دسترسی یک جزء دقیقاً پیش از بازرسی، $Q(TI)$، معادل احتمال نیاز آن جزء به تعمیر پس از بازرسی است. رابطه (۳-۹۷) نیاز به توضیح بیشتر دارد. در این رابطه، ترم اول عدم دسترسی ناشی از تعمیر است. این مقدار برابر احتمال نیاز به تعمیر است (طی تعمیر این جزء در دسترس نیست). ترم دوم سهم عدم دسترسی درصورت موفقیت بازرسی است. این مقدار برابر احتمال عدم نیاز به تعمیر (یک منهای احتمال تعمیر) ضرب در عدم دسترسی در این حالت است. مقدار میانگین عدم دسترسی درصورت لحاظ تعمیر، به صورت زیر خواهد بود.

$$Q_{mean} = 1 - \frac{1}{\lambda TI}(1 - e^{-\lambda TI}) + \frac{TR}{TI}(1 - e^{-\lambda TI}) \tag{۹۹-۳}$$

همچنین می‌توان مقدار ثابت عدم دسترسی q را به روابط افزود که معنای آن احتمال خرابی وابسته به نیاز است که از بازرسی متأثر نیست. در این صورت روابط عدم دسترسی به صورت زیر خواهند بود.

$$Q(t) = 1 - (1 - q)e^{-\lambda t}, \; for \quad t < TF \tag{۱۰۰-۳}$$

$$Q(t) = Q(TI) = 1 - (1 - q)e^{-\lambda TI}, \; for \quad t = TF + nTI \tag{۱۰۱-۳}$$

$$Q(t) = Q(TI) + (1 - Q(TI))(1 - (1 - q)e^{-\lambda(t-TI)}),\ for \quad TI < t < TI + TR \qquad (۱۰۲-۳)$$

$$Q(t) = 1 - (1 - q)e^{-\lambda(t-TI)},\ for \quad TI + TR < t < 2TI \qquad (۱۰۳-۳)$$

مقدار عدم دسترسی میانگین هنگامی که پارامتر عدم دسترسی ثابت افزوده می‌شود، به صورت زیر است.

$$Q_{mean} = 1 - \frac{1}{\lambda TI}(1 - q)(1 - e^{-\lambda TI}) + \frac{TR}{TI}\left[1 - (1 - q)e^{-\lambda TI}\right] \qquad (۱۰۴-۳)$$

شدت خرابی غیرمشروط در همهٔ حالت‌ها از رابطهٔ نرمال (۳-۹۲) به دست می‌آید.

۳-۸-۳- مدل عدم دسترسی ثابت

این مدل، ساده اما پرکاربرد است و از یک مقدار ثابت عدم دسترسی q، که تنها پارامتر است، استفاده می‌کند. این مدل در شرایطی که یک احتمال خرابی هنگام نیاز مورد نظر است، بسیار استفاده می‌شود. نوعاً این مدل هنگام مدل‌سازی یک جزء یا سیستم‌هایی که فعال‌شده و تغییر حالت دارند، به‌کار می‌رود. به عنوان مثال: شیرهایی که در یک حالت مانده و باز یا بسته شدن آنها با خرابی مواجه شده باشد، یا موج‌شکن‌های مدار که بسته یا باز شدن آنها مشکل‌دار شود، یا موتورهایی که تغییر وضعیت آنها به حالت روشن یا خاموش خراب شود، از این قبیل هستند.

این نوع از مدل، رفتار وابسته به زمان ندارد. روابط عدم دسترسی، عدم دسترسی میانگینِ بلند مدت و شدت خرابی غیرمشروط به صورت زیر محاسبه می‌شوند.

$$Q(t) = q \qquad (۱۰۵-۳)$$

$$Q_{mean} = q \qquad (۱۰۶-۳)$$

$$W(t) = 0 \qquad (۱۰۷-۳)$$

۳-۸-۴- مدل جزء با زمان مأموریت مشخص

این مدل، دقیقاً مانند مدل عدم دسترسی ثابت رفتار می‌کند. اما با این تفاوت که در این مدل، عدم دسترسی ثابت مستقیماً به عنوان ورودی دریافت نمی‌شود، بلکه از یک نرخ خرابی و یک زمان مأموریت ثابت محاسبه می‌شود. یک عدم دسترسی ثابت اختیاری q می‌تواند به روابط اضافه شود.

- پارامترهای الزامی: λ, TM
- پارامترهای اختیاری: q

$$Q(t) = 1-(1-q)e^{-\lambda TM}(const.) \quad (۱۰۸-۳)$$

$$Q_{mean} = 1-(1-q)e^{-\lambda TM}(const.) \quad (۱۰۹-۳)$$

$$W(t) = 0 \quad (۱۱۰-۳)$$

۳-۸-۵- مدل فرکانس ثابت

این مدل هنگامی که یک رویداد دارای فرایند پواسون است، یعنی رویداد با فرکانس (نرخ) ثابت رخ می‌دهد، به کار می‌رود.

$$Q(t) = 0 \quad (۱۱۱-۳)$$

$$Q_{mean} = 0 \quad (۱۱۲-۳)$$

$$W(t) = f \quad (۱۱۳-۳)$$

این مدل باید تنها برای رویدادهای آغازگر به کار رود. رویدادهای آغازگر عموماً در درخت‌های رویداد به کار می‌روند، ولی آنها می‌توانند به عنوان رویدادهای پایه در درخت‌های خطا نیز به‌کار روند. در این حالت، قوانین خاصی باید تبعیت شوند.

۳-۸-۶- مدل جزء غیرقابل تعمیر

این مدل دارای خرابی نمایی با نرخ خرابی ثابت است.

- پارامتر الزامی: $\lambda(r)$
- پارامتر اختیاری: q

این مدل نیازمند یک زمان مأموریت T است که در تحلیل مجموعه‌های برشی کمینه به کار می‌رود. رابطهٔ حالت پایهٔ این مدل به صورت زیر است.

$$Q(t) = 1-e^{-\lambda t} \quad (۱۱۴-۳)$$

درصورت داشتن احتمال خرابی هنگام نیاز در زمان صفر، می‌توان پارامتر اختیاری را در رابطه فوق به صورت زیر لحاظ کرد.

$$Q(t) = 1-(1-q)e^{-\lambda t} \qquad (۱۱۵-۳)$$

پارامتر شدت خرابی غیرمشروط در این مدل از رابطه نرمال (۳-۹۲) به دست می‌آید. برای این مدل، تعریف عدم دسترسی متوسط حالت پایای بلند مدت معنای ندارد، چراکه عدم دسترسی به صورت مجانبی به مقدار ۱ می‌رسد.

۳-۹- مدل‌سازی قابلیت اطمینان سیستم

در این بخش، تکنیک‌های مدل‌سازی قابلیت اطمینان سیستم‌ها مانند دیاگرام جعبه‌ای، سیستم‌های سری، موازی، مرکب و ... و مدل‌های مارکوف و شبیه‌سازی مونت کارلو ارائه می‌شود. قابلیت اطمینان سیستم به صورت تابعی از اجزای تشکیل‌دهندهٔ ارزیابی می‌شود.

۳-۹-۱- دیاگرام جعبه‌ای قابلیت اطمینان

یک دیاگرام جعبه‌ای قابلیت اطمینان، یک نمایش گرافیکی از منطق موفقیت یک سیستم است که متشکل از ساختارهای جعبه‌ای یا ماژولار است. با استفاده از این ابزار، درکِ سیستم آسان شده و مسیرهای موفقیت سیستم به‌صورت بصری قابل راستی‌آزمایی است. رویکرد دیاگرام جعبه‌ای با استفاده از بلوک‌ها یا زیرمدل‌ها، اجزای مختلف را یکپارچه می‌کند. با ارزیابی دیاگرام جعبه‌ای، با استفاده از روش‌های تحلیلی، قابلیت اطیمنان سیستم حاصل می‌شود.

مدل‌سازی قابلیت اطمینان با استفاده از دیاگرام جعبه‌ای در ابتدا تنها برای سیستم‌های غیرقابل تعمیر طراحی شد. به عنوان مثال، سیستم‌های فضایی از روش‌های دیاگرام جعبه‌ای برای پیش‌بینی قابلیت اطمینان استفاده می‌شود. بسیاری از سیستم‌های الکترونیکی، اگرچه تعمیر آنها ممکن است، اما تعویض به جای تعمیر بیشتر اتفاق می‌افتد.

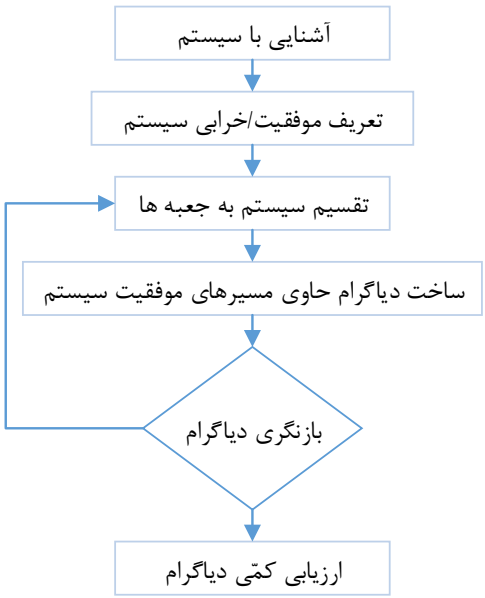
با این وجود، رویکرد دیاگرام جعبه‌ای محدودیت‌هایی در لحاظ کردن مودهای خرابی مختلف، رویدادهای خارجی مانند خطاهای انسانی، و اولویت‌بندی رویدادها در خود دارد. در چنین شرایطی مدل‌های مارکوف و درخت خطا پیشنهاد می‌شوند.

رویهٔ پیش‌بینی قابلیت اطمینان سیستم با استفاده از دیاگرام جعبه‌ای در شکل ۳۴ نشان داده شده است. آشنایی با سیستم، پیش‌نیاز انجام مدل‌سازی قابلیت اطمینان است. پس از آشنایی با سیستم، باید موفقیت سیستم تعریف شود. اگر بیش از یک تعریف ممکن باشد، برای هر تعریف یک دیاگرام جعبه‌ای نیاز است. مرحلهٔ بعد، تقسیم سیستم به جعبه‌های تجهیزات

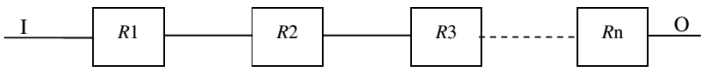
برای بیان رفتار منطقی آنها است به گونه‌ای که هر جعبه به صورت آماری مستقل بوده و تاجایی که ممکن است بزرگ باشد و همزمان هر جعبه نباید حاوی افزونگی باشد. برای برخی ارزیابی‌های عددی، هر جعبه باید حاوی اجزایی باشد که از یک توزیع آماری برای زمان خرابی پیروی می‌کنند. در عمل ممکن است تلاش‌های مکرر در تدوین دیاگرام جعبه‌ای نهایی نیاز باشد.

مرحلهٔ بعد مربوط به تعریف خرابی سیستم و برقراری ارتباطات جعبه‌ها برای تشکیل مسیر موفقیت است. مسیرهای مختلفی بین ورودی و خروجی جعبه‌ها ممکن است. اگر همهٔ جعبه‌ها برای عملکرد سیستم لازم باشند، جعبه‌های اجزا باید مانند شکل ۳۵ به صورت سری به هم متصل شوند. در این شکل، I جعبهٔ ورودی و O جعبهٔ خروجی است و R1، R2 و ... جعبه‌هایی هستند که باهم سیستم را شکل می‌دهند.

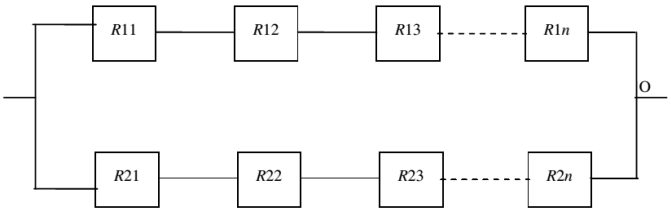
هنگامی که خرابی یک جزء یا یک جعبه، عملکرد سیستم را براساس تعریف خرابی سیستم مختل نمی‌کند، این سیستم حاوی اجزای موازی است. ترکیب حالت سری و موازی در شکل ۳۶ و شکل ۳۷ نشان داده شده است. اغلب سیستم‌ها، ترکیبی از حالت سری و موازی دارند.



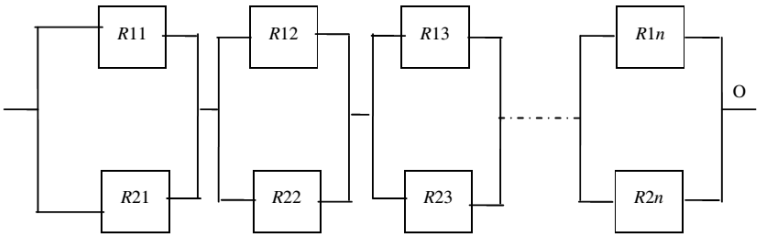
شکل ۳۴: رویهٔ ساخت دیاگرام جعبه‌ای



شکل ۳۵: مدل سری



شکل ۳۶: مدل سری – موازی



شکل ۳۷: مدل موازی - سری

۳-۹-۱-۱- سیستم‌های سری

برای سیستم ارائه شده در شکل ۳۵، همهٔ المان‌ها باید برای موفقیت سیستم عمل کنند. قابلیت اطمینان سیستم به صورت احتمال موفقیت همهٔ اجزا به صورت زیر تعریف می‌شود.

$$R_s = P(A \cap B \cap C \cap ... \cap Z) \qquad (۱۱۶-۳)$$

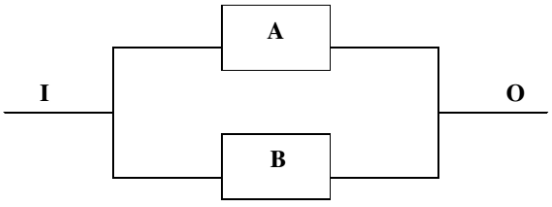
با فرض اینکه اجزا از یکدیگر مستقل هستند، خواهیم داشت:

$$R_s = R_A R_B R_C ... R_z \qquad (۱۱۷-۳)$$

که در آن، قابلیت اطمینان همهٔ جعبه‌های تشکیل دهندهٔ سیستم در هم ضرب می‌شوند.

۳-۹-۱-۲- سیستم‌های موازی

برای سیستم ارائه شده در شکل ۳۸، همهٔ اجزا باید خراب شوند تا سیستم خراب شود. خرابی سیستم برابر احتمال خرابی همهٔ اجزا است که به صورت زیر به دست می‌آید.



شکل ۳۸: مدل دو جزء موازی

$$F_s = P(\overline{A} \cap \overline{B}) \quad (۱۱۸-۳)$$

با فرض اینکه رویدادها از هم مستقل هستند، خواهیم داشت:

$$F_s = F_A F_B \quad (۱۱۹-۳)$$

بنابراین قابلیت اطمینان سیستم به صورت زیر به دست می‌آید.

$$R_s = R_A + R_B - R_A R_B \quad (۱۲۰-۳)$$

۳-۹-۱-۳- سیستم‌های مرکب

اگر یک سیستم مانند شکل ۳۶ داشته باشیم که تنها سه جزء در هر شاخه داشته باشد، قابلیت اطمینان سیستم به صورت زیر به دست می‌آید.

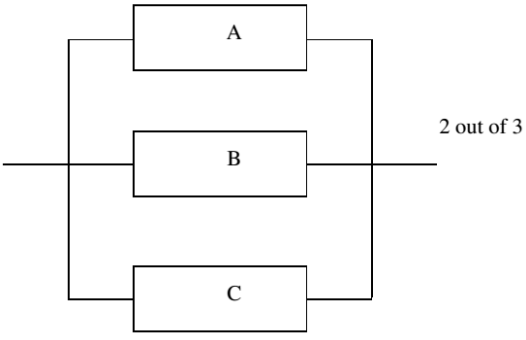
$$R_s = R_{A1}R_{B1}R_{C1} + R_{A2}R_{B2}R_{C2} - R_{A1}R_{B1}R_{C1}R_{A2}R_{B2}R_{C2} \quad (۱۲۱-۳)$$

همچنین برای یک سیستم مانند شکل ۳۷ با سه بخش موازی، قابلیت اطمینان به صورت زیر است.

$$R_s = (R_{A1} + R_{A2} - R_{A1}R_{A2})(R_{B1} + R_{B2} - R_{B1}R_{B2})(R_{C1} + R_{C2} - R_{C1}R_{C2}) \quad (۱۲۲-۳)$$

۳-۹-۱-۴- مدل سیستم M از N

یک سیستم حاوی سه جزء A، B و C را در نظر بگیرید که تنها زمانی خراب می‌شود که بیش از یک جزء در آن خراب شده باشند. این سیستم در شکل ۳۹ نشان داده شده است. در این صورت قابلیت اطمینان سیستم به صورت زیر محاسبه می‌شود.



شکل ۳۹: مدل سیستم دو از سه

$$R_s = 1 - F_A F_B - F_A F_C - F_B F_C + 2F_A F_B F_C$$
$$= 1 - (1-R_A)(1-R_B) - (1-R_A)(1-R_C) - (1-R_B)(1-R_C) + 2(1-R_A)(1-R_B)(1-R_C) \quad (۱۲۳-۳)$$
$$= R_A R_B + R_A R_C + R_B R_C - 2R_A R_B R_C$$

به طور کلی، اگر قابلیت اطمینان یک سیستم شامل n جزء موازی که باید m جزء آن سالم باشند تا سیستم موفق باشد، به صورت زیر به دست می‌آید.

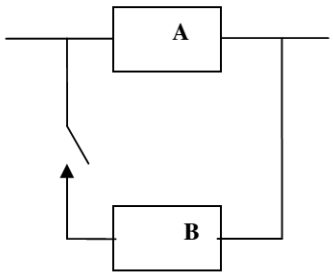
$$R_s = \sum_{r=0}^{n-m} \binom{n}{r} R^{n-r} (1-R)^r \quad (۱۲۴-۳)$$

بنابراین قابلیت اطمینان سیستم شکل ۳۹ با فرض یکسان بودن قابلیت اطمینان هر سه جزء، به صورت زیر خواهد بود:

$$R_s = R^3 + 3R^2(1-R) = 3R^2 - 2R^3 \quad (۱۲۵-۳)$$

۳-۹-۱-۵- سیستم‌های افزونه

ترکیب پرکاربرد دیگر، سیستم‌های افزونه است که در آن چند جزء به صورت موازی و به صورت آماده به کار (استندبای) برای موفقیت سیستم قرار دارند. در ابتدایی‌ترین حالت، ترکیب فیزیکی اجزا در شکل ۴۰ نشان داده شده است.



شکل ۴۰: مدل افزونه آماده به کار

در این شکل، جزء A جزء فعال در سیستم و جزء B جزء افزونهٔ آماده به کار است و جهت جایگزینی جزء A هنگام خرابی، فعال می‌شود. قابلیت اطمینان به صورت زیر محاسبه می‌شود.

$$R_s(t) = e^{-\lambda t}(1+\lambda t) \quad (۱۲۶-۳)$$

فرضیات زیر بر رابطه فوق مترتب است:

۱. هنگام کار هر دو جزء دارای نرخ خرابی ثابت λ و در حالت آماده به کار دارای نرخ خرابی صفر هستند؛

۲. سوئیچ سالم است؛

۳. مدت زمان سوئیچ قابل صرف‌نظر است؛

۴. واحد آماده به کار در زمان انتظار خراب نمی‌شود.

اگر n جزء در حالت آماده به کار باشند، این رابطه به صورت زیر خواهد بود:

$$R_s(t) = e^{-\lambda t}(1+\lambda t+\frac{(\lambda t)^2}{2!}+\frac{(\lambda t)^3}{3!}+...+\frac{(\lambda t)^n}{n!}) \quad (۱۲۷-۳)$$

باید توجه داشت که یک دیاگرام جعبه‌ایِ کاربردی باید شامل جعبه‌هایی باشد که قابلیت اطمینان سوئیچ به‌علاوهٔ مکانیزم حسگر را لحاظ کنند. همچنین، احتمال سالم بودن جزء آماده به کار به زمان خرابی جزء فعال وابسته است. به‌عبارت دیگر، این دو جزء به‌طور کامل از یکدیگر مستقل نیستند. برای لحاظ این نکات باید از مدل مارکوف در تحلیل سیستم آماده به کار استفاده کرد.

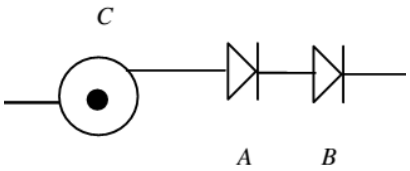
۳-۹-۱-۶- حل دیاگرام جعبه‌ای قابلیت اطمینان

علاوه‌بر مدل‌های استاندارد شرح داده شده در بخش قبلی، ممکن است ترکیب اجزای یک سیستم حالت سری، موازی یا مرکب نباشد. برای این‌گونه مسائل، رویکردهای حل عمومی برای دیاگرام جعبه‌ای ازجمله روش جدول تصدیق، روش مجموعهٔ برشی، مجموعهٔ موفقیت و روش کران‌ها وجود دارد.

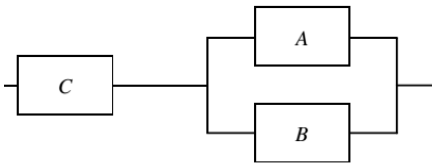
۳-۹-۱-۶-۱- روش جدول تصدیق

این روش با عنوان روش برشمارش رویداد نیز شناخته می‌شود. در این رویکرد، همهٔ ترکیب‌های رویدادها برشمرده شده و حالت سیستم برای هر ترکیب شناسایی می‌شود. به عنوان مثال، اگر n جزء در یک سیستم باشند، با لحاظ موفقیت و شکست برای هر جزء، باید ۲^n ترکیب وجود داشته باشد. همهٔ ترکیب‌ها برای موفقیت سیستم باید بررسی شوند. این روش از لحاظ محاسباتی پرهزینه است. در ادامه مثال ساده‌ای برای بیان این روش ارائه می‌شود.

مثال: بخشی از یک سیستم سیالاتی شامل یک پمپ و دو شیر یک‌طرفهٔ متصل به صورت سری است. شیرهای یک‌طرفهٔ سری در برابر بازگشت جریان هنگامی که پمپ خاموش بوده و فشار پایین‌دست به فشار بالادست می‌رسد، یک افزونگی ایجاد کرده‌اند. این سیستم، در شکل ۴۱ و دیاگرام جعبه‌ای عملکرد آن در شکل ۴۲ نشان داده شده است.



شکل ۴۱: یک سیستم ساده سیالاتی



شکل ۴۲: دیاگرام جعبه‌ای سیستم سیالاتی ساده

با توجه به دیاگرام عملکرد سیستم، عبارت بولی برای این سیستم به صورت زیر به دست می‌آید.

$$R_S = C(A+B) \qquad (۱۲۸-۳)$$

برای این سیستم می‌توان یک جدول تصدیق تهیه کرد (جدول شماره ۲۰). در این جدول مقدار صفر و یک معادل شکست و موفقیت می‌باشند.

- پمپ سالم باشد = ۱
- پمپ خراب باشد = ۰
- شیر یک‌طرفه جریان بازگشتی را ببندد = ۱
- شیر یک‌طرفه جریان بازگشتی را نبندد = ۰
- موفقیت سیستم در حالت عمل نکردن پمپ و بستن جریان بازگشتی توسط شیر = ۱
- خرابی سیستم در حالت عمل کردن پمپ = ۰

جدول شماره ۲۰: جدول تصدیق

شماره رویداد	A	B	C	S	احتمال رویداد
۱	۰	۰	۰	۰	
۲	۰	۰	۱	۰	
۳	۰	۱	۰	۰	
۴	۰	۱	۱	۱	$(1-P_A)P_BP_C$
۵	۱	۰	۰	۰	
۶	۱	۰	۱	۱	$P_A(1-P_B)P_C$

۷	۱	۱	۰	۰	
۸	۱	۱	۱	۱	$P_A P_B P_C$

قابلیت اطمینان سیستم با جمع مقادیر احتمال رویدادهای منجر به موفقیت سیستم به‌دست می‌آید.

$$R=(1-P_A)P_B P_C+P_A(1-P_B)P_C+P_A P_B P_C=P_C(P_A+P_B-P_A P_B) \quad (۱۲۹-۳)$$

درصورتی‌که نوشتن عبارت بولی برای سیستم ممکن باشد، نیازی به جدول تصدیق نیست. آنچه نیاز است این است که عبارت بولی باید به عبارت کمینهٔ خود برسد. آنگاه مستقیماً از آن عبارت، احتمال عملکرد به دست می‌آید.

۳-۹-۱-۶-۲- روش مجموعهٔ برشی و مجموعهٔ موفقیت

این یک روش مؤثر برای محاسبهٔ قابلیت اطمینان یک سیستم است. در این روش از برنامه‌های کامپیوتری نیز می‌توان استفاده کرد.

- مجموعهٔ برشی: گروهی از اجزا یا واحدهایی که خرابی آنها منجر به خرابی سیستم می‌شود. تعداد کمینهٔ این واحدها مجموعهٔ برشی کمینه را شکل می‌دهد.
- مجموعهٔ موفقیت: مجموعه‌ای از اجزایی که عمل‌کردن آنها منجر به موفقیت سیستم می‌شود.

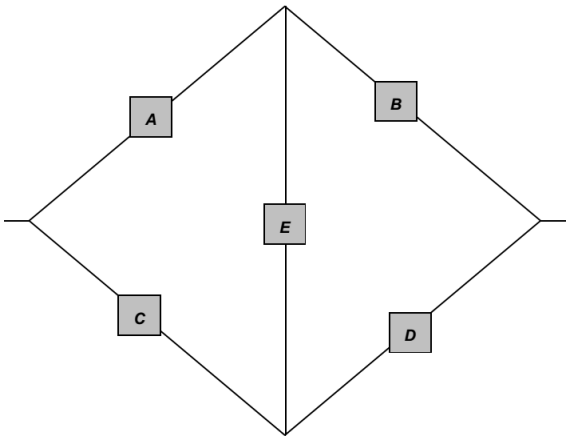
برای محاسبهٔ قابلیت اطمینان باید یکی از مجموعه‌های فوق به‌دست آیند. به عنوان مثال، در یک سیستم $T_1,T_2,...,T_n$ مجموعه‌های موفقیت کمینه هستند، در این صورت قابلیت اطمینان سیستم به صورت زیر محاسبه می‌شود:

$$R_s=P(T_1\cup T_2\cup...\cup T_n) \quad (۱۳۰-۳)$$

و اگر مجموعه‌های برشی کمینه به صورت $C_1,C_2,...,C_k$ باشند، آنگاه قابلیت اطمینان سیستم به صورت زیر است:

$$R_s=1-P(C_1\cup C_2\cup...\cup C_n) \quad (۱۳۱-۳)$$

به عنوان مثال، برای شبکهٔ پلِ شکل ۴۳ قابلیت اطمینان به روش مجموعه‌های برشی و موفقیت قابل محاسبه است.



شکل ۴۳: مثال نمونه برای روش مجموعه‌های برشی و موفقیت

مجموعه‌های موفقیت کمینه برای این مثال عبارتند از:

$$T_1=(A,B),T_2=(C,D),T_3=(A,E,D),T_4=(C,E,B) \quad (۱۳۲-۳)$$

مجموعه‌های برشی کمینه عبارتند از:

$$C_1=(A,B),C_2=(C,D),C_3=(A,E,D),C_4=(C,E,B) \quad (۱۳۳-۳)$$

احتمال موفقیت‌ها به صورت زیر است:

$$P(T_1)=P_AP_B,T_2=P_CP_D,T_3=P_AP_EP_D,T_4=P_CP_EP_B \quad (۱۳۴-۳)$$

قابلیت اطمینان به صورت زیر به دست می‌آید.

$$\begin{aligned}R_s &= P(T_1\cup T_2\cup T_3\cup T_4)\\ &= P(T_1)+P(T_2)+P(T_3)+P(T_4)\\ &-\left[P(T_1)P(T_2)+P(T_2)P(T_3)+P(T_3)P(T_4)+P(T_1)P(T_4)+P(T_1)P(T_3)+P(T_2)P(T_4)\right]\\ &+P(T_1)P(T_2)P(T_3)+P(T_1)P(T_3)P(T_4)+P(T_2)P(T_3)P(T_4)+P(T_1)P(T_2)P(T_4)\\ &-P(T_1)P(T_2)P(T_3)P(T_4)\end{aligned} \quad (۱۳۵-۳)$$

به طور مشابه روش مجموعه‌های برشی کمینه برای پیش‌بینی قابلیت اطمینان قابل استفاده است.

۳-۹-۱-۶-۳- روش کران‌ها

هنگامی‌که با یک سیستم بزرگ مواجه هستیم، روش‌های بولی و مجموعه‌های برشی و موفقیت ناکارامد می‌شوند. ولی اگر از یک برنامهٔ کامپیوتری برای مجموعه‌های برشی و موفقیت استفاده شود، می‌توان از روش کران‌ها استفاده کرد که روش

تغییریافتهٔ روش مجموعه‌های برشی و موفقیت است. اگر $T_1,T_2,...,T_n$ مجموعه‌های موفقیت کمینه باشند، کران بالا برای قابلیت اطمینان سیستم به صورت زیر است:

$$R_u < P(T_1)+P(T_2)+...+P(T_n) \quad (۱۳۶-۳)$$

این مقدار یک تخمین خوب برای کران بالای قابلیت اطمینان است. همچنین اگر $C_1,C_2,...,C_k$ مجموعه‌های برشی کمینه باشند، کران پایین قابلیت اطمینان سیستم به صورت زیر به دست می‌آید.

$$R_l > 1-[P(C_1)+P(C_2)+...+P(C_k)] \quad (۱۳۷-۳)$$

این یک تخمین خوب برای کران پایین قابلیت اطمینان است. قابلیت اطمینان سیستم به صورت زیر تخمین زده می‌شود.

$$R = 1-\sqrt{(1-R_u)(1-R_l)} \quad (۱۳۸-۳)$$

۳-۹-۲- مدل مارکوف

اغلب برای تحلیل قابلیت اطمینان سیستم با توجه به سادگی و سهولت کاربرد از ترکیب مدل‌ها (دیاگرام جعبه‌ای، درخت خطا و ...) استفاده می‌شود. این مدل‌ها برای سیستم‌های حاوی اجزای مستقل بسیار مناسب است. وابستگی اجزا در این مدل‌ها به صورت مؤثری لحاظ نمی‌شود. مدل‌سازی انعطاف برای سیستم‌های پیچیده با مدل مارکوف پوشش داده نمی‌شود، درحالی‌که فرایندهای تعمیر و نگهداری با این مدل انجام می‌شود. این روش هنگامی‌که نرخ‌های خرابی و تعمیر همهٔ اجزا ثابت (توزیع نمایی) باشند، کاربردی است.

در مدل‌های دو گانه یا دو حالته که پرکاربردترین آنها درخت خطا می‌باشد، برای مدل‌سازی قابلیت اطمینان سیستم‌ها، تنها دو حالت خرابی و عملکردی که به حالت صفر و یک معروف هستند در نظر گرفته می‌شود، این در حالیست که در روش‌های چند حالته همچون مارکوف، علاوه بر بکار رفتن حالت خرابی و عملکردی، سایر حالت ها همچون تعمیرپذیری و تست اجزا نیز در نظر گرفته خواهد شد. مشخص است که در روش‌های چندحالته نسبت به دوحالته (درخت خطا) بدلیل گسترده‌تر بودن تحلیل، نتایج دقیق‌تر و منطقی‌تری نیز ارائه خواهد شد ولی حجم محاسبات بالاتر خواهد بود.

زنجیره‌های مارکوف، توالی‌های متغیرهای تصادفی هستند. در این مدل متغیرهای خرابی با متغیرهای حاضر تعیین می‌شوند و تکامل حالت کنونی از پیشینه‌اش مستقل است. در واقع شاخصهٔ این متغیرها، بدونِ حافظه بودن است.

یک فرایند اتفاقی $\{X(t)|t\in T\}$ زمانی یک فرایند مارکوف است که برای هر $t_0<t_1<...<t_n<t_{n+1}$، توزیع شرطی $X(t_{n+1})$ برای مقادیر $X(t_0),X(t_1),...,X(t_n)$ تنها به $X(t_n)$ وابسته باشد و نه به مقادیر پیشین آن. مقادیری که $X(t)$ می‌تواند داشته باشد، «حالت‌ها» نامیده می‌شوند که مجموع همهٔ آنها یک «فضای حالت» را تشکیل می‌دهد که با Ω نشان داده می‌شود.

فرایندهای مارکوف براساس اینکه مقادیر T و Ω گسسته (قابل شمارش) یا پیوسته (غیرقابل شمارش) باشند، تقسیم می‌شوند. بنابراین چهار نوع از فرایندهای مارکوف براساس زمان و فضاهای حالت معین شده وجود دارد.

۳-۹-۲-۱- اصول روش فضای حالت

یک سیستم قابل تعمیر با n جزء که هر یک دارای تعداد حالت‌های محدود عملکردی و خرابی هستند را در نظر بگیرید. این سیستم دارای دو نوع حالت است:

- حالت‌های عملکردی: حالت‌هایی هستند که سیستم با وجود خرابی برخی اجزا، کار می‌کند. حالت عملکرد کامل حالتی است که هیچ جزئی خراب نباشد.
- حالت‌های خرابی: حالت‌هایی هستند که سیستم به دلیل خرابی یک یا چند جزء، قادر به انجام وظیفه خود نیست.

مراحل پیاده‌سازی مدل مارکوف شامل سه مرحله است:

- مرحله اول: لیست‌کردن و دسته‌بندی همهٔ حالت‌های سیستم به صورت حالت‌های عملکردی یا حالت‌های خرابی. اگر هر جزء دارای دو حالت ممکن (موفقیت و خرابی) باشد و اگر سیستم دارای n جزء باشد، حداکثر تعداد حالت‌ها برابر ۲^n خواهد بود. در طول عمر سیستم، حالت‌های خرابی می‌توانند بدلیل وجود خرابی‌ها ظاهر شده و با انجام تعمیرات، مرتفع شوند.
- مرحله دوم: لیست‌کردن همهٔ انتقال‌های ممکن بین حالت‌های مختلف و شناسایی علل همهٔ انتقال‌ها. به‌طورکلی علل انتقال‌ها یا خرابی یک یا چند جزء و یا تعمیرات اجزا است.
- مرحله سوم: محاسبهٔ احتمالات قرارگیری در حالت‌های مختلف طی یک بازهٔ زمانی مشخص در عمر سیستم یا محاسبهٔ مشخصات قابلیت اطمینان (مانند زمان متوسط خرابی، MTTF؛ زمان متوسط تعمیرات، MTTR؛ زمان متوسط بین خرابی‌ها، MTBF). این کار با تشکیل یک گراف حالت که در آن هر گره نشان دهندهٔ یک حالت

سیستم و هر خط یک انتقال بین دو نقطه است، انجام می‌شود. نرخ انتقال بین دو حالت به هر خط تخصیص داده می‌شود.

روش‌های مختلف تلخیص فضای حالت برای ساده‌سازی محاسبات وجود دارد که اغلب آنها از رویکرد ادغام حالت‌ها بهره می‌برند. در این رویکرد، حالت‌های یکسان ادغام شده و نرخ‌های انتقال و احتمالات معادل به‌دست می‌آیند.

۳-۹-۲-۲- تحلیل پایه

دو حالت i و j و انتقال از i به j را در نظر بگیرید. احتمال اینکه سیستم در زمان t در حالت i باشد، $P_i(t)$ و احتمال اینکه سیستم در زمان $t+\Delta t$ در حالت j باشد، $P_j(t+\Delta t)$ است. با این فرض، داریم:

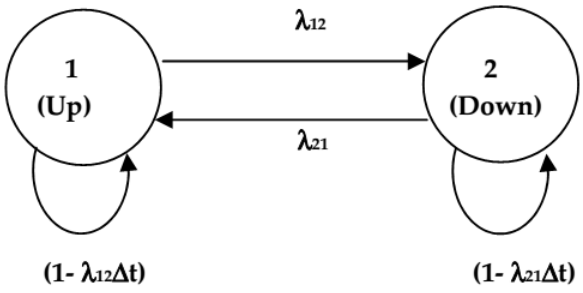
$$P_j(t+\Delta t)=\lambda_{ij}\Delta t P_i(t) \qquad (۱۳۹-۳)$$

در این رابطه، λ_{ij} نرخ انتقال از حالت i به j و $\lambda_{ij}\Delta t$ احتمال خرابی در بازهٔ Δt است. فرض می‌شود که احتمال اینکه دو یا بیش از دو انتقال به صورت همزمان رخ دهند، ناچیز است. به طور کلی داریم:

$$P_j(t+\Delta t)=\sum_{i\neq j}\lambda_{ij}\Delta t P_i(t)+\left(1-\sum_{k\neq j}\lambda_{jk}\Delta t\right)P_j(t) \qquad (۱۴۰-۳)$$

در بخش اول رابطهٔ فوق، احتمال ورود به یک حالت و در بخش دوم، احتمال ماندن در آن حالت محاسبه می‌شود.

یک سیستم تک جزئی ساده برای روشن شدن اهداف و تحلیل تفصیلی مارکوف برای ارزیابی قابلیت اطمینان در شکل ۴۴ نشان داده شده است.



شکل ۴۴: سیستم ساده تک‌جزئی

با توجه به توضیحات فوق می‌توان برای این سیستم، روابط زیر را توسعه داد:

$$P_1(t+\Delta t)=\lambda_{21}\Delta t P_2(t)+(1-\lambda_{12}\Delta t)P_1(t)\Rightarrow\frac{dP_1(t)}{dt}=\frac{P_1(t+\Delta t)-P_1(t)}{\Delta t}=\lambda_{21}P_2(t)-\lambda_{12}P_1(t)$$
$$P_1(t+\Delta t)=\lambda_{12}\Delta t P_1(t)+(1-\lambda_{21}\Delta t)P_2(t)\Rightarrow\frac{dP_2(t)}{dt}=\frac{P_2(t+\Delta t)-P_2(t)}{\Delta t}=\lambda_{12}P_1(t)-\lambda_{21}P_2(t) \quad (۱۴۱-۳)$$

روابط فوق را می‌توان به صورت زیر نوشت:

$$\lambda_{12}=\lambda,\lambda_{21}=\mu$$
$$\frac{dP_1(t)}{dt}=\mu P_2(t)-\lambda P_1(t) \quad (۱۴۲-۳)$$
$$\frac{dP_2(t)}{dt}=\lambda P_1(t)-\mu P_2(t)$$

فرم ماتریسی رابطهٔ فوق به صورت زیر است:

$$\left[\frac{dP_1(t)}{dt}\quad\frac{dP_2(t)}{dt}\right]=[P_1(t)\quad P_2(t)]\begin{bmatrix}-\lambda & \lambda\\ \mu & -\mu\end{bmatrix} \quad (۱۴۳-۳)$$
$$[\overline{P'(t)}]=[\overline{P(t)}][A]$$

در این رابطه، $[A]$ ماتریس انتقال تصادفی است. خواص ماتریس انتقال تصادفی عبارتند از:

- $[A]$ یک ماتریس مربعی با ابعاد n در n است که n تعداد حالت‌ها در مدل مارکوف است.
- درایهٔ a_{ij} نرخ انتقال از حالت i به حالت j است ($i\neq j$).
- درایهٔ a_{ii} منفی مجموع نرخ‌های انتقال از حالت i به همهٔ سایر حالت‌ها است.

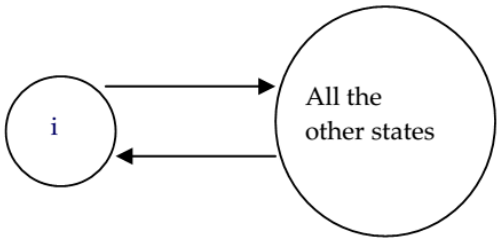
یک فرایند مارکوف زمانی همگن است که نرخ‌های خرابی و تعمیر ثابت باشند. هنگامی‌که فرایند همگن است، درایه‌های ماتریس A ثابت هستند. علاوه‌براین، مجموع درایه‌های هر ردیف برابر صفر است. بنابراین، A یک ماتریس یکّه است، یعنی دترمینان آن برابر صفر است.

هنگامی‌که توزیع اولیه $P_i(0)$ معلوم باشد، حل صحیح معادلات دیفرانسیل مارکوف با استفاده از روش‌های تبدیل لاپلاس، گسسته‌سازی یا مقادیر ویژهٔ ماتریس A به دست می‌آید. برای همهٔ فرایندهای محاسباتی می‌توان فرض کرد که سیستم ابتدا در حالت سالم قرار دارد و همهٔ اجزای آن درست عمل می‌کنند. بنابراین در لحظهٔ t=0 احتمال سیستم به صورت $P_1(0)=1$ و $P_2(0)=0$ است. با کمک تبدیل لاپلاس، مقادیر $P_i(t)$ به صورت زیر به دست می‌آید.

$$P_1(t) = \frac{\mu}{\mu+\lambda} + \frac{\lambda}{\mu+\lambda} e^{-(\mu+\lambda)t}$$
$$P_1(t) = \frac{\lambda}{\mu+\lambda} + \frac{\lambda}{\mu+\lambda} e^{-(\mu+\lambda)t} \quad (۱۴۴-۳)$$

۳-۹-۲-۳- فرکانس‌های حالت و بازه‌های زمانی

f_i فرکانس مواجهه با حالت i، به صورت تعداد مورد انتظار قرار گیری در (یا رسیدن به، یا خروج از) حالت i به ازای واحد زمان که در طول یک بازهٔ بلند محاسبه می‌شود. مفهوم فرکانس با رفتار بلند مدت فرایند تشریح کنندهٔ سیستم مرتبط است. به منظور ارتباط دادن فرکانس، احتمال و مدت زمان میانگین یک حالت سیستم، فرض می‌شود تاریخچهٔ سیستم حاوی دو دوره باشد: در حالت i بودن و خارج حالت i بودن. دیاگرام فضای حالت فرایند دو حالتی در شکل ۴۵ نشان داده شده است.



شکل ۴۵: دیاگرام فضای حالت فرایند دوحالتی

- T_i زمان میانگین بودن در حالت i،
- $T_{i'}$ زمان میانگین بودن در حالت‌های غیر i،
- $T_{ci} = T_i + T_{i'}$ زمان میانگین سیکل،
- $f_i = 1/T_{ci}$ فرکانس حالت است.

$$f_i T_i = \frac{T_i}{T_{ci}}, P_i = \frac{T_i}{T_{ci}} \Rightarrow f_i = \frac{P_i}{T_i}$$

- f_{ij} فرکانس انتقال از حالت i به حالت j است که به صورت تعداد دفعات مورد انتظارِ انتقال مستقیم از حالت i به حالت j به ازای واحد زمان تعریف می‌شود.

$$f_{ij} = \lim_{\Delta t \to 0} \frac{1}{\Delta t} P\left[(X(t+\Delta t) = j) \cap (X(t) = i)\right]$$
$$= \lim_{\Delta t \to 0} \frac{1}{\Delta t} P\left[X(t+\Delta t) = j / (X(t) = i)\right] P\left[X(t) = i\right] = \lambda_{ij} P_i \quad (۱۴۵-۳)$$

بنابراین، نرخ انتقال λ_{ij} ضرورتاً یک فرکانس شرطی است که شرایط بودن سیستم در حالت i را نشان می‌دهد. با توجه به تعریف f_i و f_{ij} ، خواهیم داشت:

$$f_i = \sum_{j \neq i} f_{ij} \Rightarrow f_i = P_i \sum_{j \neq i} \lambda_{ij} \qquad (۱۴۶-۳)$$

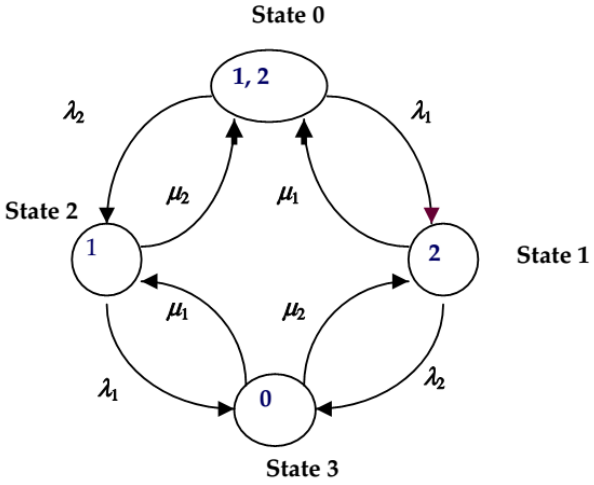
بنابراین می‌توان نوشت:

$$T_i = \frac{1}{\sum_{j \neq i} \lambda_{ij}} \qquad (۱۴۷-۳)$$

به عبارت دیگر، مدت زمانِ میانگینِ بودن در هر حالت برابر معکوس جمع نرخ‌های خروج از آن حالت است.

۳-۹-۲-۴- سیستم دوجزئی قابل تعمیر

یک سیستم حاوی دوجزء را در نظر بگیرید. در حالت صفر هر دو جزء کار می‌کنند. هنگامی‌که جزء ۱ خراب می‌شود، انتقال به حالت ۱ رخ می‌دهد. اگر در این حالت تعمیر شود، به حالت ۱ باز می‌گردد. خرابی در حالت ۱ منجر به تغییر حالت سیستم به حالت ۳ می‌شود که در آن هر دو جزء خراب هستند. مدل مارکوف در شکل ۴۶ نشان داده شده است.



شکل ۴۶: مدل مارکوف برای سیستم دوجزئی

درحالتی‌که دو جزء به صورت سری در سیستم قرار دارند، قابلیت اطمینان سیستم برابر احتمال حالتی است که هر دو جزء کار می‌کنند، یعنی حالت صفر. برای سیستم موازی، قابلیت اطمینان برابر مجموع احتمال همهٔ حالت‌هایی است که در آنها حداقل یک سیستم کار می‌کند.

- برای اجزای سری: $R_s = P_0$
- برای اجزای موازی: $R_s = P_0 + P_1 + P_2$

برای این سیستم دوجزئی، احتمالات حالت پایا به صورت زیر است:

$$
\begin{aligned}
P_0 &= \frac{\mu_1\mu_2}{(\lambda_1+\mu_1)(\lambda_2+\mu_2)},\\
P_1 &= \frac{\lambda_1\mu_2}{(\lambda_1+\mu_1)(\lambda_2+\mu_2)},\\
P_2 &= \frac{\mu_1\lambda_2}{(\lambda_1+\mu_1)(\lambda_2+\mu_2)},\\
P_3 &= \frac{\lambda_1\lambda_2}{(\lambda_1+\mu_1)(\lambda_2+\mu_2)},\\
T_0 &= \frac{1}{(\lambda_1+\lambda_2)} \Rightarrow f_0 = \frac{P_0}{T_0} = \frac{\mu_1\mu_2(\lambda_1+\lambda_2)}{(\lambda_1+\mu_1)(\lambda_2+\mu_2)}
\end{aligned}
\qquad (۱۴۸-۳)
$$

f_i احتمالِ بودن در یک حالت برابر است با احتمالِ بودن در آن حالت × مجموع نرخ خروج از آن حالت؛

یا برابر است با احتمال نبودن در آن حالت × مجموعه نرخ ورود به آن حالت.

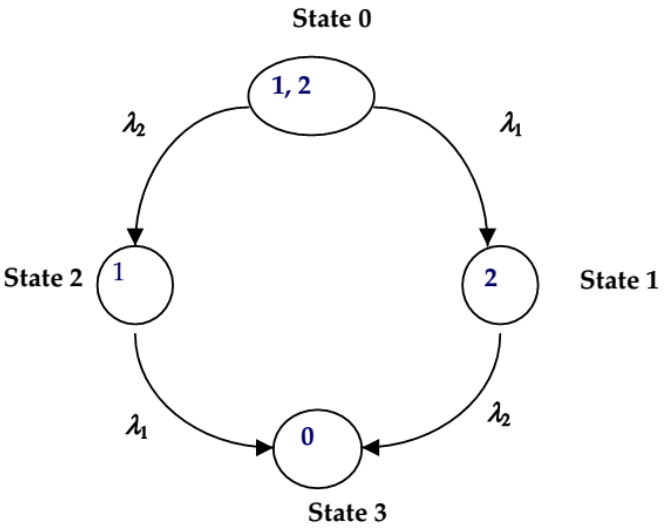
اگر دو حالت یکسان x و y در هم ادغام شوند، روابط زیر برای به‌دست آوردن نرخ‌های انتقال معادل بین حالت‌های ادغام شده و سایر حالت‌ها (حالت i) از فضای حالت به کار می‌رود.

$$
\begin{aligned}
P_z &= P_x + P_y\\
\lambda_{iz} &= \lambda_{ix} + \lambda_{iy}\\
\lambda_{zi} &= \frac{\lambda_{xi}P_x + \lambda_{yi}P_y}{P_x + P_y}
\end{aligned}
\qquad (۱۴۹-۳)
$$

انتقال بین دو حالتِ ادغام شده می‌تواند از روابط زیر به دست آید:

$$
\begin{aligned}
\lambda_{IJ} &= \frac{\sum_{i\in I}P_i\sum_{j\in J}\lambda_{ij}}{\sum_{i\in I}P_i}\\
\lambda_{JI} &= \frac{\sum_{j\in J}P_j\sum_{i\in I}\lambda_{ji}}{\sum_{j\in J}P_j}
\end{aligned}
\qquad (۱۵۰-۳)
$$

این شرایط با یک سیستم دوجزئی غیرقابل تعمیر (شکل ۴۷) روشن‌تر می‌شود.

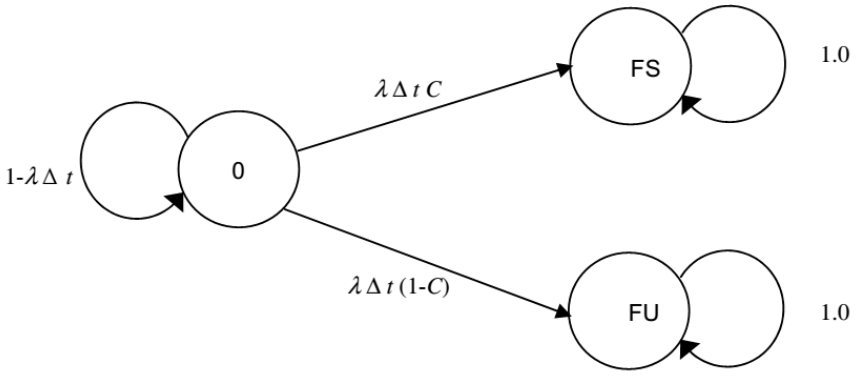


شکل ۴۷: مدل مارکوف برای سیستم دوجزئی غیرقابل تعمیر

۳-۹-۲-۵- مدل‌سازی ایمنی

ایمنی و قابلیت اطمینان هم از لحاظ ماهیّتی و هم از لحاظ ریاضی به هم مرتبط هستند. یک مسألهٔ ایمنی زمانی ایجاد می‌شود که یک خرابی بحرانی واقع شود که در تحلیلِ قابلیت اطمینان، به عنوان مثال با تحلیل خرابی و اثرات آن مورد بررسی قرار می‌گیرد.

احتمال اینکه یک خرابی به درستی شناسایی و بررسی شود، ضریب پوشش خطا (C) نامیده می‌شود. به‌کارگیری ضریب پوشش برای یک خرابی جزء در مدل مارکوف شکل ۴۸ نشان داده شده است. در این شکل، اگر یک خرابی شناسایی شود، حالت خرابی ایمن (FS) و در غیر این صورت حالت خرابی غیرایمن (FU) خواهد بود. در شکل، پوشش خطا بر حسب قابلیت اطمینان رسم شده است.



شکل ۴۸: مدل مارکوف برای سیستم ساده با مدل پوشش خطا

$$
\begin{aligned}
&P_0(t+\Delta t) = (1-\lambda\Delta t)P_0(t),\\
&P_{FS}(t+\Delta t) = \lambda\Delta t C P_0(t) + P_{FS}(t),\\
&P_{FU}(t+\Delta t) = \lambda\Delta t(1-C)P_0(t) + P_{FS}(t),\\
&R(t) = P_0(t),\\
&S(t) = R(t) + P_{FS}(t),\\
&\frac{dP_0(t)}{dt} = -\lambda P_0(t),\\
&\frac{dP_{FS}(t)}{dt} = \lambda C P_0(t),\\
&\frac{dP_{FU}(t)}{dt} = -\lambda(1-C)P_0(t).
\end{aligned}
\qquad (۱۵۱-۳)
$$

با کمک تبدیل لاپلاس و با فرض $P_{FS}(0)=0$، $P_{FU}(0)=0$ و $P_0(0)=1$ روابط زیر به دست می‌آید:

$$
\begin{aligned}
&P_0(s) = \frac{1}{(s+\lambda)},\\
&P_{FS}(s) = \frac{\lambda C}{s(s+\lambda)} = \frac{C}{s} - \frac{C}{s+\lambda},\\
&P_{FU}(s) = \frac{\lambda(1-C)}{s(s+\lambda)} = \frac{(1-C)}{s} - \frac{(1-C)}{s+\lambda}.
\end{aligned}
\qquad (۱۵۲-۳)
$$

حال، احتمالِ بودن در حالت صفر بر حسب زمان به صورت زیر به دست می‌آید:

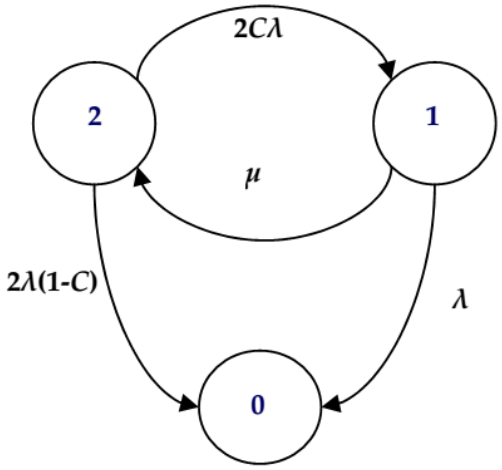
$$
\begin{aligned}
&P_0(t) = e^{-\lambda t},\\
&P_{FS}(t) = C(1-e^{-\lambda t}),\\
&P_{FU}(t) = (1-C)(1-e^{-\lambda t}),\\
&S(t) = P_0(t) + P_{FS}(t) = C + (1-C)e^{-\lambda t}.
\end{aligned}
\qquad (۱۵۳-۳)
$$

مقادیر صفر و یک برای ضریب پوشش خطا و احتمال موفقیت سیستم به صورت زیر است:

$$S(t) = C + (1-C)R(t) \geq R(t),$$
$$C = 1 \Rightarrow S(t) = 1,$$
$$C = 0 \Rightarrow S(t) = e^{-\lambda t} = R(t). \quad (۱۵۴-۳)$$

۳-۹-۲-۶- پوشش غیرکامل – سیستم با دو جزء موازی

مدل مارکوف شامل پوشش برای یک سیستم دوجزئی موازی در شکل ۴۹ نشان داده شده است.



شکل ۴۹: مدل مارکوف برای سیستم دوجزئی موازی با پوشش غیرکامل

با فرض اینکه حالت اولیه حالت ۲ است، معادلات دیفرانسیل این سیستم به صورت زیر به دست می‌آید.

$$P_2(0) = 1, P_0(0) = P_1(0) = 0.$$
$$\frac{dP_2(t)}{dt} = -2\lambda C P_2(t) - 2\lambda(1-C)P_2(t) + \mu P_1(t),$$
$$\frac{dP_1(t)}{dt} = 2\lambda C P_2(t) - (\lambda + \mu)P_1(t), \quad (۱۵۵-۳)$$
$$\frac{dP_0(t)}{dt} = 2\lambda(1-C)P_2(t) + \lambda P_1(t).$$

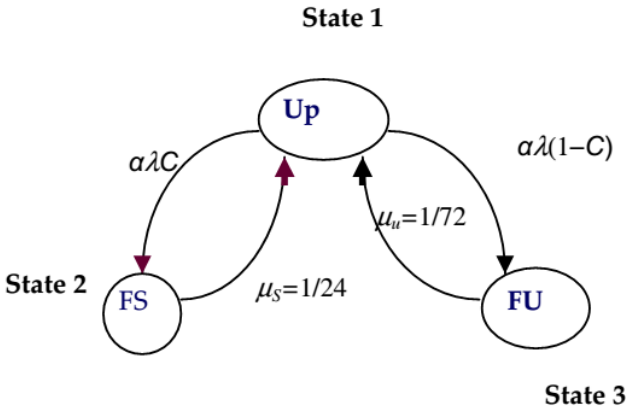
معادلات فوق برای حصول احتمال حالت‌های مختلف حل می‌شوند. قابلیت اطمینان جمع احتمالات حالت‌های ۱ و ۲ است.

زمان میانگین تا خرابی به صورت زیر به دست می‌آید.

$$MTTF = \int_0^\infty R(t)dt = \frac{\lambda(1+2C) + \mu}{2\lambda[\lambda + \mu(1-C)]} \quad (۱۵۶-۳)$$

از روابط فوق روشن است که زمان میانگین تا خرابی و قابلیت اطمینان سیستم به ضریب پوشش وابسته هستند. با افزایش ضریب پوشش، زمان میانگین تا خرابی نیز افزایش می‌یابد.

مثال: یک سیستم کامپیوتری ساده دارای نرخ خرابی λ و ضریب پوشش شناسایی خطای C است. شناسایی خطا توسط سیستم تشخیص خطا که پیوسته فعال است، انجام می‌شود. اگر این سیستم یک خطا پیدا کند، زمان مورد نیاز برای تعمیر سیستم ۲۴ ساعت است. اگر سیستم خطا را پیدا نکند، فرایند تعمیر سیستم ۷۲ ساعت طول خواهد کشید. مشکل این است که سیستمِ عیب‌یاب باعث تغییر نرخ خرابی به $\alpha\lambda$ می‌شود. به عبارت دیگر، نرخ خرابی با ضریب α افزایش می‌یابد. مقدار این ضریب چقدر است؟ مدل مارکوف این مثال در شکل ۵۰ نشان داده شده است.



شکل ۵۰: مدل مارکوف برای سیستم کامپیوتری ساده

P_1 قابلیت دسترسی حالت ۱ است. با توجه به توضیحات رابطهٔ (۳-۱۴۲) می‌توان ماتریس قابلیت دسترسی حالت‌های این مثال را به صورت زیر نوشت:

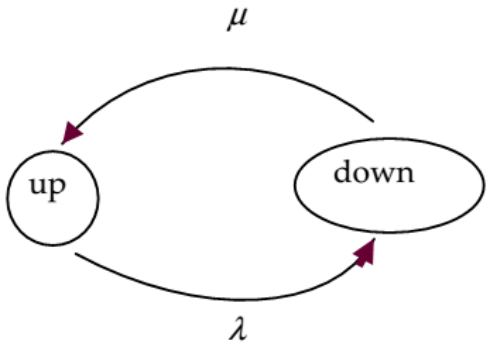
$$\dot{P}(t) = P(t)[A],$$

$$\left[\dot{P}_1(t) \quad \dot{P}_2(t) \quad \dot{P}_3(t)\right] = \left[P_1(t) \quad P_2(t) \quad P_3(t)\right] \begin{bmatrix} -\alpha\lambda & \alpha\lambda C & \alpha\lambda(1-C) \\ \frac{1}{24} & -\frac{1}{24} & 0 \\ \frac{1}{72} & 0 & -\frac{1}{72} \end{bmatrix} \qquad (۱۵۷\text{-}۳)$$

$$\begin{cases} \dot{P}(t) = 0 \\ P_1 + P_2 + P_3 = 0 \end{cases} \Rightarrow \begin{cases} P_1 = \dfrac{1}{1 + 24\alpha\lambda(3-2C)} \\ P_2 = 24P_1\alpha\lambda C \\ P_3 = 72P_1\alpha\lambda(1-C) \end{cases}$$

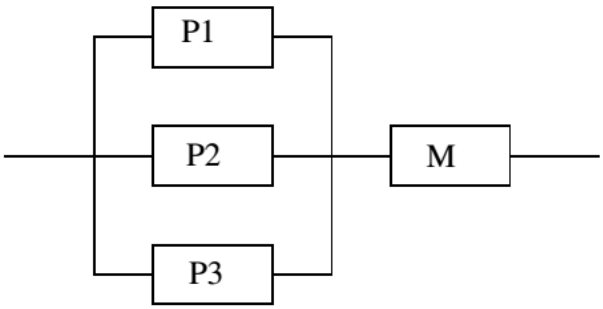
اگر پوشش خطا نباشد، سیستم به صورت شکل ۵۱ ساده می‌شود. در این صورت، نرخ تعمیر $\mu = \frac{1}{72}$ و قابلیت دسترسی برابر $\frac{\mu}{\mu+\lambda} = \frac{1}{1+72\lambda}$ است. حال می‌توان مقدار قابلیت دسترسی را برابر با مقدار P_1 در رابطهٔ (۳-۱۵۷) قرار داد.

$$\frac{1}{1+24\alpha\lambda(3-2C)} = \frac{1}{1+72\lambda} \Rightarrow \alpha = 2.7272. \qquad (۳-۱۵۸)$$



شکل ۵۱: مدل مارکوف برای یک سیستم کامپیوتری بدون سیستم تشخیص خطا

مثال: مدل مارکوف یک سیستم چهارجزئی که دیاگرام جعبه‌ای آن در شکل نشان داده شده است. P_1، P_2 و P_3 سه پردازنده مشابه هستند و M یک تراشهٔ حافظه است. فرض این است که اجزا مستقل و غیرقابل تعمیر هستند. نرخ خرابی پردازنده‌ها λ_p و نرخ خرابی حافظه λ_m است.

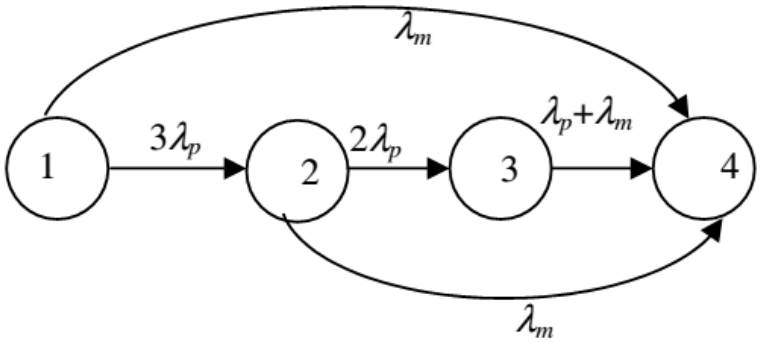


شکل ۵۲: دیاگرام جعبه‌ای یک سیستم چهارجزئی

اگر یک دیاگرام فضای حالت کامل رسم شود، 2^4 حالت خواهد داشت. با استفاده از ادغام، یک دیاگرام ساده‌شده (شکل ۵۳) به دست می‌آید.

- حالت ۱: همهٔ اجزا کار می‌کنند،

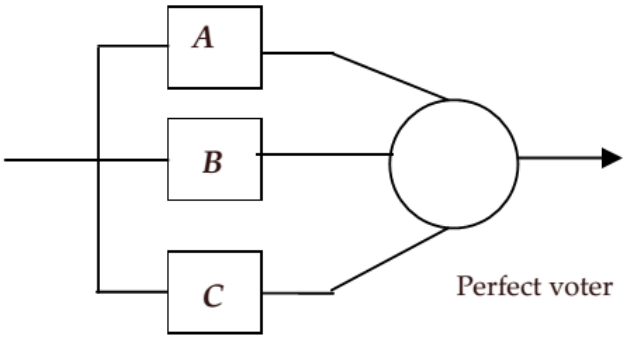
- حالت ۲: یکی از پردازنده‌ها خراب است،
- حالت ۳: دو پردازنده خراب است.
- حالت ۴: سه پردازنده یا حافظه یا هردو خراب است.



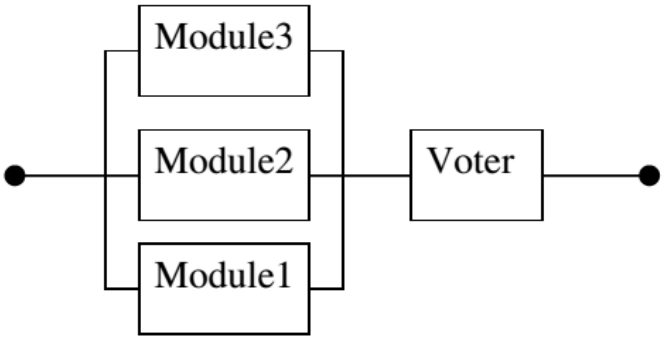
شکل ۵۳: مدل مارکوف برای سیستم چهارجزئی

۳-۹-۲-۷- مدل‌سازی سیستم‌های افزونهٔ مقاوم در برابر خرابی

مشهورترینِ این سیستم‌ها، سیستم افزونهٔ سه‌گانه است که باید حداقل دو جزء از سه جزء سالم باشند. هر سه جزء افزونه یک وظیفه دارند و جزء انتخاب‌گر، خروجی صحیح را از سه خروجی افزونه انتخاب می‌کند. تا زمانی که دو جزء از اجزای افزونه به درستی کار می‌کنند و جزء انتخاب‌گر سالم باشد، سیستم به درستی کار می‌کند.

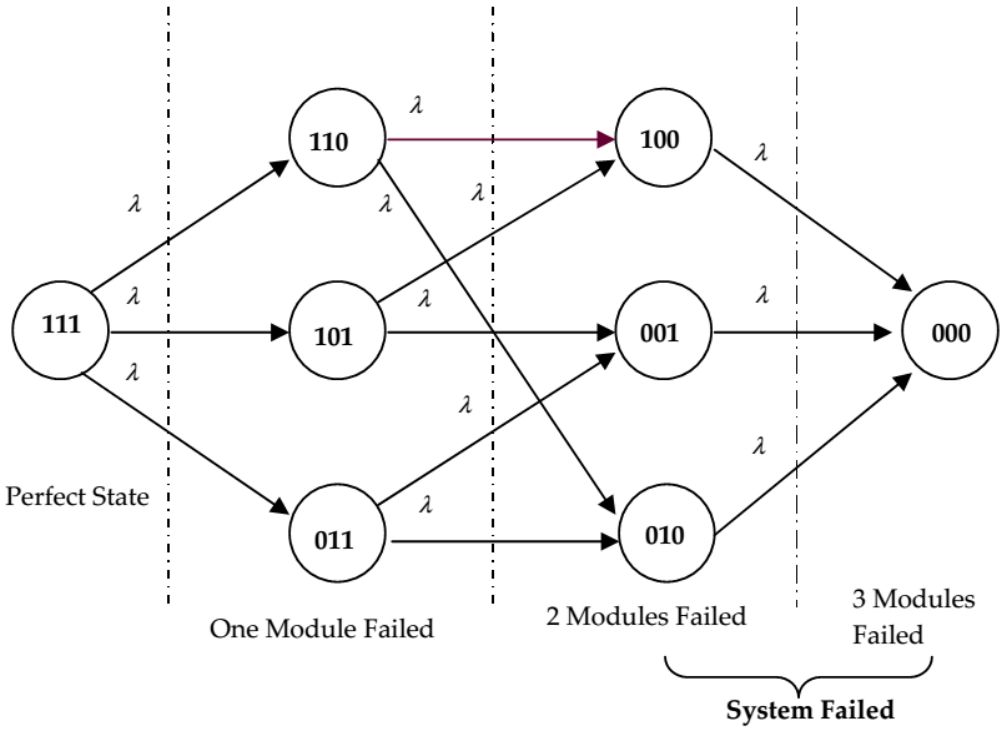


شکل ۵۴: چیدمان سیستم افزونهٔ سه‌گانه

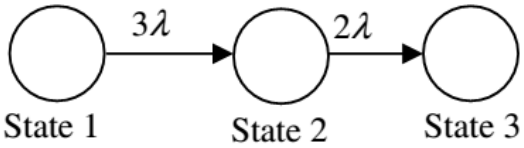


شکل ۵۵: دیاگرام جعبه‌ای یک سیستم افزونهٔ سه‌گانه

دیاگرام فضای حالت مفصّل یک سیستم افزونهٔ سه‌گانه در شکل ۵۶ نشان داده شده است. نرخ‌های خرابی هر سه جزء برابر λ است. در حالت ۱۱۱ اجزای A، B و C کار می‌کنند. در حالت ۱۰۰ جزء A کار می‌کند ولی اجزای B و C کار نمی‌کنند. سایر حالت‌ها به همین ترتیب هستند. با ترکیب حالت‌های یکسان، فضای حالت می‌تواند خلاصه شود. مدل مارکوف خلاصه شده در شکل ۵۷ نشان داده شده است. در حالت ۱، همهٔ اجزا کار می‌کنند. خرابی هر یک از سه جزء یک انتقال از حالت اولیه به حالت ۲ است که در آن یک جزء خراب و دو جزء سالم هستند. هر خرابی در حالت ۲ منجر به حالت ۳ می‌شود که حالت خراب سیستم است. در اینجا فرض می‌شود که جزء انتخاب‌گر به طور کامل قابل اطمینان است.



شکل ۵۶: مدل مارکوف سیستم افزونهٔ سه‌گانه

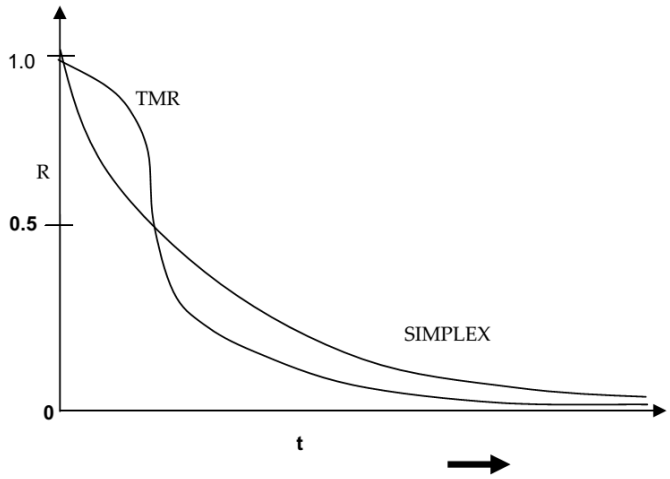


شکل ۵۷: مدل ساده شدهٔ مارکوف سیستم افزونهٔ سه‌گانه

با انجام تحلیل مارکوف این سیستم، روابط زیر به دست می‌آید:

$$R_{TMR}(t) = 3e^{-2\lambda t} - 2e^{-3\lambda t}$$
$$MTTF = \int_0^\infty (3e^{-2\lambda t} - 2e^{-3\lambda t})dt = \frac{5}{6}\lambda \qquad (۱۵۹-۳)$$

با وجود اینکه افزونگی سه‌گانه یک روش افزونهٔ مهم در طراحی سیستم‌های دیجیتال است، یک عیب مهم این روش این است که در مقایسه با سیستم تک جزئی ساده، قابلیت اطمینان بالاتر تنها در بازهٔ زمانی کوتاه مدت برقرار است. به عبارت دیگر افزونگی‌های سه‌گانه برای شرایطی که زمان‌های مأموریت کوتاه است، بسیار مناسب است (شکل ۵۸).



شکل ۵۸: منحنی قابلیت اطمینان سیستم افزونهٔ سه‌گانه در مقایسه با سیستم ساده بر حسب زمان

۴- ابزارهای اصلی تحلیل ایمنی احتمالاتی

۴-۱- درخت خطا

درخت خطا یک نمایش گرافیکی از یک عبارت بولی می‌باشد که با استفاده از قوانین جبر بولی قابل تبدیل به فرم مجموعه‌های برشی کمینه می‌باشد. هدف از تحلیل درخت خطا، بدست آوردن مجموعه‌های برشی کمینهٔ درخت خطا و محاسبهٔ احتمال وقوع رویداد رأس آن می‌باشد. در این بخش، ابتدا عناصر اصلی تشکیل دهنده درخت خطا شامل رویدادهای پایه، گیت‌های منطقی و رویدادهای مختلف، معرفی می‌شوند، سپس فرایند تحلیل درخت خطا شامل بدست آوردن مجموعه‌های برشی کمینه و محاسبهٔ احتمال وقوع رویداد رأس تشریح خواهد شد.

۴-۱-۱- مفاهیم پایهٔ تحلیل درخت خطا

این بخش حاوی مروری کلی بر مفاهیم و تعاریف اصلی در تحلیل درخت خطا می‌باشد. هر درخت خطا دارای یک رویداد رأس و تعدادی رویداد میانی و پایه می‌باشد که ارتباط بین آنها توسط گیت‌های منطقی نمایش داده می‌شود. این ارتباط، راه‌های مختلفی که وقوع رویدادهای پایه منجر به وقوع رویداد رأس درخت خطا خواهد شد را بیان می‌کنند. هر کدام از مفاهیم رویداد رأس، رویداد پایه و گیت‌های منطقی در ادامه شرح داده خواهند شد.

۴-۱-۱-۱- رویداد رأس

رویداد رأسِ درخت خطا، اولین گیت آن درخت است. این گیت ورودی هیچ گیت دیگری قرار نمی‌گیرد. رویداد رأس، نشان دهندهٔ خرابی یک سیستم یا وقوع یک رویداد نامطلوب است که هدف از رسم درخت خطا، مدل‌سازی و محاسبهٔ احتمال وقوع آن می‌باشد. تحلیل درخت خطا از تعیین رویداد رأس آغاز می‌شود و سپس عواملی که به صورت مستقیم منجر به وقوع رویداد رأس می‌شوند، شناسایی می‌گردد. در گام بعدی بایستی رویدادهای منجر به وقوع رویداد رأس تعیین شوند. این رویدادها رویدادهای میانی[۱] نیز نامیده می‌شوند. این روند تا زمانی که دیگر شاخه‌های درخت خطا قابل توسعه نباشند و بتوان به هر کدام از عوامل یک احتمال وقوع نسبت داد، ادامه می‌یابد. در واقع درخت خطا از یک رویداد رأس آغاز شده و به رویدادهای پایه ختم می‌شود.

[۱] - Intermediate Event

۴-۱-۱-۲- رویدادهای پایه

رویدادهای پایه در پایین‌ترین سطحِ یک درخت خطا قرار می‌گیرند به نحوی که درخت خطا پس از آنها قابل توسعه و تقسیم به رویدادهای جزئی‌تر نیست. در تحلیل درخت خطا، به متغیر ورودی به درخت خطا، رویداد پایه می‌گویند. ورودی‌های تحلیل درخت خطا، احتمال خرابی تجهیزات یک سیستم می‌باشند. بنابراین، عددی بین صفر و یک به آنها اختصاص می‌یابد. این مهم‌ترین و اصلی‌ترین ویژگی ورودی‌های درخت خطا و متغیرهای احتمالاتی می‌باشد. سه نوع رویداد پایه یک درخت خطا قابل استفاده است که عبارتند از: رویداد پایه، رویداد توسعه نیافته[۱] و کلید منطقی یا رویداد House.

۴-۱-۱-۲-۱- رویداد پایه

این رویداد معمولاً با یک علامت دایره نشان داده می‌شود و در پایین‌تر سطح درخت خطا قرار می‌گیرد.

۴-۱-۱-۲-۲- رویداد توسعه نیافته

این رویداد که معمولاً با علامت لوزی نشان داده می‌شود، برای نشان دادن شاخه‌هایی از درخت خطا که در مدل‌سازی بسط داده نشده‌اند، به‌کار می‌رود.

۴-۱-۱-۲-۳- کلید منطقی یا رویداد House

این رویداد، معمولاً به صورت یک پنج‌ضلعی نشان داده می‌شود و تنها سه حالت را به خود اختصاص می‌دهد. این سه حالت عبارتند از: False (F) یعنی این رویداد اتفاق نمی‌افتد، True (T) یعنی با احتمال ۱ روی می‌دهد و Ignored (I) یعنی در تحلیل درخت خطا در نظر گرفته نشود. همانطور که از ظاهر امر پیداست، رویداد Ignored هیچ تأثیری در درخت خطا ندارد و صرفاً بدین جهت رسم می‌شود که بعداً بتوان حالت منطقی آن را به یکی از حالت‌های TRUE یا FALSE تغییر داد تا تأثیر آن بررسی شود و نیازی به تشکیل ورودی جدیدی نباشد. همواره رویدادهای پایه یک احتمال وقوع دارند که احتمال اتفاق افتادن آن رویداد را مشخص می‌کند؛ ولی در کلیدهای منطقی، این احتمال همیشه یا صد درصد است (حالت TRUE) یا صفر درصد (حالت FALSE). حال این سؤال پیش می‌آید که تأثیر این احتمالات از پیش مشخص شده در درخت خطا چیست؟ اگر یک گیت OR در ورودی خود کلید منطقی TRUE داشته باشد، به این معنی است که چون احتمال رویداد آن گیت برابر با حاصل‌جمع احتمالات رویداد ورودی‌هایش است و یکی از آن ورودی‌ها کلید منطقی TRUE است که احتمال وقوعش صد درصد است، پس آن گیت، فارغ از احتمال رویداد سایر ورودی‌هایش، همیشه اتفاق می‌افتد. لذا می‌توان گیت مفروض را پیش از انجام محاسبات کمّی و در مرحلهٔ کیفی با احتمال وقوع صد درصد همیشه رخ‌داده فرض کرد و دیگر در

[۱] - Undeveloped Event

زمرهٔ محاسبات احتمالاتی نمی‌گنجد. اگر این گیت OR یک کلید منطقی ورودی با حالت FALSE داشته باشد، یعنی احتمال وقوعش صفر درصد باشد، نمی‌توان نتیجه گرفت که گیت نیز رخ نمی‌دهد، زیرا هنوز احتمال رخداد سایر ورودی‌هایش مشخص نیست. در مورد گیت‌های AND ماجرا به صورتی دیگر است؛ اگر یک گیت AND یک رویداد کلید منطقی با ورودی TRUE داشته باشد، نمی‌توان نتیجه گرفت که خود گیت روی می‌دهد یا خیر. تنها در زمانی می‌توان نتیجه قطعی گرفت که تمامی ورودی‌های آن TRUE باشند، آنگاه خود گیت نیز TRUE می‌شود. اما اگر یک گیت AND ورودی FALSE داشته باشد، آن گیت AND، فارغ از سایر ورودی‌هایش، هرگز اتفاق نخواهد افتاد.

۴-۱-۱-۳- گیت‌های منطقی

روابط بین رویدادهای پایه و رویداد رأس درخت خطا، توسط گیت‌های منطقی ایجاد می‌شود. گیت‌های منطقی پایه در تحلیل درخت خطا، گیت‌های AND و OR می‌باشند و سایر گیت‌ها را در نهایت می‌توان به گیت‌های AND و OR تبدیل نمود. در ادامه گیت‌های منطقی قابل استفاده در یک درخت خطا معرفی می‌شوند.

۴-۱-۱-۳-۱- گیت AND

وقوع همزمان تمامی ورودی‌های به این گیت منجر به وقوع خروجی آن می‌شود. به زبان مجموعه‌ها، خروجی گیت اشتراک بین تمام ورودی‌های به گیت می‌باشد.

۴-۱-۱-۳-۲- گیت OR

وقوع هرکدام از ورودی‌های به این گیت منجر به وقوع خروجی آن می‌شود. به زبان مجموعه‌ها، خروجی گیت اجتماع ورودی‌های به گیت می‌باشد.

۴-۱-۱-۳-۳- گیت N/M

وقوع N ورودی از M ورودی گیت منجر به وقوع خروجی آن می‌شود. به عنوان مثال، در یک گیت 2/3، وقوع هر ترکیب دوتایی از سه ورودی گیت منجر به وقوع خروجی آن خواهد شد.

۴-۱-۱-۳-۴- گیت انتقال

این گیت که به صورت یک مثلث رو به بالا نشان داده می‌شود، نیاز به منطق خاصی برای وقوع خروجی خود ندارد و هدف از آن فقط ساده کردن مدل‌سازی برای تحلیل‌گر می‌باشد. بدین صورت که برای جلوگیری از بزرگ‌تر شدن و پیچیدگی در درخت خطای اصلی، بخشی از آن را می‌تواند در درخت خطای دیگری مدل‌سازی کرد و این دو درخت را از طریق یک گیت

انتقال به هم وصل نمود. در هنگام تحلیل این گیت، درخت خطای مربوط به آن به درخت اصلی متصل شده و تحلیل انجام می‌گیرد.

۴-۱-۱-۳-۵- گیت NAND

این گیت از لحاظ منطقی متمم گیت AND می‌باشد و خروجی آن درصورتی روی می‌دهد که هرکدام از ورودی‌های گیت اتفاق نیفتند. این گیت را می‌توان با یک گیت OR که تمام ورودی‌های آن منفی (متمم) شده‌اند، مدل‌سازی کرد.

۴-۱-۱-۳-۶- گیت NOR

این گیت نیز از لحاظ منطقی متمم گیت OR می‌باشد و خروجی آن درصورتی روی می‌دهد که هیچکدام از ورودی‌های گیت اتفاق نیفتند. معادل این گیت، یک گیت AND است که تمام ورودی‌های آن منفی (متمم) شده‌اند.

۴-۱-۱-۳-۷- گیت XOR

این گیت مشابه گیت OR است با این تفاوت که وقوع تنها یکی از ورودی‌های به این گیت منجر به وقوع خروجی آن می‌شود.

۴-۱-۲- تحلیل مجموعهٔ برشی کمینه

مجموعهٔ برشی به ترکیبی از رویدادهای پایه در یک درخت خطا اطلاق می‌شود که وقوع همزمان رویدادهای آن مجموعه منجر به وقوع رویداد رأس درخت خواهد شد. تعدادی از این مجموعه‌های برشی با حذف چند رویداد پایه از آن، هنوز هم ممکن است منجر به وقوع رویداد رأس شوند. این مسأله نشان دهنده این است که زیرمجموعه‌ای از آن مجموعه برشی وجود دارد که آن هم منجر به وقوع رویداد رأس می‌شود. در نتیجه، بر اساس قوانین جبر بولی، مجموعهٔ اصلی را باید خلاصه کرده و زیرمجموعه آن را باید در نظر گرفت. به این مجموعه‌های برشی که هیچکدام از آنها زیرمجموعه دیگری نیست، مجموعه برشی کمینه می‌گویند.

۴-۱-۲-۱- بازآرایی درخت خطا

قبل از شروع تحلیل درخت خطا، ابتدا بازآرایی درخت خطا به منظور ساده‌ترکردن محاسبات انجام می‌شود. مراحل بازآرایی شامل پیداکردن لوپ منطقی، تبدیل گیت‌های ترکیبی (N/M) و متمم (NAND و NOR)، تحلیل کلیدهای منطقی و ادغام گیت‌های مشابه متوالی می‌باشد. در زمینهٔ بازآرایی درخت خطا محدودیت خاصی وجود ندارد و می‌توان قبل از انجام محاسبات درخت خطا به هر تعداد ممکن از روش‌های بازآرایی استفاده و ساختار درخت خطا را تا حد امکان ساده‌تر کرد.

۴-۱-۲-۱-۱- تبدیل سایر گیت‌ها به AND و OR

به طور کلی، تمامی گیت‌های منطقی را می‌توان با استفاده از یک سری روابط، به ترکیبی از گیت‌های AND و OR تبدیل کرد. دو نمونه از گیت‌های منطقی اصلی علاوه بر گیت AND و OR، گیت‌های ترکیب (N/M) و گیت‌های متمم (NAND و NOR) می‌باشند که نحوه تبدیل آنها به گیت AND و OR ارائه می‌شود.

- گیت‌های ترکیبی

یکی از مراحل بازآرایی درخت خطا تبدیل گیت‌های ترکیبی N/M به مجموعه‌ای از گیت‌های AND و OR می‌باشد. برای این کار ابتدا به جای یک گیت N از M، به تعداد جایگشت‌های Nتایی از M، گیت AND ایجاد می‌شود که ورودی این گیت‌ها نیز جایگشت‌های مختلف Nتایی از M ورودی گیت N/M می‌باشند. سپس این گیت‌های AND به یک گیت OR وارد می‌شوند، که در واقع جایگزین گیت N از M می‌باشد. تعداد ترکیب‌های Nتایی از M از رابطه (۴-۱) بدست می‌آید.

$$\binom{m}{n} = \frac{m!}{n!\,(m-n)!} \qquad (۱-۴)$$

به عنوان مثال یک گیت 2/3 را به صورت زیر در نظر بگیرید.

GATE1 2/3 INPUT 1 INPUT 2 INPUT 3

این گیت 2/3 که سه ورودی دارد به یک گیت OR تبدیل می‌شود که سه گیت AND (برابر تعداد ترکیب‌های دوتایی از سه) به آن وارد شده‌اند. ورودی‌های هر کدام از گیت‌های AND نیز یکی از ترکیب‌های دوتایی از سه ورودی گیت N/M می‌باشند.

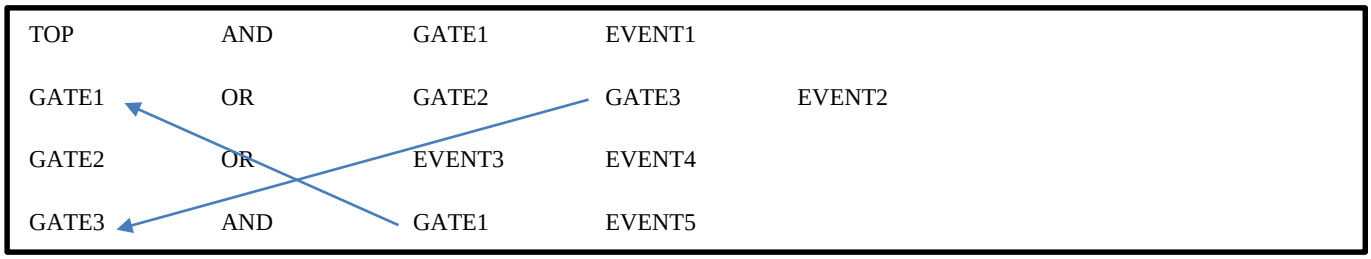
GATE1	OR	GATE 1-1	GATE 1-2	GATE 1-3
GATE 1-1	AND	INPUT 1	INPUT 2	
GATE 1-2	AND	INPUT 1	INPUT 3	
GATE 1-3	AND	INPUT 2	INPUT 3	

- گیت‌های متمم (منفی)

گیت‌های متمم نیز برای ساده‌تر شدن انجام تحلیل درخت خطا باید به گیت AND و OR تبدیل شوند. این تبدیل‌ها بر اساس قوانین دمورگان صورت می‌گیرد. برای این کار گیت NAND به OR و گیت NOR به AND تبدیل شده و ورودی‌های آن نیز همگی منفی (متمم) می‌شوند.

۴-۱-۲-۱-۲- خطای لوپ منطقی

خطای لوپ منطقی در درخت خطا درصورتی روی می‌دهد که یک گیت به‌صورت مستقیم یا غیرمستقیم دوباره به خودش رجوع داده شود. نمونه‌ای از خطای منطقی را در شکل ۵۹ مشاهده می‌کنید.



شکل ۵۹: لوپ منطقی در درخت خطا

۴-۱-۲-۱-۳- ادغام گیت‌های مشابه متوالی

یکی دیگر از مراحل بازآرایی که طی آن می‌توان درخت خطا را ساده‌تر نمود، ادغام گیت‌های مشابه متوالی است. درصورتی‌که یک گیت AND به گیت AND یا گیت OR به گیت OR وارد شود، گیت دوم که ورودی به اولی است برداشته شده و ورودی‌های آن مستقیماً به گیت بالاتر وارد می‌شود. این کار تعداد گیت‌های درخت خطا را کاهش داده و تعداد ورودی‌های به گیت‌ها را زیاد می‌کند.

۴-۱-۲-۲- بدست آوردن مجموعه‌های برشی کمینه

برای محاسبه احتمال وقوع رویداد رأس درخت خطا، ابتدا باید ساختار آن را به یک قالب منطقی معادل تبدیل نمود که بتوان با استفاده از آن، تحلیل کمّی درخت خطا را انجام داد. این قالب منطقی که برای کمّی‌سازی درخت خطا به کار می‌رود، مجموعهٔ برشی کمینه نامیده می‌شود. یک مجموعهٔ برشی، ترکیبی از رویدادهای پایه است که وقوع هم‌زمان آنها منجر به وقوع رویداد رأس درخت خطا می‌شود. مجموعهٔ برشی کمینه، کوچک‌ترین ترکیب ممکن از رویدادهای پایه است که منجر به روی دادن رویداد رأس خواهد شد. بدین معنی که با حذف هرکدام از رویدادهای پایه از یک مجموعه برشی کمینه، مجموعهٔ مورد نظر دیگر مجموعهٔ برشی نخواهد بود و منجر به وقوع رویداد رأس نمی‌شود. مجموعه‌های برشی کمینه نشان دهنده تمامی حالت‌های ممکن برای وقوع رویداد رأس ناشی از رویدادهای پایه می‌باشند.

علاوه‌بر محاسبهٔ احتمال وقوع رویداد رأس، اطلاعات قابل توجهی را تنها از ساختار مجموعه‌های برشی کمینه می‌توان به‌دست آورد. به عنوان نمونه، یک مجموعهٔ برشی کمینه که تنها دارای یک رویداد پایه است، نشان‌دهنده یک ضعف طراحی سیستم می‌باشد. این‌گونه ضعف‌ها در ساختار سیستم‌ها معمولاً با استفاده از بالا بردن درجهٔ افزونگی[۱] یا تجهیزات با قابلیت اعتماد بالاتر قابل رفع شدن است. نمونهٔ دیگر، یک مجموعهٔ برشی کمینه است که در آن چند رویداد پایه مکرّر وجود دارد. این مجموعهٔ برشی نشان‌دهندهٔ نقش و تأثیر زیاد آن رویدادهای پایه در خرابی کل سیستم می‌باشد.

۴-۱-۲-۲-۱- الگوریتم موکاس[۲]

روش‌های مختلفی برای بدست آوردن مجموعه‌های برشی یک درخت خطا وجود دارند که هر کدام دارای مزایا و معایب خاص خود می‌باشند. الگوریتم موکاس یکی از قدیمی‌ترین و پرکاربردترین روش‌ها در پیدا کردن مجموعه‌های برشی یک درخت خطا می‌باشد و بیشترین استفاده را در نرم‌افزارهای محاسباتی تحلیل درخت خطا دارد. این الگوریتم توسط فوسل و وسلی ارائه شد. در الگوریتم موکاس یک ماتریس تشکیل می‌شود که درایه‌های آن رویدادهای پایه هستند. با شروع از رویداد رأس درخت خطا، درصورت برخورد به گیت AND ورودی‌های آن را در ستون‌های جداگانه در ماتریس نوشته می‌شوند. همچنین برای هرکدام از ورودی‌های گیت OR یک سطر جدید در ماتریس ایجاد می‌شود. این روند تا انتهای درخت خطا ادامه می‌یابد. هر ردیف ماتریس حاصل در مرحلهٔ پایانی، یک مجموعهٔ برشی حاصل می‌شود. با کمینه‌سازی هر ردیف یک مجموعهٔ برشی کمینه از درخت خطای مورد نظر به دست می‌آید. تشکیل ماتریس الگوریتم موکاس شامل مراحل زیر است:

۰- اولین درایهٔ ماتریس، گیت رویداد رأس است.

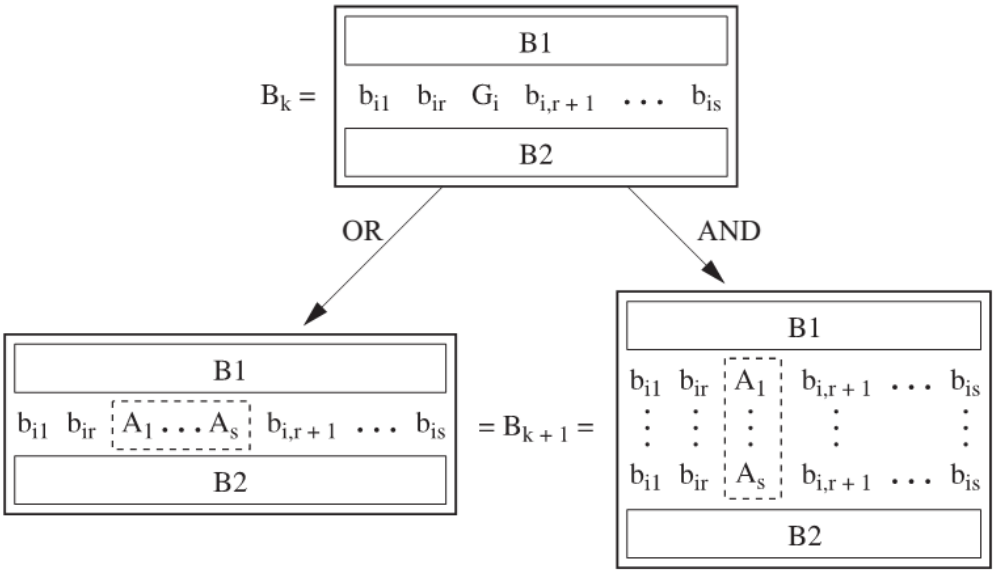
۱- گیت $G_i(A_1,...,A_s)$ که در موقعیت (i,j) از ماتریس B_k قرار دارد، در مرحلهٔ k تعیین می‌شود.

۲- اگر این گیت از نوع AND باشد، ورودی‌های آن به صورت ردیفی قرار می‌گیرند. اولین ورودی جای (i,j) را می‌گیرد و ورودی‌های بعدی در موقعیت‌های (i,j+1)، (i,j+2)، ....، (i,j+s-1) قرار می‌گیرند.

۳- اگر گیت از نوع OR باشد، ورودی‌های آن به صورت ستونی قرار می‌گیرند. اولین ورودی در جای گیت (i,j) قرار می‌گیرد و ورودی‌های بعدی در موقعیت‌های (i+1,j)، (i+2,j)، ....، (i+s,j) قرار می‌گیرند. به‌علاوه در این حالت، هر درایهٔ $b_{i,m}$ که در آن $m=1,...,s, m\neq i$ تکرار خواهد شد (شکل ۶۰). بلوک‌های B_1 و B_2 بدون تغییر باقی می‌مانند.

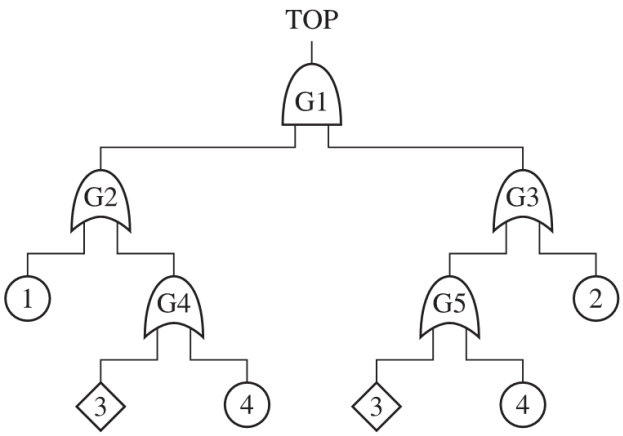
[۱] - Redundancy
[۲] - MOCUS

۴- اگر گیت دیگری وجود داشته باشد، مراحل ۱ تا آخر تکرار می‌شوند.



شکل ۶۰: تعیین درایه‌های ماتریس گیت‌های درخت خطا در الگوریتم موکاس

مثال: درخت خطای فرضی شکل ۶۱ را در نظر بگیرید. این درخت شامل یک گیت AND و چهار گیت OR است.



شکل ۶۱: درخت خطای فرضی

پیاده‌سازی الگوریتم موکاس برای درخت خطای شکل ۶۱ به صورت شکل ۶۲ است.

$$B_1 = [\underline{G_1}], \quad B_2 = [\underline{G_2}, G_3], \quad B_3 = \begin{bmatrix} 1 & \underline{G_3} \\ G_4 & G_3 \end{bmatrix},$$

$$B_4 = \begin{bmatrix} 1 & 2 \\ 1 & \underline{G_5} \\ G_4 & G_3 \end{bmatrix}, \quad B_5 = \begin{bmatrix} 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ \underline{G_4} & G_3 \end{bmatrix}, \quad B_6 = \begin{bmatrix} 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 3 & \underline{G_3} \\ 4 & G_3 \end{bmatrix},$$

$$B_7 = \begin{bmatrix} 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 3 & 2 \\ 3 & \underline{G_5} \\ 4 & \underline{G_3} \end{bmatrix}, \quad B_8 = \begin{bmatrix} 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 3 & 2 \\ 3 & 3 \\ 3 & 4 \\ 4 & 2 \\ 4 & \underline{G_5} \end{bmatrix}, \quad B_9 = \begin{bmatrix} 1 & 2 \\ 1 & 3 \\ 1 & 4 \\ 3 & 2 \\ 3 & 3 \\ 3 & 4 \\ 4 & 2 \\ 4 & 3 \\ 4 & 4 \end{bmatrix}.$$

شکل ۶۲: مراحل توسعهٔ الگوریتم موکاس برای درخت خطای فرضی شکل ۶۱

در مرحلهٔ ابتدایی، گیت رأس در درایهٔ اول ماتریس قرار می‌گیرد (B_1). در مرحلهٔ دوم ورودی‌های این گیت، با توجه به اینکه این گیت از نوع AND است، به صورت ردیفی قرار می‌گیرند (B_2). در مرحلهٔ بعد، ورودی‌های گیت‌های G_2 و G_3 به صورت ستونی قرار می‌گیرند، چراکه این دو گیت از نوع OR می‌باشند. همین روند تا اتمام گیت‌ها ادامه می‌یابد و ماتریس نهایی (B_9) حاصل می‌شود. روند توسعهٔ ماتریس موکاس برای درخت خطای شکل ۶۱ در نشان داده شده است. در این شکل، در هر مرحله زیر گیتی که در آن مرحله تکمیل می‌شود، خط کشیده شده است. ماتریس نهایی الگوریتم موکاس تنها شامل رویدادهای پایه می‌باشد. هر ردیف این ماتریس یک مجموعهٔ برشی را نشان می‌دهد.

۴-۱-۲-۲-۲- حذف مجموعه‌های برشی غیرکمینه

پس از بدست آوردن مجموعه‌های برشی درخت خطا با استفاده از الگوریتم موکاس، لازم است مجموعه‌های برشی تکراری و غیرکمینه حذف شوند. این کار با مقایسهٔ دو به دو بین مجموعه‌های برشی و استفاده از قوانین خودتوانی[۱] و جذب[۲] در جبر بولی قابل انجام است. این دو قانون جبر بولی به ترتیب در روابط (۴-۲) و (۴-۳) نمایش داده شده‌اند.

$$A + A = A \qquad (۴-۲)$$

[۱] - Idempotence
[۲] - Absorption

$$A + AB = A \quad (۳-۴)$$

با توجه به قوانین جبر بولی فوق، مجموعه‌های برشی ماتریس B_9 در شکل ۶۲ کمینه می‌شوند، به صورتی‌که درخت خطای شکل ۶۱ تنها شامل سه مجموعه برشی کمینهٔ $\{1,2\},\{3\},\{4\}$ خواهد بود.

۴-۱-۳- محاسبهٔ احتمال وقوع رویداد رأس

با داشتن مجموعه‌های برشی کمینه، احتمال رویداد رأس درخت خطا به سادگی قابل محاسبه است. برای این کار ابتدا احتمال هر مجموعهٔ برشی کمینه مطابق رابطه (۴-۴) از حاصل‌ضرب احتمال وقوع رویدادهای پایهٔ عضو مجموعهٔ برشی کمینه به‌دست می‌آید.

$$C_i = \prod_{j=1}^{n} P_j \quad (۴-۴)$$

اکنون که مجموعه‌های برشی کمینه و احتمال وقوع هر کدام از آنها محاسبه شده است، می‌توان احتمال رویداد رأس درخت خطا را به دو روش تقریب رویداد نادر (REA) و باند بالای مجموعهٔ برشی کمینه (MCUB) محاسبه کرد. مقدار تقریبی احتمال رویداد رأس درخت خطا با استفاده از تقریب REA مطابق رابطه (۴-۵) محاسبه می‌شود. با توجه به این رابطه مشاهده می‌شود که فرض اصلی در این روش صرف‌نظر کردن از اشتراک بین مجموعه‌های برشی کمینه می‌باشد. این فرض در سیستم‌های قابل اعتماد[۱] که احتمال مجموعه‌های برشی کمینه در آنها بسیار کوچک می‌باشد، فرض معقولی است.

$$T = \sum_{i=1}^{m} C_i \quad (۵-۴)$$

این روش، تنها در حالتی منجر به مقدار دقیق احتمال رویداد رأس خواهد شد که تمامی مجموعه‌های برشی کمینه درخت خطا از همدیگر مستقل باشند.

تقریب MCUB که از بسط کامل سیلوستر- پوانکاره[۲] استفاده می‌کند، منجر به نتایج دقیق‌تری برای احتمال رویداد رأس خواهد شد. نحوهٔ محاسبهٔ احتمال رویداد رأس درخت خطا با استفاده از تقریب MCUB در رابطهٔ (۴-۶) نمایش داده شده است.

[۱] - Reliable System
[۲] - Sylvester-Poincare

$$T = \sum_{i=1}^{m} C_i - \sum_{i<j}^{m} C_i C_j + \cdots + (-1)^m C_1 C_2 \dots C_m \quad (۶-۴)$$

این رابطه را می‌توان به شکل ساده‌تری نیز نوشت:

$$T = 1 - \prod_{1}^{m} (1 - C_i) \quad (۷-۴)$$

علی‌رغم اینکه در روش MCUB اشتراک بین مجموعه‌های برشی کمینه در نظر گرفته می‌شود، احتمال رویداد رأس در این روش به دلیل ساده‌سازی بسط سیلوستر – پوانکاره نیز دقیق نیست.

۴-۲- تحلیل درخت رویداد

درخت رویداد یکی دیگر از ابزارهای اصلی مورد استفاده در ارزیابی احتمالاتی ایمنی نیروگاه‌های هسته‌ای می‌باشد. فرکانس ذوب قلب راکتور که هدف نهایی تحلیل ایمنی احتمالاتی سطح ۱ در نیروگاه‌های هسته‌ای است، با استفاده از ترکیب درخت رویداد و درخت خطا محاسبه می‌شود. تحلیل درخت رویداد یک روش استنتاجی در تحلیل حوادث می‌باشد، بدین معنی که این روش در زنجیره عِلّی[۱] حادثه، رو به جلو حرکت می‌کند. به بیان دیگر، در تحلیل درخت رویداد آنچه پس از وقوع یک رویداد نامطلوب رخ می‌دهد مورد نظر تحلیل‌گر است؛ درحالی‌که در تحلیل درخت خطا، هدف پیداکردن عواملی است که منجر به یک رویداد نامطلوب می‌شود. بنابراین، مدل‌سازی ترتیب و توالی رویدادها در یک حادثه در تحلیل ایمنی احتمالاتی نیروگاه‌های هسته‌ای، معمولاً با استفاده از تحلیل درخت رویداد انجام می‌شود؛ اما مدل‌سازیِ خرابی سیستم‌های ایمنی که برای مقابله با چنین حادثه‌ای درنظر گرفته‌اند، به وسیلهٔ درخت خطا صورت می‌گیرد. در نهایت، ترکیب این دو ابزار، مدل کامل تحلیل ایمنی احتمالاتی یک نیروگاه هسته‌ای را شکل می‌دهد.

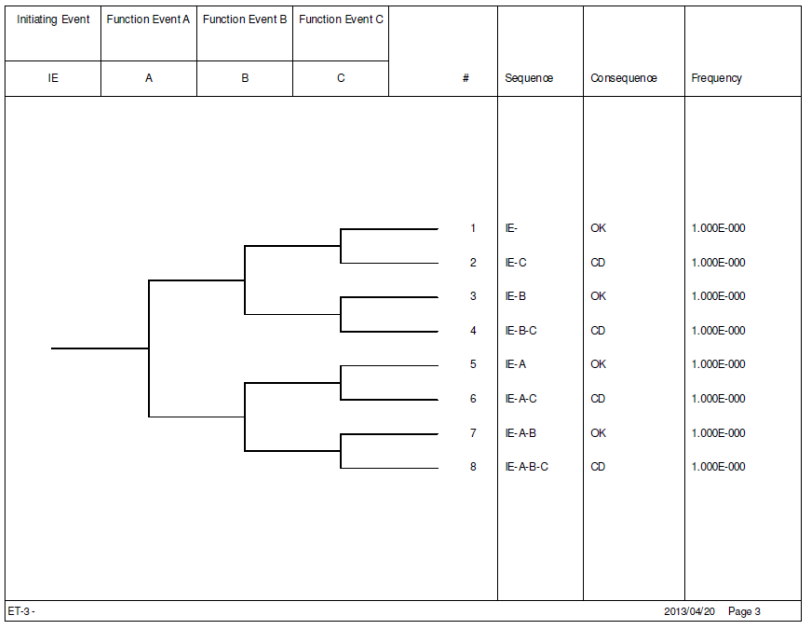
ترکیب تحلیل درخت خطا و درخت رویداد در تحلیل ایمنی احتمالاتی نیروگاه‌های هسته‌ای به یکی از دو روش FTL یا ETL صورت می‌گیرد. در روش اول که در تحلیل ایمنی احتمالاتی نیروگاه‌های هسته‌ای مرسوم‌تر است، پیامد رویدادهای آغازگر به وسیلهٔ درخت رویداد مدل می‌شود و از درخت خطا نیز برای مدل‌سازی سیستم‌های ایمنی استفاده می‌شود. با توجه به اینکه در این روش کلیهٔ اجزای سیستم‌های ایمنی در درخت خطای آن درنظر گرفته می‌شوند، این روش نهایتاً منجر به تولید درخت‌های خطای بزرگی خواهد شد. از این رو، به این روش، روش درخت خطای بزرگ[۲] نیز گفته می‌شود.

[۱] - Causal Chain
[۲] - Large Fault Tree

در روش دوم بخش‌های مشترک در بین سیستم‌های ایمنی مختلف، به عنوان مثال سیستم‌های پشتیبان مانند تغذیه الکتریکی، خود در درخت‌های خطای جداگانه مدل‌سازی شده و برخلاف روش اول، در درخت رویداد نیز به صورت مستقل وارد می‌شوند. از آنجاکه این روش در نهایت منجر به ایجاد درخت رویدادهای بزرگ خواهد شد، به آن روش درخت رویداد بزرگ[۱] نیز اطلاق می‌شود. برای محاسبهٔ فرکانس توالی‌های درخت رویداد، از دو روش Split Fraction و Delete Terms استفاده می‌شود. در ادامه مفاهیم و اجزای درخت رویداد و روش‌های حل آن معرفی می‌شوند.

۴-۲-۱- مفاهیم پایه‌ای تحلیل درخت رویداد

هر درخت رویداد دارای یک رویداد آغازگر[۲] و تعدادی رویداد عملکرد[۳] می‌باشد. رویداد آغازگر نشان‌دهندهٔ وقوع یک رویداد نامطلوب و رویدادهای عملکرد نمایندهٔ سیستم‌ها یا اقدامات ایمنی جهت جلوگیری از عواقب وخیم رویداد نامطلوب می‌باشند. وقوع یا عدم وقوع هرکدام از رویدادهای عملکرد نیز، خرابی یا موفقیت آن عملکرد ایمنی را نشان می‌دهد.



شکل ۶۳: نمونه درخت رویداد رسم شده توسط نرم‌افزار SAPHIRE

رسم یک درخت رویداد با تعیین رویداد آغازگر آن آغاز می‌شود، سپس در مرحلهٔ بعد عواملی که جهت جلوگیری از پیامدهای وخیم آن درنظر گرفته شده‌اند، تعیین می‌شود. این فرایند تا زمانی ادامه می‌یابد که کلیه رویدادهای عملکرد تعیین شده

[۱] - Large Event Tree
[۲] - Initiating Event
[۳] - Function Event

باشند. پس از تعیین رویداد آغازگر و رویدادهای عملکرد، بایستی با توجه به خرابی یا موفقیت رویدادهای عملکرد، توالی‌های مختلف ممکن، پس از وقوع رویداد آغازگر و پیامد آن‌ها را تعیین نمود. در این حالت، محاسبهٔ احتمال وقوع توالی‌های مختلف درخت رویداد با توجه به رویدادهای عملکرد قابل انجام می‌باشد. شکل ۶۳ نمونهٔ درخت رویداد رسم شده توسط نرم‌افزار SAPHIRE را نشان می‌دهد.

۴-۲-۱-۱- رویداد آغازگر

در تحلیل درخت رویداد، به اولین متغیر ورودی درخت رویداد، رویداد آغازگر می‌گویند. رویداد آغازگر در درخت رویداد نشان‌دهندهٔ وقوع یک رویداد نامطلوب می‌باشد که با ترکیب با خرابی تجهیزات، سیستم‌ها یا عملکردهای ایمنی منجر به یک پیامد نامطلوب شود. از آنجا که رویدادهای آغازگر یک فرکانس وقوع دارند، بنابراین برخلاف احتمال رویدادهای پایه، مقدار عددی آن محدودیتی ندارد و می‌تواند بزرگ‌تر از یک نیز باشد. رویداد آغازگر در شکل ۶۳، در قسمت بالا سمت چپ شکل با حروف اختصاری IE نشان داده شده‌است.

۴-۲-۱-۲- رویداد عملکرد

رویداد عملکرد نشان‌دهنده تجهیزات، سیستم‌ها یا عملکردهای ایمنی می‌باشد که برای پیشگیری از وقوع پیامدهای نامطلوب یک رویداد آغازگر درنظر گرفته شده‌است. در رسم درخت رویداد معمولاً رویدادهای عملکرد را به ترتیب وارد عمل شدن آنها پس از وقوع رویداد آغازگر، تعریف می‌کنند. درصورتی‌که وقوع یا عدم وقوع رویداد عملکرد تأثیر محسوسی در جلوگیری از پیامد نامطلوب رویداد آغازگر داشته باشد، درخت رویداد در این نقطه به دو شاخه تقسیم می‌شود که شاخه بالا موفقیت و شاخه پایین خرابی سیستم را نشان می‌دهد. رویدادهای عملکرد در قسمت بالای شکل ۶۳ با حروف A، B و C نشان داده شده‌اند. ورودی یک رویداد عملکرد می‌تواند یک درخت خطا یا فقط یک رویداد پایه باشد.

۴-۲-۱-۳- توالی درخت رویداد

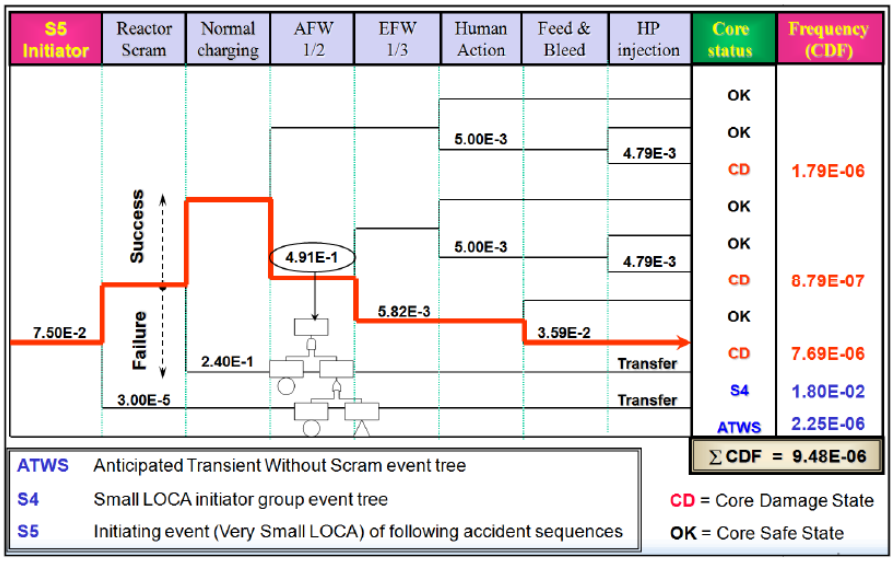
با توجه به آنچه در بخش پیش ذکر شد، هرکدام از مسیرهای درخت رویداد نشان‌دهنده عدم موفقیت تعدادی از سیستم‌ها یا عملکردهای ایمنی و موفقیت سایر سیستم‌ها پس از وقوع رویداد آغازگر می‌باشد. به هرکدام از این مسیرهای درخت رویداد یک توالی حادثه[۱] گفته می‌شود. توالی‌های مختلف درخت رویداد در شکل ۶۳، به ترتیب با اعداد ۱ تا ۸ مشخص

[۱] - Accident Sequence

شده‌اند. به عنوان مثال، توالی شماره ۷ نشان‌دهنده خرابی سیستم‌های A و B و همچنین موفقیت سیستم C پس از وقوع رویداد آغازگر می‌باشد.

۴-۲-۱-۴- پیامد درخت رویداد

هرکدام از مسیرهای درخت رویداد در نهایت منتهی به یک وضعیت پایدار مشخص برای سیستم خواهند شد. به عنوان مثال، در مورد راکتورهای هسته‌ای، وضعیت نهایی[۱] می‌تواند یکی از دو حالت خاموشی راکتور یا ذوب قلب راکتور درنظر گرفته شود. به هرکدام از این وضعیت‌های نهایی یک پیامد درخت رویداد گفته می‌شود و در یک تحلیل ایمنی احتمالاتی هدف اصلی پیدا کردن فرکانس یک پیامد خاص مانند ذوب قلب راکتور است که ممکن است از رویدادهای آغازگر مختلف ناشی شده باشد. این مسأله در شکل ۶۴ نشان داده شده‌است.



شکل ۶۴: درخت رویداد حادثه شکست بسیار کوچک مدار اول

رویداد آغازگر این درخت رویداد، شکست بسیار کوچک در یک مدار اولیه نیروگاه هسته‌ای می‌باشد که با S5 نمایش داده شده‌است. سیستم‌های ایمنی جهت مقابله با این رویداد آغازگر نیز در قسمت بالای شکل با رنگ متمایز و پس از رویداد آغازگر قرار گرفته‌اند. در قسمت پایین سمت راست شکل نیز نشان داده شده است که هدف، پیداکردن مجموع فرکانس ذوب قلب راکتور است که با حروف اختصاری CD مشخص شده‌است. در ستون پیامد مربوط به این درخت رویداد دو حالت S4 و ATWS نیز دیده می‌شود که بر روی توالی مربوط به آن‌ها نیز کلمه Transfer درج شده‌است. این عبارت بدین معنی است که رویداد آغازگر اولیه با ترکیب با خرابی عملکردهای ایمنی منجر به رویداد آغازگر دیگری شده‌است که باید در یک درخت

[۱] - End State

رویداد دیگر مدل‌سازی شود. انتقال در درخت رویداد نیز مشابه انتقال در درخت خطا می‌باشد و برای هرکدام از توالی‌های انتقال یافته، یک درخت رویداد جداگانه رسم می‌شود.

۴-۲-۲- روش‌های تحلیل درخت رویداد

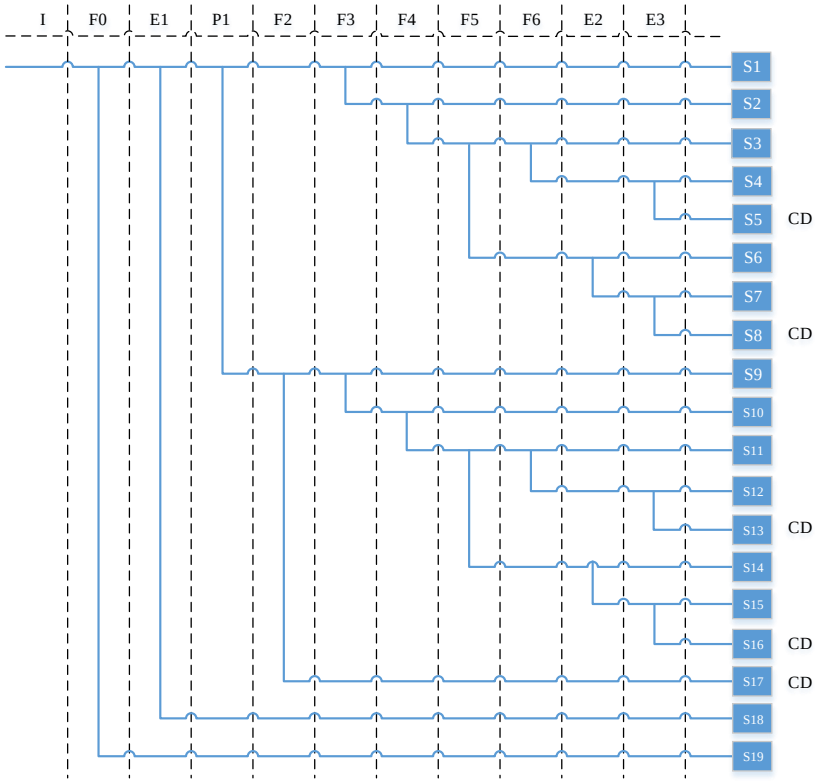
هدف اصلی در تحلیل درخت رویداد، محاسبهٔ فرکانس پیامد نامطلوب ناشی از یک رویداد آغازگر می‌باشد. از آنجا که در یک درخت رویداد، ممکن است توالی‌های متعددی منجر به پیامد نامطلوب شوند، باید ابتدا فرکانس هرکدام از این توالی‌ها محاسبه شود. بنابراین، محاسبات تحلیل درخت رویداد درنهایت به محاسبه فرکانس توالی‌های مختلف آن ختم می‌شود. احتمال وقوع هرکدام از توالی‌های درخت رویداد نیز، احتمال اشتراک رویداد آغازگر و رویدادهای عملکرد در آن توالی می‌باشد. برای محاسبه احتمال یا فرکانس هرکدام از توالی‌های درخت رویداد و یا پیامدهای آن روش‌های مختلفی وجود دارد که در ادامه به برخی از این روش‌ها اشاره می‌شود.

۴-۲-۲-۱- روش Split Fraction

ساده‌ترین روش برای محاسبه فرکانس توالی‌های مختلف درخت رویداد استفاده از حاصل‌ضرب احتمال رویدادهای عملکردی و فرکانس رویداد آغازگر می‌باشد. در این حالت، فرض بر این است که رویدادهای عملکردی از همدیگر مستقل می‌باشند. بنابراین، احتمال اشتراک آنها، برابر حاصل‌ضرب احتمال آن‌ها می‌باشد. در این روش، اگر ورودی رویداد عملکردی خود یک گیت یا درخت خطا نیز باشد، فقط احتمال رویداد رأس آن در محاسبه فرکانس توالی مربوطه استفاده خواهد شد. بدیهی است که در مورد رویدادهای عملکرد موفق احتمال متمم آنها در نظرگرفته می‌شود. روش Split Fraction وابستگی بین رویدادهای عملکردی را در نظر نمی‌گیرد و فرض می‌کند که این رویدادها از همدیگر مستقل می‌باشند. بنابراین نتایج حاصل از این روش تنها در صورتی معتبر است که رویدادهای عملکردی از همدیگر مستقل باشند.

۴-۲-۲-۲- روش Delete Terms

در تحلیل‌های مرسوم ایمنی احتمالاتی معمولاً وابستگی‌های متعددی بین رویدادهای عملکرد وجود دارد، در نتیجه استفاده از روش Split Fraction به نتایج دقیقی منجر نخواهد شد. به عنوان نمونه، در این زمینه درخت رویداد حادثه شکست بزرگ مدار اول در یک نیروگاه آب جوشان در شکل ۶۵ داده شده‌است.



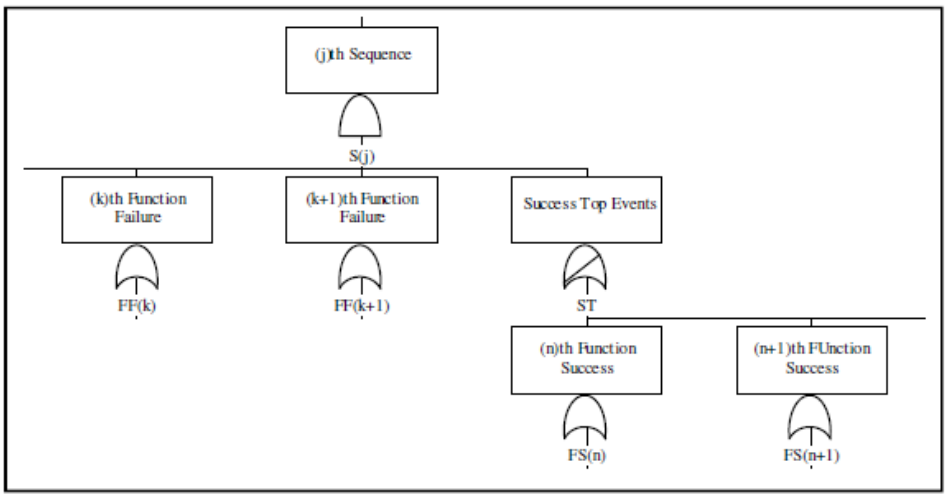
شکل ۶۵: درخت رویداد حادثه شکست بزرگ مدار اول یک راکتور آب جوشان

ماتریس وابستگی‌های بین رویدادهای عملکردی این درخت رویداد در جدول شماره ۲۱ آمده است. اعداد درون جدول نشان دهنده تعداد رویدادهای پایهٔ مشترک بین رویدادهای عملکردی می‌باشد.

جدول شماره ۲۱: ماتریس وابستگی بین رویدادهای عملکردی درخت رویداد

No.	F1	F2	F3	F4	F5	F6
F1	275	5	5	5	0	5
F2	5	797	706	646	17	543
F3	5	706	767	673	17	551
F4	5	646	673	731	17	543
F5	0	17	17	17	79	17
F6	5	543	551	543	17	657

با توجه به جدول، مشاهده می‌شود که مجموعه رویدادهای عملکردی F2، F3، F4 و F6 دارای بیشترین رویدادهای مشترک هستند. با توجه به ماتریس وابستگی بین رویدادهای عملکردی، فرض استقلال آنها در این مورد درست نبوده و منجر به نتایج دقیق نخواهد شد. برای حل دقیق‌تر این مسئله، می‌توان هرکدام از توالی‌های یک درخت رویداد را مانند شکل ۶۶ به درخت خطای معادل آن تبدیل کرده، سپس با استفاده از مجموعه‌های برشی کمینه، فرکانس آن توالی را محاسبه نمود.



شکل ۶۶: درخت خطای معادل یک توالی درخت رویداد

همانگونه که در شکل ۶۶ مشاهده می‌شود، هر توالی به صورت یک گیت AND در نظرگرفته می‌شود که ورودی‌های آن وقوع یا عدم وقوع رویدادهای عملکردی می‌باشند. رویدادهای عملکرد ناموفق به‌طور مستقیم به گیت AND وارد می‌شوند و رویدادهای عملکرد موفق به یک گیت NOR وارد می‌شوند، که خود به گیت AND اصلی وارد شده‌است. با توجه به قوانین دمورگان گیت NOR به گیت AND تبدیل می‌شود. درصورتی‌که ورودی گیت متمم، خود یک گیت باشد، نوع آن منفی شده و فرایند تبدیل تا آخرین زیر شاخه‌های آن گیت ادامه پیدا می‌کند.

با وجود اینکه روشِ دقیقِ مدل‌سازی شاخه‌های موفقیت درخت رویداد تبدیل دمورگان می‌باشد، اما به دلیل هزینهٔ بالای محاسباتی (زمان و حافظه زیاد مورد نیاز) در تبدیل گیت‌های متمم، این کار در اکثر نرم‌افزارهای تحلیل ایمنی احتمالاتی انجام نمی‌شود.

۵- خرابی عامل مشترک

خرابی اجزای مختلف در اثر عامل مشترک یکی از مهم‌ترین مباحث در ارزیابی قابلیت اطمینان یا عدم دسترسی سیستم است. چنین رویدادهایی در مقایسه با خرابی‌های تصادفی اجزای منفرد، نسبتاً احتمال پایینی دارند، اما در بسیاری از حالت‌ها پیامد این رویدادها آسیب مستقیم به سیستم ایمنی یا آسیب مستقیم به اقدامات پیش‌گیرانهٔ ایمنی است. به همین دلیل، وجود خرابی عامل مشترک و مدل‌سازی آن در ساختار درخت خطا، بیشترین اهمیت در تحلیل ایمنی احتمالاتی را دارد.

طی سالیان گذشته مدل تحلیل ایمنی احتمالاتی نیروگاه‌های اتمی دچار تغییرات کوچک و بزرگ بسیاری برای حصول مقاصد اساسی آن شده است که به عنوان یک مثال برای فراهم آوردن اطلاعات مناسب در زمینهٔ ریسک مرتبط با طراحی و عملکرد تأسیسات واقعی ارائه می‌شود. همهٔ تغییرات در مدل تحلیل ایمنی احتمالاتی نیروگاه به منظور بهبود صحت عملکرد در ارائه عملکرد نیروگاه انجام شده است. در ادامه سیر تکامل مدل‌سازی خرابی عامل مشترک ارائه می‌شود.

خرابی‌های عامل مشترک که زیرمجموعه‌ای از کلاس عمومی رویدادهای وابسته است، به صورت خرابی‌های چندگانه اجزا در اثر علت ریشه‌ای مشترک تعریف می‌شود. مشخصهٔ کلیدی یک رویداد با عامل مشترک این است که دو یا چند جزء باید یک علت مشترک داشته باشند، به‌طوری‌که آن علت، نباید خرابی یا عدم دسترسی عملکردی جزء دیگر باشد.

خرابی‌های عامل مشترک لحاظ شده در مدل‌های منطقی (درخت خطا و رویداد)، شامل وابستگی اجزای داخلی است که اهمیت بالقوّه‌ای برای آنها لحاظ نمی‌شود و مکانیزم‌های آنها به‌صورت صریح در مدل منطقی (درخت خطا و رویداد) اشاره نشده است. هرگاه امکان‌پذیر باشد، مکانیزم‌های خرابی وابستهٔ ویژه باید به‌صورت صریح مدل‌سازی شوند و توصیه می‌شود که تمایز مشخصی بین چنین مدل‌سازی و حیطهٔ تحلیل خرابی عامل مشترک لحاظ شود.

خرابی‌های عامل مشترک یک کلاس مهم از رویدادهای وابسته با لحاظ سهم آنها در عدم دسترسی سیستم است. تحلیل‌های سیستم‌هایی که تنها خرابی‌های مستقل تصادفی را لحاظ می‌کنند، منجر به تخمین ناچیز عدم دسترسی شده و منجر به شناخت نادرست از مزایای افزونگی و تنوع در طراحی سیستم می‌شود. در ادامه بررسیِ تاریخچه‌ای مدل خرابی عامل مشترک ارائه می‌شود.

۵-۱- خرابی ناشی از عامل مشترک چیست؟

یک خرابی عامل مشترک خرابی است که:

- دو یا چند جزء در یک زمان مشخص به گونه‌ای خراب شوند که موفقیت مأموریت سیستم غیرقطعی شود؛
- خرابی‌های جزء، ناشی از یک علت و مکانیزم مشترک (عامل اتصال) باشد.

دو جزء ۱ و ۲ را در نظر بگیرید. E_i رویدادی است که جزء i در آن در حالت خراب قرار دارد. احتمال اینکه هر دو جزء در حالت خراب باشند عبارت است از:

$$q(E_1 \cap E_2) = q(E_1|E_2).q(E_2) = q(E_2|E_1).q(E_1) \quad (۱-۵)$$

اگر شروط زیر برقرار باشد، آنگاه دو رویداد E1 و E2 از لحاظ آماری مستقل خواهند بود.

$$q(E_1|E_2) = q(E_1), \quad q(E_2|E_1) = q(E_2) \quad (۲-۵)$$

در این حالت خواهیم داشت:

$$q(E_1 \cap E_2) = q(E_1).q(E_2) \quad (۳-۵)$$

هنگامی‌که $E_1 \cap E_2 = 0$ باشد، آنگاه $q(E_1 \cap E_2) = 0$ و $q(E_1|E_2) = 0$ خواهد بود.

دو آیتم ۱ و ۲ زمانی وابسته هستند که شرایط زیر برقرار باشند:

$$q(E_1|E_2) \neq q(E_1), \quad q(E_2|E_1) \neq q(E_2) \quad (۴-۵)$$

دو آیتم ۱ و ۲ وابستهٔ مثبت هستند، هرگاه $q(E_1|E_2) > q(E_1)$ و $q(E_2|E_1) > q(E_2)$ باشد. در این حالت خواهیم داشت:

$$q(E_1 \cap E_2) > q(E_1).q(E_2) \quad (۵-۵)$$

دو آیتم ۱ و ۲ وابستهٔ منفی هستند، هرگاه $q(E_1|E_2) < q(E_1)$ و $q(E_2|E_1) < q(E_2)$ باشد. در این حالت خواهیم داشت:

$$q(E_1 \cap E_2) < q(E_1).q(E_2) \quad (۶-۵)$$

وابستگی مثبت در تحلیل‌های ریسک و قابلیت اطمینان معمولاً بسیار رایج است. وابستگی منفی نیز در برخی حالت‌ها وجود دارد. به عنوان مثال، دو جزء که با تولید ارتعاشات یا حرارت بر یکدیگر تأثیرگذار هستند و از این طریق به یکدیگر آسیب می‌رسانند را در نظر بگیرید. هنگامی که یک آیتم خراب می‌شود و تحت تعمیر قرار می‌گیرد، آیتم دیگر یک محیط عملکرد بهتری خواهد داشت و احتمال خرابی آن کاهش می‌یابد. در این مثال، احتمال خرابی آیتم ۲ به شرط خرابی آیتم ۱ کوچکتر از احتمال خرابی آیتم ۲ بوده و وابستگی منفی حاکم است.

۵-۱-۱- وابستگی ذاتی

به حالتی که وضعیت یک جزء تحت تأثیر وضعیت عملکردی سایر اجزا است، وابستگی ذاتی می‌گویند. وابستگی ذاتی شامل زیرمجموعه‌های زیر است:

- وابستگی الزامات عملکردی،
- وابستگی ورودی عملکردی،
- خرابی آبشاری.

خرابی آبشاری به سلسلهٔ توالی خرابی‌های جزء گفته می‌شود که در آن، بارِ اولین خرابی به جزء یا اجزای مجاور منتقل شده به گونه‌ای که منجر به خرابی آنها می‌شود و در ادامه، این بار خرابی به سایر اجزای دیگر منتقل می‌شود. این نوع خرابی گاهی به نام اثر دومینو نیز شناخته می‌شود.

۵-۱-۲- وابستگی فرعی

به حالتی‌که وابستگی یا ارتباط به صورت ذاتی نباشد یا در مشخصات عملکردی سیستم نباشد، وابستگی فرعی می‌گویند. وابستگی فرعی می‌تواند به موارد زیر مرتبط باشد:

- تنش‌های فیزیکی یا محیطی،
- مداخلهٔ انسانی.

۵-۲- مؤلفه‌های اصلی خرابی عامل مشترک

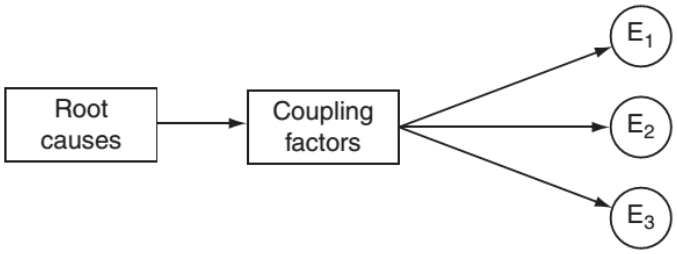
وجود یک عامل مشترک اساس این نوع خرابی‌ها است. عامل مشترک، دو جزء دارد که شامل علت ریشه‌ای و عامل ارتباط است.

- علت ریشه‌ای در پاسخ به سوال «چرا جزء خراب شد؟» که مرتبط با جزء است، جستجو می‌شود؛
- عامل ارتباط در پاسخ به سوال «چرا چند جزء خراب شدند؟» که به ارتباطات بین چند جزء اشاره دارد، حاصل می‌شود.

۵-۲-۱- بیان دیگر علت ریشه‌ای و عامل ارتباط

علت ریشه‌ای: اساسی‌ترین علت خرابیِ جزء است که اگر اصلاح شود، می‌توان از وقوع چنین خرابی و خرابی‌های مشابه جلوگیری کرد.

عامل ارتباط: خصوصیتی که باعث می‌شود اجزای چندگانه، مستعد علت ریشه‌ای یکسان شوند. به عامل ارتباط، مکانیزم ارتباط نیز گفته می‌شود.



شکل ۶۷: علت ریشه‌ای و عامل ارتباط در خرابی عامل مشترک

۵-۲-۱-۱- علل ریشه‌ای نوعی

در علل ریشه‌ای، می‌توان بین علل عملکردی و غیرعملکردی تمایز قائل شد.

علل ریشه‌ای غیرعملکردی، علل ریشه‌ای ناشی از خطاهای طراحی، تولید، ساخت، نصب و برپاسازی هستند. درحالی‌که علل ریشه‌ای عملکردی شامل دو مورد زیر است:

- علل وابسته به بهره‌برداری و نگهداری: رویّه‌ها، اقدامات، کفایت و زمان‌بندی ناکافی بهره‌برداری و نگهداری،
- تنش‌های محیطی: در معرض‌قرار گیری داخلی و خارجی محدودهٔ طراحی یا رویدادهایی مانند زمین‌لرزه، آتش‌سوزی، سیل و ... .

۵-۲-۱-۲- عامل ارتباط نوعی

عامل ارتباط در شباهت‌ها یافت می‌شود. شباهت‌های اجزا ممکن است یکی از موارد زیر باشد:

- طراحی یکسان،
- سخت‌افزار یکسان،
- عملکرد یکسان،

- نرم‌افزار یکسان،
- کارکنان نصب یکسان،
- کارکنان بهره‌برداری و نگهداری یکسان،
- رویه‌های یکسان،
- واسط سیستم/جزء یکسان،
- محیط یکسان،
- موقعیت (فیزیکی) یکسان.

۵-۲-۲- گروه اجزای خرابی عامل مشترک

گروه اجزای خرابی علت مشترک، مجموعهٔ اجزای سیستم هستند که می‌توانند مودهای خرابی عامل مشترک یکسانی داشته باشند. به طور کلی یک گروه خرابی عامل مشترک، دارای مؤلفه‌هایی می‌باشد. اسمیت و واتسون (۱۹۸۰) پیشنهاد کردند که یک تعریف خرابی عامل مشترک باید محتوی موارد زیر باشد:

- اجزای آسیب دیده قادر به انجام کار مورد نیاز نباشند؛
- خرابی‌های چندگانه در ترکیب‌های افزونه وجود داشته باشد؛
- خرابی‌ها از نوع نتیجهٔ خرابی آبشاری نباشد و خرابی اولیه باشد؛
- خرابی در بازهٔ زمانی بحرانی تعریف شده رخ دهد (مثلاً زمانی که یک هواپیما درحال پرواز در هوا باشد)؛
- خرابی‌ها در اثر یک عیب اساسی یا پدیدهٔ فیزیکی (عامل مشترک) باشند؛
- اثر خرابی‌ها باید منجر به غیرفعال شدن عمده در قابلیت مورد نیاز سیستم شود.

۵-۲-۳- رویداد خرابی عامل مشترک

رویداد خرابی عامل مشترک، رویدادی است که شامل خرابی یک مجموعهٔ خاص از اجزا در اثر عامل مشترک باشد. این رویداد دارای شاخصه‌های زیر است:

- یک رویداد خرابی عامل مشترک حاوی خرابی دو یا چند جزء است؛
- خرابی‌های اجزای یک رویداد خرابی عامل مشترک می‌توانند همزمان یا در یک بازهٔ زمانی کوتاه مشخص شده رخ دهند؛

- وقوع یا عدم وقوع خرابی اجزا به صورت همزمان، وابسته به عامل مشترک است؛
- رویداد خرابی عامل مشترک با نام رویداد پایهٔ عامل مشترک نیز شناخته می‌شود.

۵-۲-۳-۱- مثال رویداد خرابی عامل مشترک

یک سیستم با تعداد m آشکارساز گازی که در اتاق تولید نصب شده‌اند را در نظر بگیرید. یک رویداد عامل مشترک بالقوّه، افزایش رطوبت در اتاق است. این عامل مشترک، به افزایش احتمال خرابی آشکارساز منجر خواهد شد. ولی خرابی‌ها به صورت عادی در یک زمان رخ نخواهد داد. زمان بین خرابی‌های آشکارسازها ممکن است نسبتاً زیاد باشد.

۵-۳- تعریف‌های خرابی عامل مشترک در صنایع مختلف

خرابی عامل مشترک در صنعت هسته‌ای (NEA، ۲۰۰۴) به صورت خرابی وابسته که به صورت همزمان یا در بازهٔ زمانی کوتاهی، در دو یا چند جزء در اثر نتیجهٔ مستقیم یک علت مشترک روی می‌دهد، تعریف می‌شود.

در صنعت فضایی (NAS A PRA guide، ۲۰۰۲)، خرابی (یا حالت عدم دسترسی) بیش از یک جزء در اثر یک علت مشترک هنگام مأموریت سیستم، خرابی عامل مشترک نامیده می‌شود.

در صنعت فرایند (IEC 61511، ۲۰۰۳) خرابی ناشی از اثر یک یا چند رویداد، که باعث خرابی دو یا چند کانال مجزا در یک سیستم چندکاناله شده و منجر به خرابی سیستم شود، خرابی عامل مشترک می‌باشد.

۵-۴- رویکرد مدل‌سازی

مراحل اصلی مدل‌سازی خرابی عامل مشترک، شامل موارد زیر است:

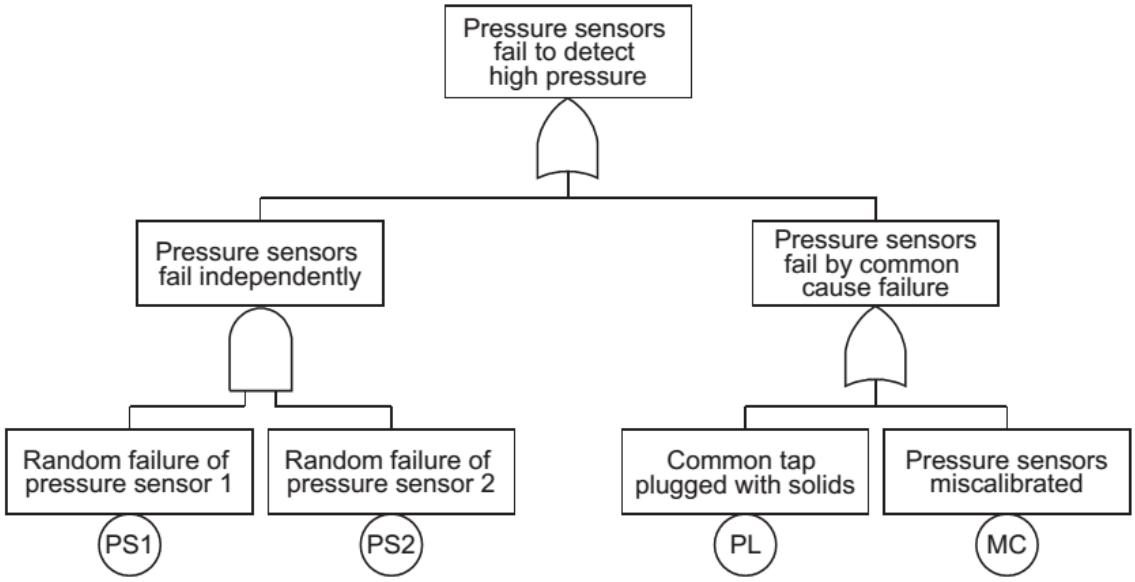
- توسعهٔ یک مدل منطقی سیستمی (به عنوان مثال یک درخت خطا یا یک دیاگرام قابلیت اطمینان)،
- شناسایی گروه‌های خرابی عامل مشترک،
- شناسایی علل ریشه‌ای مرتبط و عوامل/ مکانیزم ارتباط،
- ارزیابی کارایی حفاظ‌های خرابی عامل مشترک،
- توسعهٔ مدل‌های صریح،
- لحاظ مدل‌های ضمنی،
- کمّی‌سازی قابلیت اطمینان و تفسیر نتایج.

۵-۴-۱- مدل‌سازی صریح

علت مشترک به صورت یک رویداد پایهٔ مجزا در مدل قابلیت اطمینان است. علت‌های صریح می‌تواند یکی از موارد زیر باشد:

- خطاهای انسانی،
- خرابی‌های منابع توان، سرمایش و گرمایش، توان هیدرولیک،
- تجهیزات مشترک،
- رویدادهای محیطی (طوفان، سیل، صاعقه و ...)

در شکل ۶۸ نمونهٔ مدل‌سازیِ صریحِ خرابی عامل مشترک در یک درخت خطای منطقی برای خرابی دو حسگر فشار ارائه شده است.



شکل ۶۸: نمونهٔ درخت خطای منطقی شامل خرابی عامل مشترک دو حسگر فشار

۵-۴-۲- مدل‌سازی ضمنی

هنگامی‌که یک مجموعه از اجزا شماری از علت‌های ریشه‌ای و عوامل ارتباطی مشترک دارند و مدل‌سازی صریح قابل مدیریت نباشد، علل باقی‌ماندهٔ مشترک به صورت رویدادهای پایهٔ مرکب مدل می‌شود؛ برخلاف مثال شکل ۶۸ که دو علت خرابی مشترک به صورت مجزا لحاظ شده‌اند.

۵-۴-۳- خرابی‌های چندگانه

اجزای یک گروه خرابی عامل مشترک در اثر روی‌دادن خرابی، به صورت واقعی دچار خرابی می‌شوند. این خرابی می‌تواند دو حالت داشته باشد:

۱. خرابی کامل: درصورتی‌که همهٔ اجزای گروه خراب شوند.

۲. خرابی جزئی: درصورتی‌که بیش از یک جزء و نه همهٔ اجزا خراب شوند.

هنگامی که علت مشترک رخ می‌دهد، چندگانگی رویداد خرابی عامل مشترک (تعداد اجزای خراب شده در اثر عامل مشترک) اغلب یک متغیر تصادفی است. برخی از تحلیل‌گرانِ ریسک می‌گویند هنگامی که تنها خرابی یک جزء از یک گروه در اثر عامل مشترک داریم نیز، آن رویداد خرابی از جنس خرابی عامل مشترک است. برخی تحلیل‌گران دیگر ممکن است بگویند هنگامی‌که هیچ جزئی از یک گروه خراب نشود نیز، یک رویداد خرابی عامل مشترک خواهیم داشت. یعنی هنگامی که علت مشترک منجر به خرابی هیچکدام از اجزای گروه نشود، رویداد خرابی عامل مشترک واقع شده است. این تفسیر از خرابی عامل مشترک جای بحث و بررسی دارد، اما ممکن است برای برخی از مدل‌های خرابی عامل مشترک سودمند باشد.

۵-۴-۴- فرضیات تقارن

یک سیستم با m جزء را در نظر بگیرید. در بسیاری از مدل‌های خرابی عامل مشترک، فرضیات تقارن زیر به کار می‌روند:

- فرض تقارن کامل: تقارن کامل در m جزء وجود دارد و بخش‌های هر جزء دارای نرخ خرابی ثابت یکسان است.
- فرض تقارن جزئی: همهٔ ترکیبات که در آنها k جزء خراب نشده و m-k جزء خراب می‌شوند، دارای احتمال وقوع یکسانی هستند.
- حذف j جزء از m جزء، اثری بر احتمالات خرابی m-j جزء باقی‌مانده ندارد.

مثال: یک سیستم با سه جزء ۱، ۲ و ۳ را در نظر بگیرید. E_i رویدادی است که جزء i در حالت خرابی قرار دارد. یک رویداد خرابی می‌تواند ۳ نوع چندگانگی مختلف داشته باشد:

خرابی تک جزئی: به سه طریق مختلف قابل وقوع است:

$$(E_1 \cap E_2^* \cap E_3^*), (E_1^* \cap E_2 \cap E_3^*), (E_1^* \cap E_2^* \cap E_3) \qquad (۷-۵)$$

خرابی دو جزئی:

$$(E_1 \cap E_2 \cap E_3^*), (E_1 \cap E_2^* \cap E_3), (E_1^* \cap E_2 \cap E_3) \quad (۸-۵)$$

خرابی سه جزئی:

$$(E_1 \cap E_2 \cap E_3) \quad (۹-۵)$$

احتمال اینکه تعداد مشخصی از اجزا، (مثلاً k جزء)، خراب شوند:

$$q_{1,3} = q(E_1 \cap E_2^* \cap E_3^*) = q(E_1^* \cap E_2 \cap E_3^*) = q(E_1^* \cap E_2^* \cap E_3) \quad (۱۰-۵)$$

$$q_{2,3} = (E_1 \cap E_2 \cap E_3^*) = (E_1 \cap E_2^* \cap E_3) = (E_1^* \cap E_2 \cap E_3) \quad (۱۱-۵)$$

$$q_3^3 = (E_1 \cap E_2 \cap E_3) \quad (۱۲-۵)$$

احتمال اینکه یک رویداد عامل مشترک در یک سیستم m جزئی باعث خرابی k جزء شود:

$$Q_{1:3} = \binom{3}{1} q_{1,3} = 3.q_{1,3} \quad (۱۳-۵)$$

$$Q_{2:3} = \binom{3}{2} q_{2,3} = 3.q_{2,3} \quad (۱۴-۵)$$

$$Q_{3:3} = \binom{3}{3} q_{3,3} = q_{3,3} \quad (۱۵-۵)$$

۵-۵- مدل پارامترهای یونانی چندگانه[۱]

در مدل MGL، پارامترها بر حسب احتمال خرابی کلی جزء به دست می‌آید، که شامل اثرات همهٔ مؤلفه‌های (مستقل و مشترک) سهیم در خرابی جزء و یک مجموعهٔ حاوی سهم‌های خرابی همهٔ راه‌های ممکن خرابی عامل مشترک یک جزء که می‌تواند با سایر اجزا در همان گروه به اشتراک گذارد، می‌باشد.

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \prod_{i=1}^{k} \rho_i (1-\rho_{k+1}) Q_t$$

[۱] - MGL

ρ_1 برابر ۱، ρ_{m+1} برابر صفر و ρ_i برای $i=2,...,m$، احتمال شرطی اینکه علت خرابی یک جزء که با $i-1$ جزء مشترک است، با i جزء یا بیشتر مشترک خواهد بود و منجر به خرابی $i-1$ جزء می‌شود. حروف یونانی تعیین شده برای این احتمالات شرطی به صورت $\rho_2=\beta,\rho_3=\gamma,\rho_4=\delta,...$ است.

در حالتی که m برابر ۲ باشد، مدل MGL به مدل فاکتور بتا که برای گروه‌های دو جزئی خرابی عامل مشترک مناسب است، خلاصه می‌شود.

$$Q_1^{(2)}=(1-\beta)Q_t\ ,\ Q_2^{(2)}=\beta Q_t$$

مدل فاکتور بتا می‌تواند برای گروه‌های با بیش از ۲ جزء نیز به کار رود. در این صورت اگر خرابی عامل مشترک روی دهد، آنگاه همهٔ m جزء خراب خواهند شد. در این حالت، $\rho_1=\rho_2=...=\rho_{m-1}=1,\rho_m=\beta,\rho_{m+1}=0$ خواهد بود.

یک فرض عمومی در تحلیل ایمنی احتمالاتی Krsko این است که افزونگی بیش از ۴ اعتبار ندارد. با توجه به رابطهٔ فوق، برای یک گروه بیش از ۴ جزء، $\rho_5=\rho_6=...=\rho_{m-1}=1$ خواهد بود.

۵-۶- مدل فاکتور بتا

در این مدل، نرخ خرابی یک جزء به دو بخش مستقل و وابسته تقسیم می‌شود. فاکتور بتا به صورت زیر تعریف می‌شود:

$$\lambda=\lambda_I+\lambda_c \qquad (۱۶-۵)$$

$$\beta=\frac{\lambda_c}{\lambda} \qquad (۱۷-۵)$$

بنابراین، فاکتور بتا کسری از خرابی همهٔ آیتم‌های موجود است که سهم خرابی‌های عامل مشترک می‌باشد. یک سیستم با m جزء مشابه را در نظر بگیرید. خرابی هر جزء می‌تواند دو علت مجزا داشته باشد: (۱) علت مستقل که تنها این جزء را تحت تأثیر قرار می‌دهد و (۲) علت مشترک که همهٔ m جزء را تحت تأثیر قرار می‌دهد و منجر به خرابی همهٔ اجزا در یک زمان می‌شود. این توضیح به این معناست که چندگانگی هر رویداد خرابی عامل مشترک باید ۱ یا m باشد. یعنی ممکن نیست که رویدادهای خرابی عامل مشترک با چندگانگی میانی بین ۱ و m داشته باشیم. در این مدل فرض می‌شود که با وقوع خرابی عامل مشترک، تمامی اجزای گروه خراب می‌شوند و یا با وقوع علت مستقل یکی از اجزا خراب می‌شود. در این حالت خواهیم داشت:

$$Q_1^{(m)} = 1-\beta,$$
$$Q_k^{(m)} = 0,$$
$$Q_m^{(m)} = \beta,$$
$$for k = 2,3,...,m-1$$

(۱۸-۵)

مدل فاکتور بتا ساده بوده و فهم و به‌کارگیری آن آسان است. این مدل تنها یک پارامتر دارد و معنای آن پارامتر به سهولت قابل فهم است. این مدل عموماً راحت‌ترین کاربرد و استفاده را دارد و در مستند IEC 61508 یک مدل مرجّح است.

تلاش برای کاهش استعداد اجزا برای خرابی‌های عامل مشترک، پارامتر بتا را کاهش می‌دهد، اما به صورت همزمان، نرخ خرابی مستقل را تا زمانی‌که از رابطه زیر استفاده می‌شود، افزایش خواهد داد.

$$\lambda_I = (1-\beta).\lambda$$

(۱۹-۵)

هنگام استفاده از مدل فاکتور بتا، نرخ خرابی کلی λ ثابت گرفته می‌شود. به روشنی می‌توان این نکتهٔ ضعف مدل را جبران نمود، اما در عمل فراموش می‌شود.

۵-۶-۱- تعیین فاکتور بتا

فاکتور بتا را می‌توان براساس نظر متخصصین یا با استفاده از چکلیست‌ها و یا تخمین مبتنی بر داده‌های مشاهدات تعیین کرد.

در بخش ۶ ضمیمهٔ D مستند IEC 61508، یک چکلیست با ۴۰ پرسش وجود دارد که برای تعیین مقدار فاکتور بتا برای سیستم‌های ابزاردقیق ایمنی ویژهٔ یک تأسیسات به کار می‌رود. کلیهٔ پرسش‌ها، پاسخ آری یا خیر دارند. به پرسش‌ها نمرهٔ X و Y داده می‌شود. برای همهٔ پرسش‌ها با پاسخ آری، نمرات X و نمرات Y با هم جمع می‌شوند. یک جدول برای تعیین فاکتور بتا بر اساس مقدار $\sum(X_i + Y_i)$ تشکیل می‌شود و یک مقدار فاکتور بتا بین ۰/۵ تا ۵ درصد برای حل‌گرهای منطقی و بین ۱ تا ۱۰ درصد برای سنسورها و المان‌های پایانی تولید می‌شود. ۴۰ پرسش شامل موارد زیر است:

- درجهٔ جداسازی/ تفکیک فیزیکی،
- تنوّع/ افزونگی (به عنوان مثال تکنولوژی، طراحی و کارکنان نگهداری متفاوت)،
- پیچیدگی طراحی و یا بلوغ تجربیات،
- به‌کارگیری ارزیابی‌ها و تحلیل‌ها و داده‌های بازخورد،
- رویه‌ها و واسط‌های انسانی (مثلاً نگهداری و تست)،

- صلاحیت، آموزش و فرهنگ ایمنی،
- کنترل محیطی (مثلاً دما، رطوبت، دسترسی کارکنان)
- تست‌های محیطی.

۵-۶-۲- روش یکپارچهٔ بخشی (UPM)

این روش در سال ۱۹۹۶ توسط برند پیشنهاد شد و توسط زیترو و بدفورد در سال ۲۰۰۳ بیشتر توسعه یافت. این روش، روش استاندارد در صنعت هسته‌ای انگلستان است. در این روش فرض می‌شود که فاکتور بتا متأثر از هشت عامل است که هر عامل با یک وزن و یک مقدار مرتبط است. این هشت عامل عبارتند از:

- کنترل محیطی،
- تست‌های محیطی،
- تحلیل،
- فرهنگ ایمنی،
- جداسازی،
- افزونگی و تنوّع،
- فهم،
- واکنش اپراتور.

این عوامل از یکدیگر مستقل نیستند. بین فاکتور بتا و موقعیت هر عامل، یک رابطهٔ خطی فرض می‌شود:

$$\beta = \sum_{i=1}^{8} w_i . x_i \qquad (۲۰-۵)$$

در عمل، دستیابی به نتایج مشخص برای رابطه مشکل است، چراکه رویدادهای خرابی عامل مشترک کمیاب هستند و وجود یک رابطه خطی، روشن و واضح نیست. برای غلبه بر این مسأله، زیترو و بدفورد تئوری مقدار چند-مؤلفه را پیشنهاد کردند.

۵-۷- مدل فاکتور C

مدل فاکتور C اساساً همان مدل فاکتور بتا است، با این تفاوت که نرخ خرابی‌های وابسته به صورت کسری از خرابی مستقل به جای کسری از نرخ خرابی کلی تعریف می‌شود.

$$\lambda = \lambda_I + C.\lambda_I \quad (۲۱-۵)$$

این انتخاب به این معنی است که تلاش در راستای کاهش استعداد جزء در خرابی عامل مشترک، نرخ خرابی کلی را کاهش خواهد داد، برخلاف مدل فاکتور بتا که باعث افزایش نرخ خرابی مستقل می‌شد.

۵-۸- مدل پارامتر پایه

یک سیستم با سه جزء را در نظر بگیرید. E_i رویدادی است که جزء i در حالت خراب قرار دارد. احتمال اینکه جزء ۱ در اثر همهٔ علل خراب شود عبارت است از:

$$q(E_1) = q\left[E_1^i \cup (E_1^c \cap E_2^c) \cup (E_1^c \cap E_3^c) \cup (E_1^c \cap E_2^c \cap E_3^c)\right] \quad (۲۲-۵)$$

رابطه فوق به این معنی است که خرابی جزء ۱ می‌تواند یک خرابی مستقل و یا خرابی چندگانه ۲ یا ۳ جزئی از نوع خرابی عامل مشترک باشد. برای جزء ۲ و ۳ نیز رابطه مشابهی بدست می‌آید.

$$Q_1^{(3)} = q(E_1^i) = q(E_2^i) = q(E_3^i) \quad (۲۳-۵)$$

$$Q_2^{(3)} = q(E_1^c \cap E_2^c) = q(E_1^c \cap E_3^c) = q(E_2^c \cap E_3^c) \quad (۲۴-۵)$$

$$Q_3^{(3)} = q(E_1^c \cap E_2^c \cap E_3^c) \quad (۲۵-۵)$$

$Q_{i:3}$ احتمال خرابی چندگانهٔ i جزء در یک سیستم سه جزئی است.

در این مدل با فرض تقارن، احتمال کلی خرابی همهٔ ترکیبات یک جزء مشخص در یک سیستم سه جزئی برابر است با:

$$Q_t = Q_1^{(3)} + 2.Q_2^{(3)} + Q_3^{(3)} \quad (۲۶-۵)$$

برای یک سیستم با m جزء، رابطه احتمال کلی خرابی همهٔ ترکیبات یک جزء به صورت زیر خواهد بود:

$$Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_k^{(m)} \quad (۲۷-۵)$$

در این رابطه، $\binom{m-1}{k-1}$ تعداد حالت‌های مختلفی است که یک جزء مشخص می‌تواند به همراه $k-1$ جزء دیگر در یک گروه m جزئی قرار گیرد.

مصلح و همکاران در سال ۱۹۸۸ نشان داده است هنگامی‌که $Q_k^{(3)}$ مبتنی بر نیاز باشد، تخمین احتمال بیشینه برابر خواهد بود با:

$$\hat{Q}_k^{(m)} = \frac{n_k}{N_k} \qquad (۲۸-۵)$$

n_k تعداد رویدادهای خرابی شامل k خرابی جزء و N_k تعداد نیازها به همهٔ k جزءها در گروه اجزای عامل مشترک است.

اگر همهٔ m جزء در هر زمانی که سیستم در حالت کار باشد، مورد نیاز باشند و N_D تعداد نیازها باشد، آنگاه تعداد نیازها به k جزء از این گروه، برابر است با:

$$N_k = \binom{m}{k} N_D \qquad (۲۹-۵)$$

مقدار $\binom{m}{k}$ برابر تعداد گروه‌های kجزئی که می‌توانند از m جزء تشکیل شوند، می‌باشد.

$$\hat{Q}_k^{(m)} = \frac{n_k}{\binom{m}{k} N_D} \qquad (۳۰-۵)$$

۵-۹- مدل فاکتور آلفا

$\alpha_k^{(m)}$: درصدی از رویدادهای خرابی که در یک گروه m جزئی روی می‌دهند و شامل خرابی دقیقاً k جزء در اثر عامل مشترک هستند، با عنوان فاکتور آلفا لحاظ می‌شوند.

به عنوان مثال، اگر $\alpha_2^{(m)}$ برابر ۰/۰۵ باشد، به این معنی است که ۵ درصد همهٔ رویدادهای خرابی در یک گروه m جزئی، یک خرابی عامل مشترک با چندگانگی برابر ۲ (خرابی دو جزء) است.

فاکتور آلفا را می‌توان از رابطه زیر محاسبه کرد:

$$\alpha_k^{(m)} = \frac{\binom{m}{k} . Q_k^{(m)}}{\sum_{j=1}^{m} \binom{m}{j} . Q_j^{(m)}} \qquad (۳۱-۵)$$

در این رابطه، عبارت صورت کسر برابر احتمال وقوع رویدادهای خرابی شامل دقیقاً k جزء است و عبارت مخرج کسر، مجموع احتمال همهٔ رویدادها است.

بنابراین، $\alpha_k^{(m)}$ احتمال شرطی یک خرابی عامل مشترک با چندگانگی k است که در یک گروه m جزئی رخ می‌دهد. برای یک گروه سه جزئی خواهیم داشت:

$$\alpha_1^{(3)} = \frac{3.Q_1^{(3)}}{3.Q_1^{(3)} + 3.Q_2^{(3)} + Q_3^{(3)}} \quad (۳۲-۵)$$

$$\alpha_2^{(3)} = \frac{3.Q_2^{(3)}}{3.Q_1^{(3)} + 3.Q_2^{(3)} + Q_3^{(3)}} \quad (۳۳-۵)$$

$$\alpha_3^{(3)} = \frac{Q_3^{(3)}}{3.Q_1^{(3)} + 3.Q_2^{(3)} + Q_3^{(3)}} \quad (۳۴-۵)$$

$$\alpha_1^{(3)} + \alpha_2^{(3)} + \alpha_3^{(3)} = 1 \quad (۳۵-۵)$$

۵-۱۰- نوع دیگری از مدل فاکتور آلفا

احتمال خرابی k جزء در گروه خرابی عامل مشترک، به چگونگی تست اجزا وابسته است. برای تست همزمان این احتمال برابر است با:

$$Q_k^{(m)} = \frac{k}{\binom{m-1}{k-1}} . \frac{\alpha_k^{(m)}}{\alpha_t} . Q_t = \frac{m}{\binom{m}{k}} . \frac{\alpha_k^{(m)}}{\alpha_t} . Q_t \quad (۳۶-۵)$$

$$\alpha_t = \sum_{k=1}^{m} k . \alpha_k^{(m)} \quad (۳۷-۵)$$

هنگامی که فاکتور آلفا کسری از همهٔ رویدادهای خرابی که شامل دقیقاً k جزء باشد، می‌توان آن را به صورت زیر به دست آورد:

$$\alpha_k^{(m)} = \frac{n_k}{\sum_{j=1}^{m} n_j} \quad (۳۸-۵)$$

بنابراین برای بدست آوردن احتمال $Q_k^{(m)}$ ، تنها باید Q_t و n_k مشخص باشند.

۵-۱۱- مقابله با خرابی‌های عامل مشترک

برای مقابله با خرابی‌های عامل مشترک اقدامات زیر قابل انجام است:

- تنوع اجزا،

- جداسازی اجزا،
  - حفاظ‌های فیزیکی،
  - محفظه‌های فیزیکی،
  - جداسازی فیزیکی.
- محدوده‌های طراحی اجزا،
- جلوگیری از خطای انسانی.

۶- تحلیل مودهای خرابی و اثرات آنها[۱]

۶-۱- معرفی و جایگاه

تحلیل مودهای خرابی و اثرات آنها ابزاری است که در صنایع مختلف به منظور شناسایی خرابی‌ها، ارزش‌گذاری اثرات خرابی‌ها و اولویت‌بندی خرابی‌ها بر اساس وخامت اثرات به کار می‌رود.

اولویت‌بندی یا طبقه‌بندی ریسک عمدتاً با استفاده از دو روش ماتریس ریسک (درجهٔ اولویت ریسک) و تحلیل بحرانیت[۲] انجام می‌شود.

دلایل استفاده از تحلیل مودهای خرابی و اثرات آنها عبارتند از:

- شناسایی حالت‌های حادثه خاص،
- لحاظ پیشرفت‌های ایمنی جایگزین،
- جمع‌آوری داده‌ها برای تحلیل ریسک کمّی،
- ارزش‌گذاری ریسک‌های حاصل از طراحی‌ها و رویّه‌های عملکردی اولیه،
- ارتقای قابلیت اطمینان فرایند،
- برقراری الزامات مقرراتی،
- مستندسازی یک ارزیابی مخاطرات فرایند سیستماتیک،
- ارزش‌گذاری فرایندهای پیچیده در جایی‌که ریسک‌های مشاهده شده قابل توجه است،
- شناسایی خرابی‌های تک نقطه‌ای.

شاخصه‌های تحلیل مودهای خرابی و اثرات آنها به صورت زیر است:

- به‌کارگیری و اجرای تحلیل مودهای خرابی و اثرات آنها به محض آماده شدن طراحی‌های اولیه، تضمین کنندهٔ قابلیت انجام تغییرات ضروری طراحی در زودترین زمان ممکن می‌باشد؛
- فایدهٔ تحلیل مودهای خرابی و اثرات آنها در ممانعت از وقوع خرابی‌ها در آینده است. بنابراین، معمولاً این تحلیل در فاز طراحی انجام می‌شود، زمانی‌که هنوز مودهای خرابی، جزئی از فرایند نیستند؛

---

[۱] - Failure Mode and Effect Analysis (FMEA)
[۲] - Failure Mode and Effect Criticality Analysis (FMECA)

- یک تحلیل خوبِ مودهای خرابی و اثرات، یک فرایند مداوم و پیوسته است که به موجب آن به صورت پیوسته در طول عمر فرایند به‌روزرسانی و ویرایش می‌شود.

جامعه هدف تحلیل مودهای خرابی و اثرات آنها عبارت است از:

- تجهیزات مکانیکی مانند پمپ‌ها، چگالنده‌ها و غیره که یک تاریخچه خرابی‌های اجزا دارند؛
- سیستم‌هایی که نقشه‌ها و جزئیات کمی دارند ولی اجزای مجزای آنها به آسانی قابل شناسایی است؛
- مطالعات قابلیت اطمینان و یا برای ورودی مطالعات ارزیابی ریسک کمّی.

عموماً در مقررات پیشنهاد می‌شود که در تحلیل مودهای خرابی و اثرات آنها، موارد زیر، رسیدگی و انجام شوند:

- یافتن اشتباهات،
- اقدامات اصلاحی،
- مستندسازی،
- ایمنی و سلامت،
- مدیریت تغییرات،
- استفاده نادرست و یا بی‌ملاحظه،
- مسائل قابلیت بهره‌برداری،
- پیش‌گیری،
- مخاطرات فرایند،
- اجرای مقررات،
- مدیریت ریسک.

استانداردهایی که به صورت ویژه شامل روش‌های تحلیل مودهای خرابی و اثرات آنها می‌شوند، عبارتند از:

3. MIL STD 1629,
4. SAE ARP5580,
5. SAE J1739.

سایر استانداردهای مرتبط عبارتند از:

- AIAG, APQP Manual,
- FDA, GMP, QS Regulation Title 21, CFR Part 820,
- ISO 9001 2000,
- IATF, ISO/TS 16949,
- PSM CFR 1910,119,
- QS 9000.

۶-۲- واژه‌شناسی تحلیل مودهای خرابی و اثرات آنها

- علل: به دلایل ریشه‌ای مود خرابی بالقوّه گفته می‌شود. به عنوان نمونه تنش بیش از حد، افزایش غیرقابل کنترل دما، ضخامت ناصحیح یک دیوار می‌توانند از جمله علل خرابی بالقوّه باشند؛
- بحرانیت: مقیاسی از پیامدهای یک مود خرابی که توسط وخامت و احتمال وقوع آن تعیین می‌شود (این پیامدها از نوع داده‌های نرخ خرابی واقعی گذشته هستند). تحلیل بحرانیت، رویه‌ای است که در آن این مقیاس به دست می‌آید. به جای درجه‌بندی ریسک با استفاده از ماتریس ریسک، و یا روش شمارهٔ اولویت ریسک، پارامترهای خاصی به نام بحرانیت‌های جزء و مود خرابی (به ترتیب C_r و C_m)، محاسبه شده و برای اولویت‌بندی استفاده می‌شوند؛
- کنترل‌های کنونی: حفاظ‌های موجود یا کنترل‌های مهارکننده‌ای که درحال حاضر به کار رفته‌اند؛
- آشکارسازی: قابلیت شناسایی خرابی پیش از تأثیر خرابی بر هدف است. سطوح آشکارسازی که همان سطوح وقوع و وخامت هستند، یک مقدار اختیاری برای محاسبه درجهٔ اولویت ریسک تعیین می‌کنند؛
- اثرات: پیامدهای مودهای خرابی بر اهداف مختلف مانند عملکرد سیستم، افراد، محیط و غیره است.
- مود خرابی: چگونگی امکان خرابی یک جزء در انجام عملکرد طراحی منظور است. مودهای خرابی شامل فعل‌هایی مانند خرابی باز/ بسته شدن، ترک برداشتن، کوچکتر/ بزرگتر از معمول بودن و ... است؛
- احتمال وقوع: فرکانس خرابی (حاصل از سالیان گذشته) برای فرایند و یا بخشی از فرایند مورد مطالعه است؛
- درجهٔ اولویت ریسک: ماتریس ریسک، اطلاعات کیفی را با تعریف درجهٔ اولویت ریسک کمّی می‌سازد. درجهٔ اولویت ریسک با ضرب وخامت، احتمال وقوع و آشکارسازی به دست می‌آید. مقادیر وخامت، وقوع و آشکارسازی به صورت اختیاری تعریف می‌شوند و باید همواره بزرگتر از صفر باشند. درجهٔ اولویت ریسک به خودی خود هیچ معنایی ندارد و تنها برای اولویت‌بندی اقدامات بعدی به کار می‌رود؛
- خرابی تک‌نقطه‌ای: یک جزء یا اِلمانی که خرابی آن می‌تواند منجر به خرابی سیستم شود، خرابی تک نقطه‌ای نامیده می‌شود؛

- وخامت: مقیاسی از درجهٔ آسیب یک مود خرابی است که بر اهداف مختلف وارد می‌شود. وخامت می‌تواند تنها از طریق تغییر در طراحی کاهش یابد؛

۶-۳- انواع مختلف تحلیل مودهای خرابی و اثرات آنها

طبیعت مطالعه و مراحل سیکل عمر فرایند، نوع تحلیلی که باید برای مودهای خرابی و اثرات آنها به‌کار رود را تعیین می‌کند. ۶ نوع مختلف برای تحلیل مودهای خرابی و اثرات آنها به نام تحلیل ماشینی، تحلیل طراحی، تحلیل سیستم، تحلیل فرایند، تحلیل کاربردی و تحلیل محصول وجود دارد. همه انواع تحلیل مودهای خرابی و اثرات، یک رویکرد را دنبال می‌کنند. طبیعت، هدف و دامنهٔ مطالعه، تعیین می‌کند که کدام نوع از تحلیل و با چه میزان از جزئیات باید استفاده شود. اغلب فرایندها، تجهیزات، طراحی‌ها می‌توانند به سطوح سیستم‌ها، زیرسیستم‌ها، مجتمع‌ها، زیرمجتمع‌ها، اجزا، بخش‌ها و غیره قابل شکستن هستند. شکست موضوع مطالعه، به تعریف دامنه کمک می‌کند.

۶-۳-۱- مراحل انجام تحلیل

مراحل انجام تحلیل مودهای خرابی و اثرات آنها به صورت زیر است:

- جمع‌آوری اطلاعات، مانند نقشه‌های سایت، اطلاعات عملکردی، رویه‌ها، داده‌های مربوطه، نقشه‌های طراحی و ...،
- پایه‌ریزی هدف، دامنه، عمق مطالعه، هزینه‌های مربوطه، تخصص، تجربه موجود و ...،
- شکست سیستم به اجزای منطقی و قابل مدیریت براساس عملکرد (سیستم سرمایش، سیستم توقف، پمپاژ، مبدل‌های حرارتی) و یا موقعیت مکانی (بخش پایین برج تقطیر، بخش بالای برج، سیستم خط تغذیه، سیستم خط تولید) و ثبت این اطلاعات در جدول‌های تحلیل،
- شناسایی همهٔ مودهای خرابی بالقوّه برای هر جزء،
- تعیین علل هر مود خرابی،
- شناسایی و لیست‌کردن کنترل‌های فعلی،
- تخصیص یک درجه (نمره) برای وخامت، وقوع و حذف هر خرابی،
- تعیین اقدامات اصلاحی مناسب،
- انجام اقدامات پیشنهادی.

۶-۴- اولویت‌بندی ریسک‌ها

تا زمانی‌که منابع کمیاب هستند، اولویت‌بندی به تمرکز بر اقدامات ضروری کمک می‌کند. وخامت ریسک تحمیلی و دامنهٔ کاهش ریسک دو معیار عمومی برای اولویت‌بندی هستند.

۶-۴-۱- دسته‌بندی ریسک با استفاده از ماتریس ریسک

برای وخامت، مقادیر قراردادی تعیین می‌شوند. به عنوان مثال، در جدول شماره ۲۲ نمونهٔ دسته‌بندی وخامت ارائه شده است.

جدول شماره ۲۲: نمونهٔ دسته‌بندی وخامت

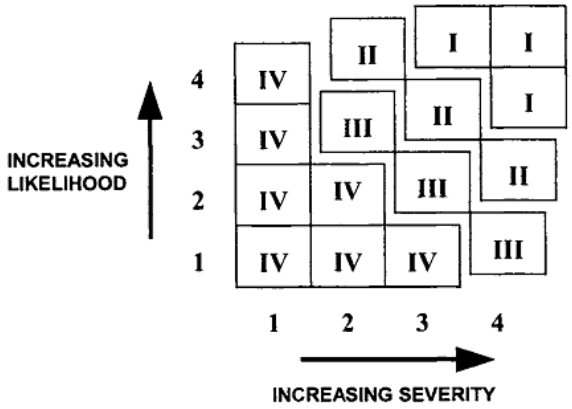
شماره	توضیح
۱	بدون اثرات صدمه‌ای و یا بهداشتی
۲	صدمه کم و یا اثرات بهداشتی کم
۳	صدمه و یا اثرات بهداشتی متوسط
۴	مرگ و یا اثرات بهداشتی وخیم

برای احتمال وقوع نیز، مقادیر قراردادی تعیین می‌شوند. در جدول شماره ۲۳ نمونهٔ دسته‌بندی احتمال وقوع و شماره تخصیص داده شده ارائه شده است.

جدول شماره ۲۳: نمونهٔ دسته‌بندی احتمال وقوع

شماره	توضیح
۱	عدم انتظار وقوع طی طول عمر تأسیسات
۲	انتظار وقوع کمتر از یک بار در طول عمر تأسیسات
۳	انتظار وقوع چندبار طی طول عمر تأسیسات
۴	انتظار وقوع بیش از یک بار در سال

ماتریس ریسک با استفاده از پارامترهای مشابه جدول شماره ۲۲ و جدول شماره ۲۳ توسعه می‌یابد. همانگونه که در شکل ۶۹ مشاهده می‌شود، ماتریس ریسک حاوی دو محور افقی و عمودی است. محور افقی، میزان وخامت و محور عمودی، احتمال وقوع را نشان می‌دهد. در مقدار هر درایهٔ ماتریس نیز میزان ریسک تعیین شده است. دسته‌های دسته‌بندی ریسک از پیش تعریف‌شده می‌باشد. به عنوان نمونه، در جدول شماره ۲۴ دسته‌بندی میزان ریسک تعیین شده است.



شکل ۶۹: نمونهٔ ماتریس ریسک

جدول شماره ۲۴: نمونهٔ دسته‌های دسته‌بندی ریسک

شماره	دسته	اقدامات
۱	غیرقابل پذیرش	باید با اقدامات مهندسی و یا کنترل‌های اجرایی به دستهٔ سوم ریسک مهار شوند در دورهٔ زمانی خاص مانند ۶ ماه
۲	نامطلوب	باید با اقدامات مهندسی و یا کنترل‌های اجرایی به دستهٔ سوم ریسک مهار شوند در دورهٔ زمانی خاص مانند ۱۲ ماه
۳	قابل پذیرش با کنترل‌ها	باید رویه‌ها و یا کنترل‌ها لحاظ شوند.
۴	قابل پذیرش	نیاز به مهار نیست.

۶-۴-۲- شمارهٔ اولویت ریسک[۱]

شمارهٔ اولویت ریسک با یک ضرب ساده مقادیر وخامت S در احتمال وقوع O و آشکارسازی D محاسبه می‌شود. معمولاً شرکت‌ها مقادیر کمینه برای شمارهٔ اولویت ریسک، به عنوان استاندارد خود منتشر می‌کنند. هر شمارهٔ اولویت ریسک که بزرگتر از مقدار کمینه باشد، می‌تواند مطالعهٔ بیشتر را تضمین کرده و هر مقدار کمتر به صورت ایمن، و یا ریسک قابل قبول، و یا اولویت بسیار پایین برای تحلیل بیشتر لحاظ شود. مثال‌های مقادیر وخامت، وقوع و آشکارسازی در جدول شماره ۲۵، جدول شماره ۲۶ و جدول شماره ۲۷ به ترتیب ارائه شده است.

جدول شماره ۲۵: نمونهٔ مقادیر وخامت به کار رفته در محاسبهٔ شماره اولویت ریسک

اثر	شماره	معیار
بدون اثر	۱	می‌تواند مورد توجه اپراتور (فرایند) قرارگیرد. غیرمحتمل و یا غیرقابل توجه از لحاظ کاربر (محصول).
بسیار خفیف	۲	بدون اثر پایین‌دستی (فرایند). اثر غیرمهم و یا قابل صرف‌نظر (محصول).

[۱] - Risk Priority Number (RPN)

خفیف	۳	ممکن است کاربر اثر آن را متوجه شود، ولی اثر خفیف است. (فرایند و محصول)
کم	۴	فرایندهای محلی و یا پایین‌دستی می‌تواند تحت تأثیر قرار گیرد (فرایند). کاربر اثر منفی کمی بر محصول تجربه خواهد کرد (محصول).
متوسط	۵	اثرات طی بهره‌برداری قابل توجه خواهد بود. عملکرد به صورت تدریجی کاهش یافته و عدم رضایت کاربر (محصول).
وخیم	۶	شکست فرایند پایین‌دستی (فرایند). محصول قابل کار کردن و ایمنی است ولی عملکرد آن تنزل می‌یابد. عدم رضایت کاربر (محصول).
وخامت زیاد	۷	مدت تعطیلی قابل توجه (فرایند). عملکرد محصول به صورت وخیمی متأثر می‌شود. نارضایتی کاربر (محصول).
وخامت بسیار زیاد	۸	مدت تعطیلی قابل توجه و اثرات مالی عمده (فرایند). محصول کار نمی‌کند ولی ایمن است. کاربر بسیار ناراضی است (محصول).
وخامت نهایی	۹	خرابی منجر به اثرات خطرناک بسیار محتمل است. ایجاد نگرانی‌های ایمنی و مقرراتی (فرایند و محصول)
وخامت بیشینه	۱۰	صدمه و یا آسیب متوجه اپراتور (فرایند). خرابی منجر به اثرات خطرناک به صورت تقریباً قطعی. عدم تطابق با مقررات دولتی (محصول).

جدول شماره ۲۶: نمونهٔ مقادیر درجهٔ وقوع به کار رفته در محاسبهٔ شماره اولویت ریسک

وقوع	درجه	معیار
حد نهایی احتمال عدم وقوع	۱	خرابی به میزان زیادی غیر محتمل است
احتمال بعید	۲	مقدار نادر برای احتمال خرابی
احتمال بسیار کم	۳	خرابی بسیار کم محتمل است.
احتمال کم	۴	احتمال خرابی کم است.
احتمال میانهٔ کم	۵	خرابی به صورت گاه و بیگاه محتمل است.
احتمال متوسط	۶	احتمال خرابی متوسط است.
احتمال میانهٔ زیاد	۷	احتمال خرابی میانهٔ زیاد است.
احتمال زیاد	۸	احتمال خرابی زیاد است.
احتمال بسیار زیاد	۹	احتمال خرابی بسیار زیاد است.
حد نهایی احتمال وقوع	۱۰	خرابی تقریباً قطعی است.

جدول شماره ۲۷: نمونهٔ درجهٔ آشکارسازی به کار رفته در محاسبهٔ شمارهٔ اولویت ریسک

آشکارسازی	درجه	معیار
حد نهایی احتمال	۱	کنترل‌ها تقریباً به صورت قطعی وجود عیب را آشکار خواهند کرد.
احتمال بسیار بالا	۲	به حتمال بسیار بالا کنترل‌ها وجود عیب را آشکار می‌کنند.
احتمال بالا	۳	وجود اثربخشی بالا برای آشکارسازی
احتمال میانهٔ بالا	۴	وجود اثربخشی میانهٔ بالا برای آشکارسازی
احتمال متوسط	۵	وجود اثربخشی متوسط برای آشکارسازی
احتمال میانهٔ پایین	۶	وجود اثربخشی میانهٔ پایین برای آشکارسازی

احتمال پایین	۷	وجود اثربخشی پایین برای آشکارسازی
احتمال بسیار پایین	۸	وجود پایین‌ترین اثربخشی برای آشکارسازی
احتمال نادر	۹	کنترل‌ها دارای احتمال بسیارپایین در آشکارسازی وجود عیب هستند.
حد نهایی عدم احتمال	۱۰	تقریباً به صورت قطعی کنترل‌ها وجود عیب را آشکار نمی‌کنند.

۶-۵- کاربرگ تحلیل مودها خرابی

قالب کاربرگ تحلیل مودهای خرابی و اثرات آنها شامل موارد زیر است:

- مودهای خرابی بالقوّه،
- علل بالقوّه مودهای خرابی،
- اثرات بالقوّه مودهای خرابی،
- کنترل‌ها جاری (حفاظ‌های موجود)،
- وخامت،
- وقوع/ احتمال،
- آشکارسازی،
- درجه‌بندی ریسک، شماره اولویت ریسک و یا تحلیل بحرانیت،
- توصیه‌ها و اقدامات اصلاحی،
- مسئولیت،
- تاریخ تکمیل هدف،
- اقدامات اتخاذشده،
- درجه‌بندی جدید ریسک، شماره اولویت ریسک و یا نتایج تحلیل بحرانیت،
- پیغام‌ها.

طبقه‌بندی مودهای خرابی بر وخامت همراه با احتمال وقوع، مبتنی است. تحلیل بحرانی، اول نیاز به محاسبه درجهٔ بحرانیت مود خرابی دارد:

$$C_m = \beta\alpha\lambda_p t \qquad (۱-۶)$$

در این رابطه، β احتمال شرطی شکست مأموریت، α نسبت مود خرابی، λ_p نرخ خرابی جزء و t مدت زمان عملکرد (ساعت) و یا تعداد سیکل‌های عملکردی است.

سپس درجهٔ بحرانیت یک جزء با استفاده از رابطه زیر به دست می‌آید.

$$C_r = \sum_{n=1}^{j} (C_m)_j \qquad (۲-۶)$$

یک ماتریس بحرانیت از پارامترهای C_r برحسب دسته‌های بحرانیت ساخته می‌شود. این ماتریس، همانند روش ماتریس ریسک، به تعیین اولویت اقدام کمک می‌کند.

۶-۶- روش‌شناسی تحلیل بحرانیت مودهای خرابی

در روش‌شناسی تحلیل بحرانیت مودهای خرابی اقدامات زیر انجام می‌شود:

- تعریف فرایند و یا سیستمی که باید تحلیل شود،
- شناسایی همهٔ مودهای خرابی بالقوّه، و تخصیص اثرات به مودهای خرابی و وخامت به اثرات،
- وارد کردن داده‌های مود خرابی مانند روش‌های شناسایی خرابی، و نرخ‌های خرابی،
- استفاده از وخامت و بحرانیت برای درجه‌بندی مودهای خرابی،
- برجسته‌سازی و گزارش کردن خرابی‌های بحرانی،
- کاهش خرابی‌های بحرانی با به کارگیری اقدامات اصلاحی.

۶-۷- مزایای FMEA و FMECA

- ایجاد تصویری بهتر از یک شرکت و رقابت‌پذیری،
- برآوردن مقررات، استانداردها و خصوصیات،
- ارتقای پیوستهٔ کیفیت محصولات، قابلیت اطمینان و ایمنی،
- تعریف اقدامات اصلاحی،
- مستندسازی دلایل تغییرات،
- قابلیت اطمینان، قابلیت تولید، کیفیت، ایمنی و بازدهی اقتصادی ارتقایافته،
- افزایش رضایت مشتری،

- شناسایی و ارزشیابی خرابی‌های بالقوّه و اثرات آنها،
- کاهش زمان توقف کار،
- کاهش انحرافات فرایند ساخت،
- انتخاب مواد، اجزا، وسایل، بخش‌ها و مأموریت‌های جایگزین،
- انتخاب طراحی سیستم بهینه.

۶-۸- نواقص FMEA و FMECA

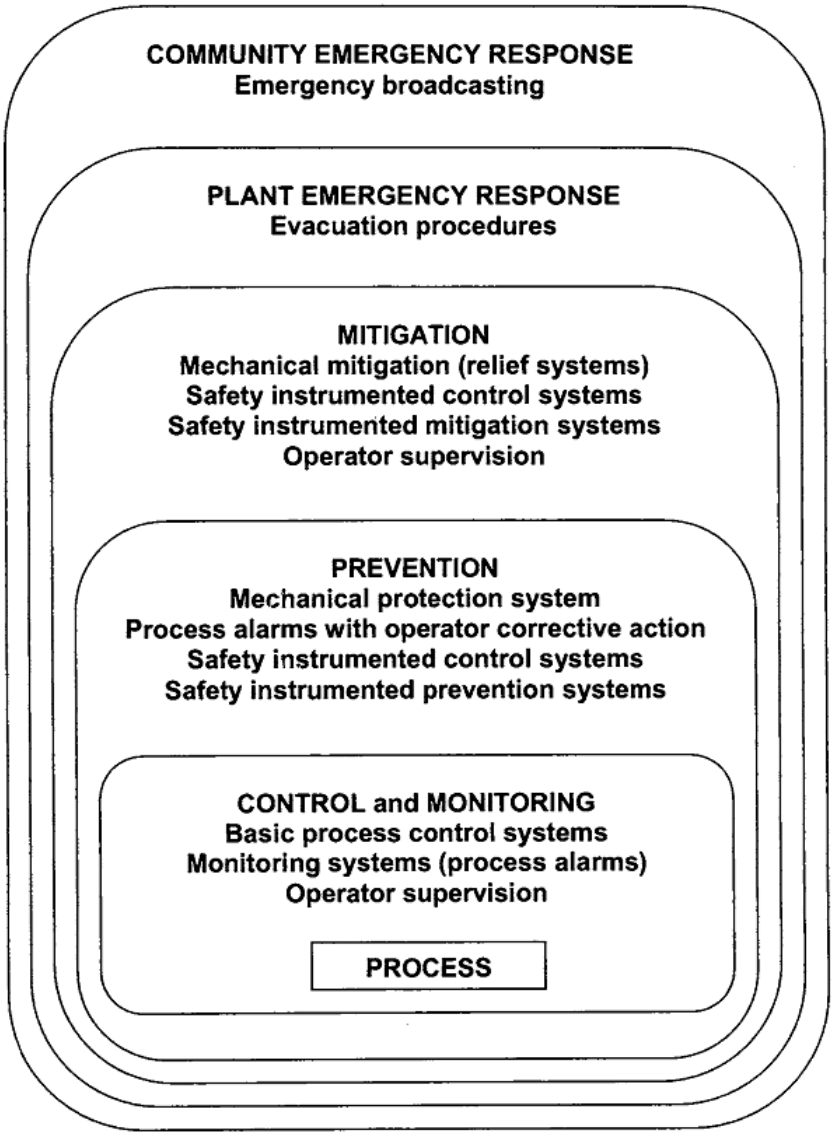
۱. در این روش‌ها خطاهای انسانی و اثرات محیطی به سادگی چشم‌پوشی می‌شوند.
۲. این روش‌ها منحصر در خرابی‌های تک نقطه‌ای بوده و در آن‌ها خرابی‌های چندنقطه‌ای چشم‌پوشی می‌شوند.
۳. این روش‌ها برای فرایندهای بزرگ و پیچیده به غایت ملال‌آور هستند.
۴. تکمیل موفقیت‌آمیز این تحلیل‌ها مستلزم تخصص، تجربه و مهارت خوب است.
۵. این روش‌ها می‌توانند پرهزینه و زمان‌بر باشند.
۶. در تحلیل بحرانیت، به دست آوردن نرخ‌های خرابی گذشته، مشکل است.

۷- تحلیل لایه‌های حفاظت[۱]

۷-۱- تحلیل لایه‌های حفاظت چیست؟

مبحث تحلیل لایه‌های حفاظت، این مفهوم را ارائه می‌کند که محافظت در برابر پیامد نامناسب یا وخیم مانند آتش‌سوزی، تنها به سادگی در یک سطح یا لایه محدود نیست و احتمالاً سطوح یا لایه‌های چندگانه از حفاظت وجود دارد. در شرایط آتش‌سوزی، سیستم خاموش‌سازی اضطراری یک لایه را تشکیل می‌دهد؛ سیستم تخلیه فشار و زبانه کشیدن شعله یک لایه دیگر را تشکیل می‌دهد؛ سیستم حفاظتی غرق‌سازی یک لایه دیگر را تشکیل می‌دهد؛ سیستم پاسخ اضطراری یک لایهٔ دیگر و .... تحلیل این لایه‌ها مربوط به مبحث تحلیل لایه‌های حفاظت است. در شکل ۷۰ برخی لایه‌های حفاظت برای یک فرایند ارائه شده است.

[۱] - LOPA



شکل ۷۰: لایه‌های عمومی برای فرایند حفاظت در تأسیسات فرایند (IEC 61511, 2003)

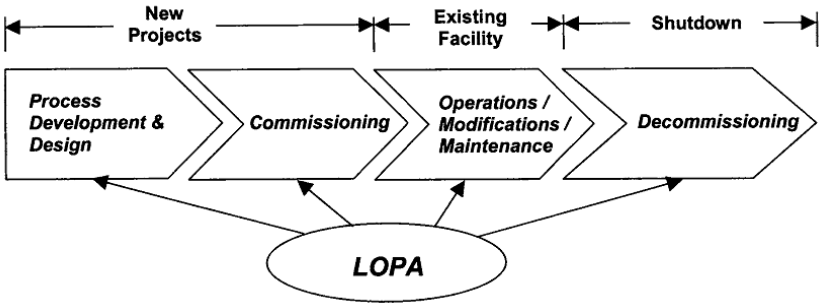
تحلیل لایه‌های حفاظت یک روش تحلیل ریسک نیمه کمّی است که برای ارزشیابی ریسک یک سناریوی خطرناک منتخب با تعیین یک تخمین اندازه از ریسک استفاده می‌شود. نیمه کمّی بودن این تحلیل به دلیل نیاز به ورودی‌های کمّی مانند فرکانس رویداد و احتمال خرابی است که به منظور فراهم کردن تخمین ریسک محافظه‌کارانه انتخاب می‌شوند.

سپس ریسک تخمین زده شده با معیار ریسکِ قابل تحمل که توسط توسط کارخانه تولید کننده تعیین می‌شود، مقایسه می‌شود. سپس تصمیم گرفته می‌شود که آیا لایه‌های حفاظت موجود کافی هستند و یا کاهش بیشتر ریسک مورد نیاز است. بدون لحاظ معیار ریسکِ قابل تحمل، تمایل به افزودن اقدامات مهارکنندهٔ ریسک با این باور که ایمنی بیشتری ایجاد می‌شود، وجود دارد. افزودن اقدامات مهارکنندهٔ ریسکِ بیشتر ممکن است ایمنی بیشتر را فراهم کند، اما در برخی مراحل ممکن است

به طور قابل توجهی هزینهٔ بیشتری بدون افزودن مهار قابل توجه، اضافه کند. همچنین اقدامات مهارکننده‌ای ممکن است اضافه شوند که غیرضروری بوده و باعث افزایش پیچیدگی تأسیسات شود که منجر به سناریوهای خطر تعریف‌نشدهٔ جدید بالقوّه می‌شوند. تحلیل لایه‌های حفاظت به تمرکز بر منابع محدود در اغلب اقدامات مهارکننده و ممانعت‌کنندهٔ ریسک بحرانی کمک می‌کند.

۷-۲- تحلیل لایه‌های حفاظت و سیکل عمر فرایند

تحلیل لایه‌های فرایند می‌تواند در طول سیکل عمر یک فرایند، کاربردی باشد. شکل ۷۱ فازهای اصلی در سیکل عمر فرایند را نشان می‌دهد.



شکل ۷۱: چگونگی تطبیق سیکل عمر فرایند در تحلیل لایه‌های حفاظت

برخی کاربردهای تحلیل لایه‌های حفاظت در فازهای مختلف عبارتند از:

۱. توسعهٔ فرایند و طراحی

سیستم حفاظت در برابر فشار زیاد – تحلیل لایه‌های حفاظت می‌تواند لایه‌های مستقل حفاظت موجود و احتمال خرابی آنها را تعیین نماید. این کار برای کمک به تعریف حالت کنترل‌کننده برای پایهٔ طراحی سیستم اطمینان برای تعیین اندازهٔ ابزارهای اطمینان فشار هنگامی که از استاندارد ASME Code 2211 با عنوان «حفاظت در برابر فشار زیاد با طراحی سیستم» و یا استاندارد API 520 «تعیین اندازه، انتخاب و نصب ابزارهای اطمینان فشار برای پالایشگاه‌ها» استفاده می‌شود، به کار می‌رود.

تعیین سطوح یکپارچگی ایمنی[1] هدف – تحلیل لایه‌های حفاظت یک روش توصیه‌شده برای تعیین سطح یکپارچگی ایمنی هدف برای یک اقدام ابزارمند ایمنی[2] است.

ارزش‌یابی گزینه‌های طراحی فرایند – تحلیل لایه‌های حفاظت می‌تواند برای آزمایش گزینه‌های طراحی پایه و انتخاب طراحی‌هایی که فرکانس‌های رویدادهای آغازگر کمتری دارند، یا پیامدهای کمتری دارند، به‌کار رود. این تحلیل به طراحی فرایندهای ایمن به صورت ذاتی با مقایسهٔ سریع و بی‌طرفانهٔ طراحی‌های مختلف کمک می‌کند.

برنامه‌ریزی هزینهٔ ایمنی – روش تحلیل لایه‌های حفاظت یکپارچه با یک روش هزینه- فایده، به تصمیم‌گیری و انتخاب سدها حفاظتی کمک می‌کند. این روش، به فهم مزایای اقتصادی کاهش ریسک و تخصیص اولویت منابع و مقایسه پروژه‌های مختلف کمک می‌کند.

سیستم‌های ایزوله‌سازی اضطراری – تحلیل لایه‌های حفاظت برای ارزشیابی نیاز به سیستم‌های ایزوله‌سازی در فرایندهایی که در آنها شرایط نقص در محدود نگهداشتن، به عنوان مثال نشت در سیستم خطوط لوله، می‌تواند رخ دهد، به کار می‌رود.

۲. ساخت/ بهره‌برداری/ نگهداری/ ارتقا

ارزشیابی فاکتورهای انسانی طی روشن‌سازی – تحلیل لایه‌های حفاظت می‌تواند برای آزمایش سناریوهای خرابی مرتبط با انسان طی فرایندهای روشن‌سازی سیستم به کار رود.

سیستم‌های ایمنی کنارگذر – تحلیل لایه‌های حفاظت به تعیین اینکه آیا یک سیستم ایمنی لایهٔ مستقل حفاظت بحرانی می‌تواند به صورت موقت برای دورهٔ زمانی کوتاهی از سرویس خارج شود؟ و اینکه چه لایه‌های اضافی حفاظت می‌تواند نیاز باشد؟ کمک می‌کند.

مدیریت تغییر – تحلیل لایه‌های حفاظت، وظایف ایمنی درگیر در ارتقای فرایندها، رویه‌ها، تجهیزات، ابزارها و ... را تعیین می‌کند و تطابق ارتقای صورت گرفته با معیارهای ریسک قابل تحمل را مشخص می‌کند.

[1] - Safety Integrated Levels (SIL)
[2] - Safety Instrumented Function (SIF)

برنامه‌های یکپارچگی مکانیکی – تجهیزات ایمنی بحرانی، فرایند را در معیار ریسک میانهٔ تعیین شده توسط سازمان‌ها نگه می‌دارند. تحلیل لایه‌های حفاظت می‌تواند به میزان قابل توجهی نیاز به تجهیزات ایمنی بحرانیِ اضافی را کاهش دهد. چراکه یک رویکرد فوقِ محافظه‌کارانه در ایمنی می‌تواند منجر به شمار زیادِ غیرمعقولی از این تجهیزات شود که می‌تواند اثر شدیدی بر هزینه‌ها در تأسیسات جدید و تعمیرشده داشته باشد.

آموزش ایمنی و راهنمای بهره‌برداری – تحلیل لایه‌های حفاظت می‌تواند اقدامات و عکس‌العمل‌های اپراتور را که برای ایمنی فرایند بحرانی است، شناسایی نماید. این امر، به تعریف بهتر آموزش و آزمایش مورد نیاز طی عمر فرایند و نیز به ارتقای وضوح دستورالعمل راهنمای بهره‌برداری کمک می‌کند.

۷-۳- تحلیل لایه‌های حفاظت چگونه عمل می‌کند؟

تحلیل لایه‌های حفاظت یک روش‌شناسی مشتق‌شده از سناریو است. بنابراین، این تحلیل بر سناریوهای از پیش تعریف شدهٔ حاصل از مطالعاتی مانند تحلیل‌های خطر فرایند کمّی، مدیریت ارزشیابی تغییر و یا بازنگری طراحی مبتنی است. یک سناریو با یک زوجِ علت – پیامد تعریف می‌شود. اگر یک پیامد علل مختلفی داشته باشد، هر زوج علت – پیامد به صورت یک سناریوی مجزا تحلیل می‌شود. به طور مشابه، اگر یک علت منجر به چند پیامد مختلف شود، سناریوهای اضافی باید توسعه یابند. زوج‌های علت – پیامد معمولاً براساس وخامت پیامد غربال می‌شوند. روش‌های دسته‌بندی وخامت مختلفی، از ارتباط غیرمستقیم آسیب انسانی گرفته تا تخمین کمّی آسیب انسانی، می‌تواند استفاده شود. هزینه‌های مالی ایجاد شده نیز می‌تواند معیار دیگری از نتایج رویداد باشد.

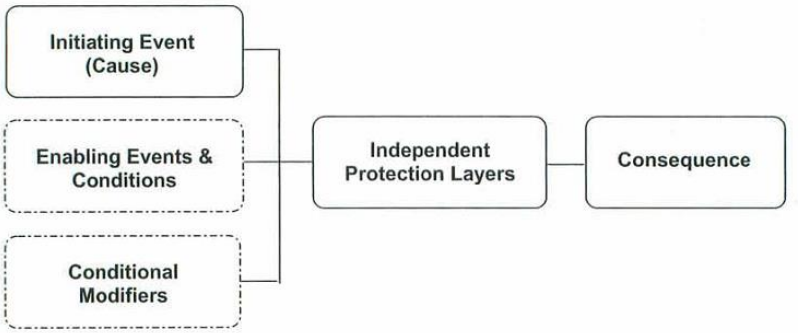
۷-۳-۱- مراحل روند تحلیل لایه‌های حفاظت

مراحل روند تحلیل لایه‌های حفاظت عبارتند از:

- شناسایی و تعریف سناریو،
- انتخاب یک سناریوی رویداد،
- شناسایی رویداد آغازگر سناریو و تعیین فرکانس وقوع رویداد آغازگر (تعداد رویداد در سال)،
- شناسایی لایه‌های حفاظت مستقل (IPL) و تخمین احتمال خرابی هنگام نیاز (PFD) هر لایه مستقل حفاظت،
- تخمین ریسک سناریو با ترکیب پیامد، رویداد آغازگر و داده‌های لایه‌های حفاظت مستقل.

۷-۴- توسعهٔ سناریو

شکل ۷۲ اجزای دخیل در یک سناریو را نشان می‌دهد. در این شکل، اجزای داخل باکس‌های با خط ممتد برای شکل‌گیری یک سناریو نیاز هستند و آیتم‌های اختیاری در باکس‌های نقطه‌چین ارائه شده‌اند.



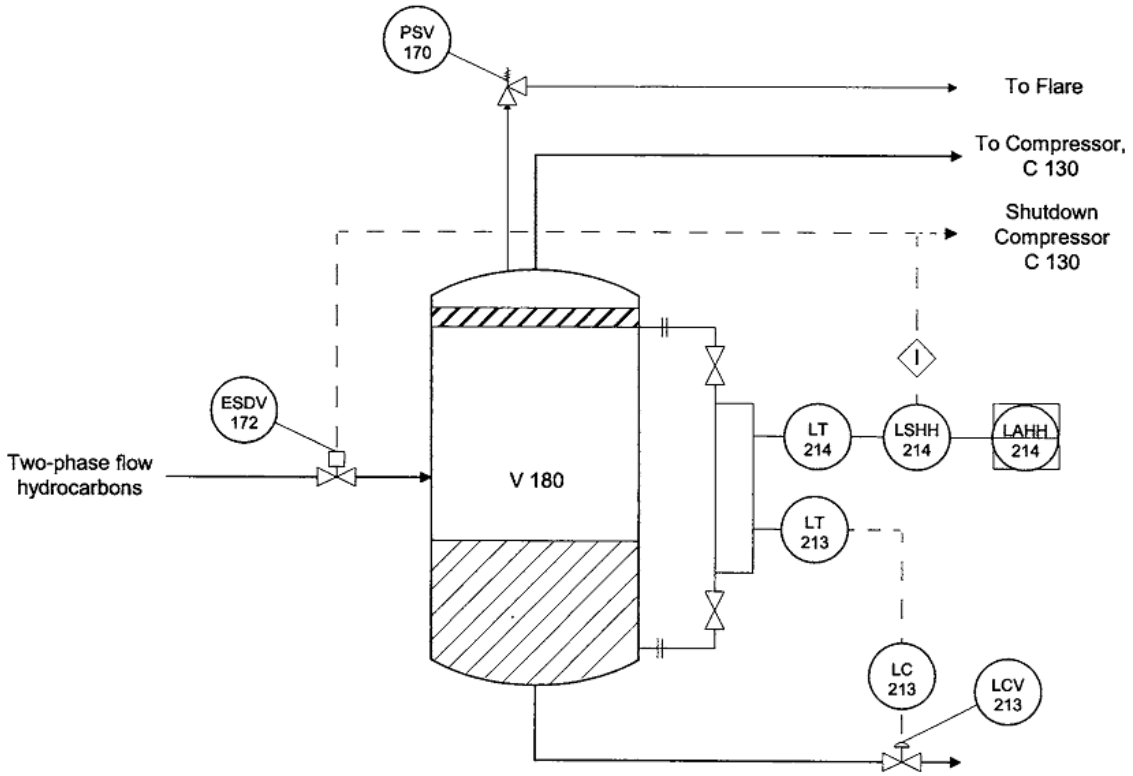
شکل ۷۲: اجزای یک سناریوی تحلیل لایه‌های حفاظت

رویداد آغازگر، علت منجرشدن سناریو به پیامد مشخص است. در برخی حالت‌ها، اگر رویداد آغازگر به تنهایی نتواند منجر به پیامد مشخص شود، ممکن است نیاز به شرایط و یا رویدادهای دیگری برای وقوع داشته باشد.

اگر دسته‌بندی وخامتِ پیامد بر اساس مرگ و میرها یا زیان اقتصادی و یا محیطی باشد، شرایطِ محیطی محتمل، می‌توانند برای پالایش خروجی سناریو به کار روند. شرایط محیطی محتمل نوعی ممکن است شامل موارد زیر باشند:

- احتمال اشتعال،
- احتمال صدمه جانی،
- احتمال قرار گرفتن فرد در ناحیه آلوده،
- احتمال فرار فرد از رویداد،
- احتمال نجات فرد.

یک لایهٔ حفاظت مستقل، یک حفاظ است که قادر است از رسیدن یک سناریو به پیامد نامطلوبش ممانعت کند. این لایه از رویداد آغازگر و یا اقدامات هر لایهٔ دیگر حفاظتی مرتبط با سناریو، مستقل است. برای روشن‌سازی مفهوم تحلیل لایه‌های حفاظت، یک مثال ارائه می‌شود که شامل جداکنندهٔ هیدروکربن‌های دوفاز مطابق شکل ۷۳ است.



شکل ۷۳: جداکنندهٔ دوفاز به همراه سیستم کنترلی آن

در این جداکنندهٔ V 180، کنترل سطح توسط کنترل کنندهٔ LC 213 کنترل می‌شود. درحالت بالارفتن سطح مایع، سوئیچ سطح LSHH 214 می‌تواند شیر خاموشی اضطراری ESDV 172 را بسته و کمپرسور C 130 واقع در پایین‌دست مخزن V 180 را خاموش نماید. این کار برای ممانعت از رسیدن مایع به کمپرسور و خرابی آن انجام می‌شود. طی مطالعهٔ HAZOP، سناریوی مخاطره‌آمیز زیر شناسایی شده است.

جدول شماره ۲۸: علت و پیامد سناریوی مخاطره‌آمیز در جداکننده

موقعیت:	جداکنندهٔ دوفاز V 180
انحراف:	سطح بالا
علت:	خرابی مدار کنترل ۲۱۳
پیامد:	امکان رسیدن مایع به کمپرسور C 130 منجر به خرابی کمپرسور، آسیب به یکپارچگی و امکان آتش‌سوزی و صدمه فردی
حفاظ‌ها:	فعال شدن هشدار LAHH 214 مربوط به سوئیچ سطح LSHH 214 و بسته‌شدن ESDV 172 و خاموش‌شدن کمپرسور C 130

جدول شماره ۲۹: سناریوی مخاطره‌آمیز در جداکننده

رویداد آغازگر:	خرابی مدار کنترل سطح ۲۱۳
رویداد فعال‌کننده:	بسته شدن LCV 213 و منجرشدن به تجمع مایع در مخزن

شرایط محتمل محیطی:	در اثر نقص در محدودنگهداشتن ناشی از خرابی کمپرسور یا آسیب وخیم، موارد زیر باید بعنوان شرایط محتمل محیطی ارزشیابی شوند: احتمال وجود افراد در محل، احتمال اشتعال، احتمال صدمه.
لایه‌های حفاظت مستقل:	سیستم ابزاردقیق ایمنی: فعال‌شدن سوئیچ سطح LSHH 214 و بسته شدن ESDV 172 و خاموشی کمپرسور C 130
پیامد:	خرابی کمپرسور منجر به صدمه به افراد

به عبارت دیگر، سناریو به این صورت است که کنترل‌کنندهٔ سطح LC 213 خراب شده و منجر به خرابی LCV 213 می‌شود به گونه‌ای که اجازه نمی‌دهد جریان مناسب خروجی از جداکننده برقرار شود و سیستم ابزاردقیق ایمنی به درستی عمل نمی‌کند و درنتیجه سطح مایع تا کمپرسور افزایش می‌یابد که منجر به صدمه و آسیب بالقوّه می‌شود.

هنگامی که سناریو تهیه می‌شود، سوالات عمده عبارتند از:

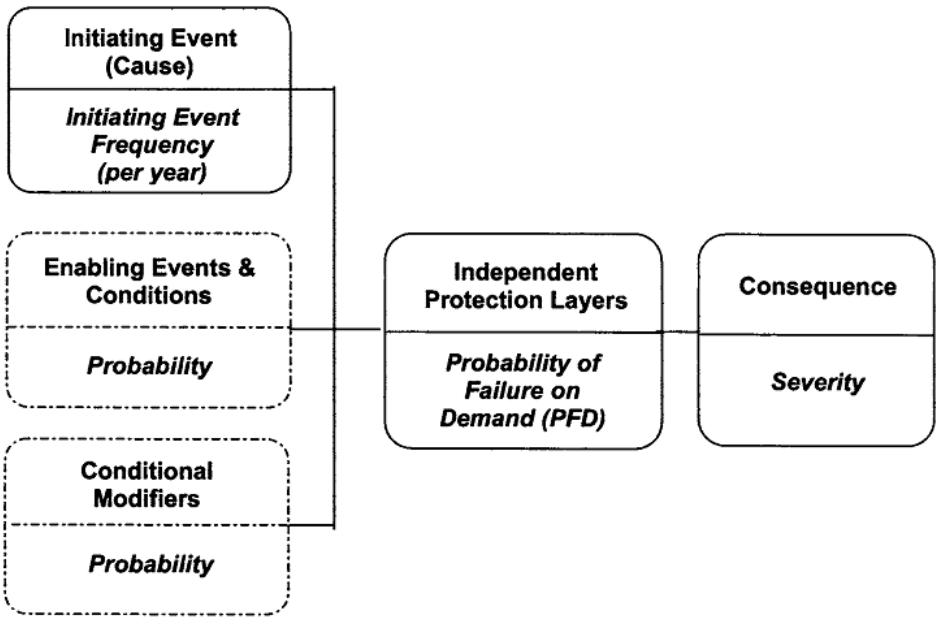
- احتمال وقوع این رویداد نامطلوب چه میزان است؟
- ریسک ناشی از این سناریو چه میزان است؟
- آیا اقدامات کافی برای کاهش ریسک وجود دارد؟

به منظور پاسخ به این سولات، باید برای اجزای سناریو مقادیر عددی تعیین شود. شکل ۷۴ نشان می‌دهد کدام مقادیر عددی برای اجزای سناریو لازم است. به منظور ارزشیابی کفایت اقدامات کاهش ریسک، معیار ریسک قابل تحمل باید تعیین شود. این معیار معمولاً بر مقادیر محک از داده‌های صنعتی، تاریخچهٔ شرکت و یا داده‌های آماری مبتنی است.

در سناریوهایی که فرکانس رویداد آغازگر کمتر از دو برابر فرکانس تست یک لایهٔ حفاظت مستقل است، فرکانس پیامد نامطلوب از رابطه زیر محاسبه می‌شود:

$$f_i^C = f_i^I \times PFD_{i1} \times PFD_{i2} \times ..... \times PFD_{ij} \qquad (۱-۷)$$

در این رابطه، f_i^C فرکانس پیامد C برای رویداد آغازگر I (به ازای سال)، f_i^I فرکانس رویداد آغازگر I (به ازای سال) و PFD_{ij} احتمال خرابی هنگام نیاز برای لایهٔ حفاظت مستقل Jام که از سیستم در برابر پیامد C رویداد آغازگر I محافظت می‌کند.



شکل ۷۴: اجزا در سناریوی تحلیل لایه‌های حفاظت و ورودی‌های عددی مورد نیاز

برای سناریوهای «با نیاز بالا»، یعنی فرکانس چالش در برابر لایهٔ حفاظت مستقل که بیش از دو برابر فرکانس تست لایهٔ حفاظت مستقل است، به عنوان مثال، لایهٔ حفاظت مستقل یک بار در سال تست می‌شود و بیش از دو بار در سال به آن نیاز است، رابطهٔ زیر باید برای محاسبهٔ فرکانس پیامد نامطلوب استفاده شود:

$$f_i^C = 2 \times \left(IPL_{i1} test \quad frequency, \quad per \quad year \right) \times PFD_{i1} \times PFD_{i2} \times ..... \times PFD_{ij} \qquad (۲-۷)$$

این رویکرد نتایج فرکانس واقع‌بینانه‌تری فراهم می‌آورد. اگر رویدادهای فعال‌کننده و یا بهبوددهنده‌های شرایط وجود داشته باشد، روابط بالا به صورت زیر اصلاح می‌شوند.

برای مود نیاز کم:

$$f_i^C = f_i^I \times PFD_{i1} \times PFD_{i2} \times ..... \times PFD_{ij} \times P_{Enabling \quad event} \times P_{Condition \quad modifier} \qquad (۳-۷)$$

در این رابطه، $P_{Enabling \quad event}$ احتمال وقوع رویداد فعال‌کننده و $P_{Condition \quad modifier}$ احتمال فاکتورهای بهبوددهنده است.

برای مود نیاز بالا:

$$f_i^C = 2 \times \left(IPL_{i1} test \quad frequency, \quad per \quad year \right) \times PFD_{i1} \times PFD_{i2} \times ..... \times PFD_{ij} \times P_{Enabling \quad event} \times P_{Condition \quad modifier} \qquad (۴-۷)$$

احتمال خرابی هنگام نیاز (PFD) برای هر لایهٔ حفاظت مستقل نوعاً با استفاده از داده‌های در دسترس و یا جدول‌های جستجو تخمین زده می‌شود. فرکانس هر رویداد آغازگر تعیین شده برای سناریو، یعنی علت سناریو معمولاً از داده‌های نرخ

خرابی و یا از جدول جستجو تخمین زده می‌شود. برای روشن شدن موضوع، فرض کنید دسته‌های وخامت زیر برای پیامد استفاده شده و درجه ۴ وخامت انتخاب شود. مقادیر انتخاب شده برای اجزای سناریو در جدول شماره ۳۱ داده شده است.

جدول شماره ۳۰: دسته‌بندی کمی وخامت (جدول مقادیر زیر، روش‌شناسی را روشن می‌کند)

درجه وخامت	توضیح	صدمه/ دسته آسیب
۱	پیامد کم	مانند دسته ۲
۲	پیامد کم	بدون صدمه یا صدمه کم، بدون زمان از دست رفته
۳	پیامد متوسط	صدمه تک، غیر وخیم، زمان از دست رفته محتمل
۴	پیامد زیاد	یک صدمهٔ وخیم یا بیشتر
۵	پیامد بسیار زیاد	مرگ یا صدمهٔ معلولیت دائمی

جدول شماره ۳۱: مقادیر عددی به کار رفته در سناریوی جداکنندهٔ دوفاز (جدول مقادیر زیر، روش‌شناسی را روشن می‌کند)

اجزای سناریو	توضیح	مقدار
پیامد (وخامت)	خرابی کمپرسور منجر به صدمه به افراد	دسته ۴
فرکانس رویداد آغازگر (به ازای سال)	خرابی مدار کنترل سطح ۲۱۳	۱×۱۰^{-۱}
رویدادها یا شرایط فعال‌کننده	بسته شدن LCV 213 منجر به تجمع مایع در مخزن	۰/۵
بهبوددهنده‌های شرایط (احتمال)	احتمال اشتعال احتمال حضور فرد در محل احتمال صدمه	۰/۷ ۰/۵ ۰/۸
لایه‌های حفاظت مستقل	(سوئیچ سطح LSHH 214 با هشدار LAHH 214 برای بستن ESDV 172 و خاموشی کمپرسور PM 130)	۱×۱۰^{-۲}

براساس مقادیر جدول فوق، خواهیم داشت:

$$f_i^C = 1\times10^{-1}\times1\times10^{-2}\times0.5\times0.7\times0.5\times0.8 = 1.4\times10^{-4}\,(per \quad year) \qquad (۵-۷)$$

روش ماتریس ریسک برای تعیین معیار ریسک قابل تحمل در این مثال به کار می‌رود. ماتریس ریسک در جدول شماره ۳۲ آمده است.

جدول شماره ۳۲: ماتریس ریسک به کار رفته در مثال جداکننده دوفاز

Conseq. Cat. / Freq. (per yr)	Category 1	Category 2	Category 3	Category 4	Category 5
1 to 10^{-1}	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Not Desirable – Risk control measures to be introduced within a specified time period	Unacceptable	Unacceptable
10^{-1} to 10^{-2}	Acceptable with control	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Not Desirable – Risk control measures to be introduced within a specified time period	Unacceptable
10^{-2} to 10^{-3}	Acceptable – No actions are needed	Acceptable – No actions are needed	Optional (evaluate alternatives)	Not Desirable – Risk control measures to be introduced within a specified time period	Not Desirable – Risk control measures to be introduced within a specified time period
10^{-2} to 10^{-3}	Acceptable – No actions are needed	Acceptable – No actions are needed	Optional (evaluate alternatives)	Optional (evaluate alternatives)	Not Desirable – Risk control measures to be introduced within a specified time period
10^{-3} to 10^{-4}	Acceptable – No actions are needed	Acceptable – No actions are needed	Acceptable – No actions are needed	**Optional (evaluate alternatives)**	Optional (evaluate alternatives)
10^{-4} to 10^{-5}	Acceptable – No actions are needed	Acceptable – No actions are needed	Acceptable – No actions are needed	Acceptable – No actions are needed	Optional (evaluate alternatives)

شرایط مثال جداکننده در ماتریس ریسک در دستهٔ «ارزشیابی اختیاری گزینه‌های جایگزین» قرار دارد. گزینه‌های دیگری که می‌توانند در این حالت در نظر گرفته شوند، عبارتند از:

- ارتقای قابلیت اطمینان مدار کنترل سطح ۲۱۳،
- ارتقای قابلیت اطمینان سیستم ابزاردقیق ایمنی،
- لایه‌های حفاظت مستقل اضافی ممکن.

۷-۵- تخمین وخامت و پیامدها

روش‌های مختلفی برای ارزشیابی پیامدها وجود دارد که عبارتند از:

- رویکرد دسته‌ای بدون ارجاع مستقیم به صدمهٔ انسانی،
- تخمین‌های کیفی با صدمهٔ انسانی،
- تخمین‌های کیفی با صدمهٔ انسانی با لحاظ احتمال‌های پسا-انتشار،
- تخمین‌های کمّی با صدمه انسانی،
- هزینه‌های کلی حاصل از رویدادهای بالقوّه (به عنوان مثال، زیان‌های سرمایه‌ای، زیان‌های تولید و ...)

۷-۵-۱- رویکرد دسته‌ای بدون ارجاع مستقیم به صدمهٔ انسانی

این رویکرد حاوی مشخصات زیر است:

- تمرکز بر جلوگیری از انتشار نسبت به مهار پیامدها،
- عدم استفاده از صدمه/ مرگ و میر انسانی به عنوان نقطه پایان معیار ریسک قابل تحمل،
- نوعاً استفاده از ماتریس‌هایی برای مشتق‌کردن پیامدها به دسته‌های مختلف.

نمونه‌ای از دسته‌بندی پیامد با رویکرد دسته‌ای در جدول شماره ۳۳ ارائه شده است.

جدول شماره ۳۳: مثالی از دسته‌بندی پیامد

Release Characteristic	1- to 10-lb release	10- to 100- lb release	100- to 1000- lb release	1000- to 10,000- lb release	10,000- to 100,000- lb release	> 100,000 lb release
Extremely toxic above boiling point	Cat. 3	Cat. 4	Cat. 5	Cat. 5	Cat. 5	Cat. 5
Extremely toxic below boiling point or highly toxic above boiling point	Cat. 2	Cat. 3	Cat. 4	Cat. 5	Cat. 5	Cat. 5
Highly toxic below boiling point or flammable above boiling point	Cat. 2	Cat. 2	Cat. 3	Cat. 4	Cat. 5	Cat. 5
Flammable below boiling point	Cat. 1	Cat. 2	Cat. 2	Cat. 3	Cat. 4	Cat. 5
Combustible liquid	Cat. 1	Cat. 1	Cat. 1	Cat. 2	Cat. 2	Cat. 3

هر پیامدی یک شماره دسته بین ۱ تا ۵ دارد. دستهٔ شمارهٔ ۵ وخیم‌ترین دسته است. دسته‌بندی پیامدها در جدول فوق می‌تواند همراه با یک ماتریس ریسک مانند جدول ماتریس ریسک مثال جداکنندهٔ دوفاز به کار رود.

۷-۵-۲- تخمین‌های کیفی با صدمهٔ انسانی

این رویکرد حاوی مشخصات زیر است:

- در این روش تمرکز بر اثر نهایی بر انسان است و میزان وخامت بر اساس قضاوت کیفی تخمین زده می‌شود.
- ریسک حاصل می‌تواند مستقیماً با معیار ریسک قابل تحمل مرگ و میر مقایسه شود.

نمونه‌ای از روش تخمین کیفی با صدمه انسانی در جدول شماره ۳۴ ارائه شده است.

جدول شماره ۳۴: نمونهٔ دسته‌بندی کیفی – دسته‌های زیان مرکب

Low Consequence	
Personnel	Minor or no injury; no lost time
Community	No injury, hazard, or annoyance to public
Environment	Recordable event with no agency notification or permit violation
Facility	Minimal equipment damage at an estimated cost of less than $100,000 and with no loss of production.
Medium Consequence	
Personnel	Single injury, not severe; possible lost time
Community	Odor or noise complaint from the public
Environment	Release that results in agency notification or permit violation
Facility	Some equipment damage at an estimated cost greater than $100,000 and with minimal loss of production.
High Consequence	
Personnel	One or more severe injuries
Community	One or more minor injuries
Environment	Significant release with serious offsite impact
Facility	Major damage to process area(s) at an estimated cost greater than $1,000,000 or some loss of production
Very High Consequence	
Personnel	Fatality or permanently disabling injury
Community	One or more sever injuries
Environment	Significant release with serious offsite impact and more likely than not to cause immediate or long-term health effects.
Facility	Major or total destruction of process area(s) at an estimated cost greater than $10,000,000 or a significant loss of production

۷-۵-۳- تخمین‌های کیفی با صدمهٔ انسانی با لحاظ احتمال‌های پسا-انتشار

این رویکرد مشابه رویکرد قبلی است، البته با برخی ملاحظات اضافی از جمله:

- لحاظ احتمال اینکه رویداد به ابر سمی و یا قابل اشتعال منجر خواهد شد،
- لحاظ احتمال اینکه آیا یک فرد در منطقه حاضر خواهد بود،
- لحاظ احتمال صدمه/ مرگ و میر.

۷-۵-۴- تخمین‌های کمّی با صدمهٔ انسانی

این رویکرد نیازمند تحلیل‌های تفصیلی و مدل‌سازی ریاضی برای تعیین اثرات بر مردم و تجهیزات است.

۷-۵-۵- هزینهٔ کلی رویداد بالقوّه

یک رویداد می‌تواند معادل اثرات مالی مانند زیان‌های سرمایه‌ای، زیان‌های تولید و .... باشد. هنگامی که این زیان‌ها تجمیع شود، مجموع کل می‌تواند به صورت مقیاس اقتصادی ریسک لحاظ شود.

۷-۶- رویدادهای آغازگر و تخمین فرکانس

لیستی از رویدادهای آغازگر نوعی که می‌توانند پیش زمینهٔ یک حادثه باشند در جدول شماره ۳۵ ارائه شده است. اگرچه این رویدادها ضرورتاً منجر به اثرات وخیم و ویران‌گر نمی‌شوند، اما این قابلیت را دارند.

جدول شماره ۳۵: رویدادهای آغازگر نوعی

Type of event	Examples
Mechanical failures	○ Corrosion ○ Vibration ○ Erosion ○ Flow surge or hydraulic hammer ○ Seal/gasket/flange failure ○ Relief device stuck open ○ Puncture ○ Fracture ○ Fabrication defects ○ Brittle fracture
Control systems failures	○ Sensors failure ○ Logic solver failure ○ Final elements failure ○ Field wiring failure ○ Communication interface failure ○ Software failures or crashes
Utility failures	○ Power failure ○ Loss of instrument air ○ Loss of plant nitrogen ○ Loss of cooling water ○ Loss of steam
Natural external events	○ Earthquakes ○ Tornadoes ○ Hurricanes ○ Floods ○ High winds ○ Lightning
Human external events	○ Major accidents in adjacent facilities ○ Incidents in adjacent processes ○ Incidents within the process ○ Mechanical impact by motor vehicles
Human failures	○ Operational error ○ Maintenance error ○ Critical response error ○ Programming error

۷-۶-۱- انواع رویدادهای آغازگر

همهٔ رویدادها را نمی‌توان به صورت علت مستقیم یا غیرمستقیم برای یک رویداد دسته‌بندی کرد. ممکن است برخی از رویدادها مورد شک واقع شوند، اما نمی‌توان آنها را تأیید کرد. با این حال، اگر یک نشانهٔ روشن از اینکه رویداد آغازگر و حادثهٔ نهایی به طور قطعی مرتبط هستند، وجود داشته باشد، مقتضی است از آنها در تحلیل استفاده کرد. مثال‌های نوعی از رویدادهای آغازگر عبارتند از:

- آموزش/ مدرک ناکافی اپراتور – علت محتمل یک رویداد آغازگر،
- تست و شناسایی ناکافی - علت محتمل یک رویداد آغازگر،

- عدم دسترسی به ابزارهای حفاظتی مانند شیرهای ایمنی یا تله‌های سرعتِ بیش از حد – نیازمند آغاز رویدادهای دیگر پیش از ایجاد چالش برای ابزارهای حفاظتی،
- رویه‌های عملکردی غیر واضح یا غیر دقیق – علت محتمل یک رویداد آغازگر.

۷-۶-۲- راستی‌آزمایی رویداد آغازگر

پیش از تخصیص فرکانس‌های رویداد آغازگر به علت یک سناریو، لازم است از معتبر بودن رابطهٔ بین علت – پیامد اطمینان حاصل شود. موارد زیر معیارهای نوعی است که باید برقرار باشند:

- نیاز به راستی‌آزمایی اینکه رابطهٔ علت – پیامد برای هر سناریو یکتا است.
- تلاش برای شکست و تقسیم علت به رویدادهای خرابی گسسته، به عنوان مثال «از دست رفتن خنک‌سازی» می‌تواند ناشی از شماری از خرابی‌های محتمل مانند موارد زیر است:
  - خرابی پمپ خنک‌کننده،
  - خرابی دمنده‌های خنک‌کننده در مبدل‌های هواخنک،
  - خرابی در منبع توان،
  - خرابی مدار کنترلی، منجر به خرابی در خنک‌کننده و یا کنارگذر شدن خنک‌کننده از مبدل‌ها.

۷-۶-۳- رویدادها/ شرایط فعال‌کننده

رویدادها یا شرایط فعال‌کننده اقدامات یا شرایطی هستند که مستقیماً مسبب سناریو نیستند، ولی به عنوان اجزای سناریو باید حاضر یا فعال باشند. این اقدامات هنگامی که مکانیزم بین رویداد آغازگر و پیامدهای آن نیاز به توضیح دارند، باید به کار روند.

۷-۶-۴- تخمین فرکانس رویداد آغازگر

معمولاً فرکانس رویداد آغازگر از یک یا چند منبع مختلف به دست می‌آید. از آن مهم‌تر باید دامنهٔ اندازه این احتمال از منابع مختلف مشابه هم باشد. نوعاً داده‌های نرخ خرابی از منابع زیر به دست می‌آید:

- داده‌های صنعتی – برای خرابی اجزا:
  - ✓ اصول راهنما برای داده‌های قابلیت اطمینان تجهیزات فرایند، CCPS (۱۹۸۶)،

- ✓ راهنمای مجموعه و نمایش داده‌های قابلیت اطمینان الکتریکی، الکترونیکی و اجزای حسگر برای تأسیسات تولید توان هسته‌ای، IEEE (۱۹۸۴)،
- ✓ داده‌های قابلیت اطمینان ساحلی (OREDA).

- داده‌های صنعتی – نرخ‌های خطای انسانی:
  - ✓ فرایندهای شیمیایی ایمن‌تر ذاتی: یک رویکرد سیکل عمر، CCPS (۱۹۹۶)،
  - ✓ هندبوک تحلیل قابلیت اطمینان انسانی با تمرکز بر کاربردهای نیروگاه‌های هسته‌ای Swain, A.D., and H.E. Guttman (۱۹۸۳).
- تجربیات کارخانه – شامل داده‌های تاریخی برای فرایند و تجربیات کارکنان تأسیسات/ داده‌های نرخ خرابی.
- داده‌های مشتریان – این داده‌ها چنانچه در شرایط تمیز و نگهداری خوب توسعه یابند، نوعاً به صورت خوش‌بینانه هستند.

جدول جدول شماره ۳۶ حاوی فرکانس‌های رویدادهای آغازگر نوعی است.

جدول شماره ۳۶: مقادیر فرکانس نوعی (CCPS, 2001)

Initiating Event	Frequency Range (per year)
Pressure vessel residual failure	10^{-5} to 10^{-7}
Cooling water failure	1 to 10^{-2}
Pump seal failure	10^{-1} to 10^{-2}
Atmospheric tank failure	10^{-3} to 10^{-5}
Gasket / packing blowout	10^{-2} to 10^{-6}

برای بهره‌برداری غیرپیوسته، مانند بارگذاری، باربرداری، روشن‌سازی/خاموش‌سازی و نگهداری، فرکانس‌های خرابی باید مربوط به زمان فعال‌بودن باشد. برای مثال، در عملکرد مجموعهٔ راکتورهای شیمیایی، هنگامی که یک واکنش گرمازا رخ می‌دهد، سیستم خنک‌کننده باید به مدت ۲ ساعت روشن شود. با فرض اینکه دو راکتور در هر روز آماده می‌شود و تأسیسات ۵ روز در هفته کار می‌کنند و فرکانس خرابی سیستم خنک‌کننده برابر ۱×۱۰^{-۲} بار به ازای هر سال است، فرکانس واقعی خرابی سیستم خنک‌کننده به صورت زیر بدست می‌آید:

$$f^{I} = 1\times10^{-2}\times\frac{2\times2\times5\times52}{24\times365} = 1.19\times10^{-3}\left(per \quad year\right) \qquad (۶-۷)$$

۷-۷- لایه‌های حفاظت مستقل

همهٔ لایه‌های حفاظت مستقل، حفاظ هستند، ولی الزاماً همهٔ حفاظ‌ها، لایه‌های حفاظت مستقل نیستند. یک لایهٔ حفاظت مستقل دو مشخصه دارد:

- اثرگذاری لایهٔ حفاظت مستقل در جلوگیری از سناریو،
- استقلال لایه حفاظت مستقل از رویداد آغازگر و سایر لایه‌های حفاظت مستقل.

۷-۷-۱- قوانین سه D، چهار E و I بزرگ

در ارزشیابی لایه‌های حفاظت مستقل اصول زیر توسعه یافته است.

۱. قانون سه D، به تعیین اینکه یک لایهٔ حفاظت مستقل است، کمک می‌کند و شامل آشکارسازی، تصمیم‌گیری و مهار است.

- آیا لایهٔ حفاظت مستقل می‌تواند یک شرایط در سناریو را آشکار کند؟
- آیا لایهٔ حفاظت مستقل می‌تواند تصمیم به انجام یک اقدام بگیرد؟
- آیا لایهٔ حفاظت مستقل می‌تواند یک رویداد نامطلوب را با ممانعت از آن منحرف سازد؟

۲. قانون چهار E، به ارزشیابی اثربخشی یک لایهٔ حفاظت مستقل کمک می‌کند و شامل معیارهای به اندازهٔ کافی بزرگ بودن، به اندازهٔ کافی سریع بودن، به اندازهٔ کافی مستحکم بودن و به اندازهٔ کافی هوشمند بودن است.

- آیا لایهٔ حفاظت مستقل به اندازهٔ کافی بزرگ است که رویدادهای نامطلوب را مهار و از پیامد نامطلوب آن جلوگیری نماید (به این معنی که آیا لایهٔ حفاظت مستقل به اندازهٔ صحیح و کافی دارد؟ مثلاً اوریفیس شیر اطمینان، حجم سد، ظرفیت پمپ و ...)
- آیا لایهٔ حفاظت مستقل به اندازهٔ کافی در آشکارسازی، تصمیم‌گیری و مهار سریع است؟ (یعنی آیا لایهٔ حفاظت مستقل زمان کافی برای آشکارسازی شرایط، پردازش اطلاعات، اتخاذ تصمیم، اقدام مؤثر مورد نیاز را انجام می‌دهد؟)

- آیا لایهٔ حفاظت مستقل برای مقاومت در برابر رویداد نامطلوب به اندازه کافی استحکام دارد؟ (مثلاً استحکام کافی خطوط لوله در برابر افزایش فشار برای مدت کوتاه ناشی از نیروهای ایجاد شده از انفجارها)
- آیا لایهٔ حفاظت مستقل برای ممانعت از وقوع پیامدهای نامطلوب به اندازه کافی هوشمند است؟ (مؤثر بودن اقدام آغازین برای یک حفاظ و سازگار بودن زمان‌بندی/ توالی با سایر الزامات سیستم. مثلاً اگر یک شیر خاموشی اضطراری در بالادست یک پمپ باید قبل از خاموشی پمپ باشد، می‌تواند منجر به کاویتاسیون شدید در پمپ شود.)

۳. قانون I بزرگ می‌گوید که لایهٔ حفاظت مستقل باید از رویداد آغازگر و همهٔ سایر لایه‌های حفاظت مستقل، مستقل باشد. این فرض اصلی در تحلیل لایه‌های حفاظت است. این قانون برای توجه نسبت به خرابی‌های با عامل مشترک مهم است. خرابی با عامل مشترک، خرابی بیش از یک جزء، آیتم یا سیستم در اثر علت یا رویداد آغازگر یکسان است. اگر در یک سناریو خرابی با عامل مشترک وجود داشته باشد، همهٔ حفاظ‌های متأثر از خرابی با عامل مشترک باید تنها به عنوان یک لایهٔ حفاظت مستقل لحاظ شوند.

۷-۷-۲- مشخصات لایه‌های مختلف حفاظت

لایه‌های نوعی حفاظت عبارتند از:

- طراحی فرایند،
- سیستم کنترل فرایند پایه (BPCS)،
- هشدارهای بحرانی و دخالت انسان،
- سیستم ابزاردقیق ایمنی (SIS)،
- حفاظت فیزیکی،
- حفاظت پسا- انتشار،
- پاسخ اضطراری تأسیسات،
- پاسخ اضطراری جامعه،

۷-۷-۲-۱- طراحی فرایند

معمولاً دو راه برای اعتباربخشی به طراحی فرایند ایمن‌تر در تحلیل لایه‌های حفاظت وجود دارد:

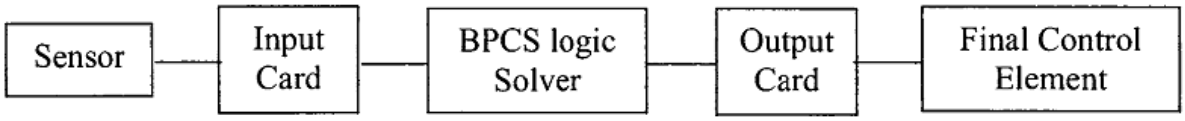
- حذف برخی سناریوها با طراحی فرایند ایمن‌تر، به عنوان مثال فضای بیشتر، کاهش اجزا و ...،

- به کار بردن برخی اجزای طراحی فرایند ایمن‌تر ذاتی به عنوان لایه‌های حفاظت مستقل و تخصیص احتمال خرابی هنگام نیاز غیرصفر به آنها. این رویکرد امکان مقایسهٔ بین ریسک حاصل از فرایندها/ طراحی تجهیزات مختلف مبتنی بر استانداردها/ تجارب مهندسی مختلف را فراهم می‌آورد.

به منظور تضمین سازگاری بین مطالعات تحلیل لایه‌های حفاظت، یکی از دو رویکرد باید به طور صحیح به کار رود.

۷-۷-۲-۲- سیستم‌های کنترل فرایند پایه

سیستم‌های کنترل فرایند پایه به صورت پیوسته فرایندها را در حدود عملکردی ایمن پایش، کنترل و نگه می‌دارند. یک مدار سیستم کنترل فرایند پایه معمولاً شامل اجزای شکل ۷۵ است.



شکل ۷۵: اجزای مدار سیستم کنترل فرایند

سه نوع مختلف از اقدامات ایمنی وجود که توسط سیستم‌های کنترل فرایند پایه انجام می‌شود. این اقدامات، خود می‌توانند لایه‌های حفاظت مستقل باشند:

اقدامات کنترل پیوسته – این اقدامات فرایند را در حدود عملکردی نرمال نگه می‌دارد. به عنوان مثال، یک کنترل‌کنندهٔ سطح، که سطح مایع را داخل یک مخزن نگه می‌دارد، مانع از سرزیر شدن جریان از مخزن می‌شود.

اقدامات هشدار – حل‌گر منطقی یا واحد تریپ که انحرافات فرایند از حدود عملکردی نرمال را شناسایی می‌کند و نوعاً به شکل پیام‌های اخطار، به اپراتور برای انجام اقدامات اصلاحی اخطار می‌دهد.

فرایند بازگشت به حالت پایه – حل‌گر منطقی یا رله‌های کنترلی، که می‌توانند اقدامات اتوماتیک برای بازگرداندن فرایند به حالت پایدار انجام دهند. به عنوان مثال، یک واحد تقطیر درصورتی‌که انحرافات غیرقابل قبول در عملکرد آن رخ دهد می‌تواند به طور کامل عملکرد خود را ازسرگیرد.

فاکتورهای زیر در تعیین میزان اعتبار ضروری برای یک سیستم کنترل فرایند پایه، باید لحاظ شوند:

کفایت رویه‌های امنیت و دسترسی – بسیاری از تأسیسات سیستم کنترل فرایند پایه به صورت تعمدی در دسترس اپراتوری ساخته می‌شوند که می‌تواند نقاط کنترلی، هشدارها و ... را تغییر دهد. این امر باعث می‌شود سیستم کنترل فرایند

پایه مستعد دریافت خطاهای انسانی باشد و درصورتی‌که کنترل و امنیت کافی نباشد، کارایی مورد انتظار این سیستم کاهش می‌یابد.

سطح افزونگی – معمولاً سیستم کنترل فرایند پایه افزونگی کمی دارد. اما برای برخی طراحی‌های پیچیده مانند فرایند تجزیه هیدروکربن‌ها و نیز جداسازی نفت و گاز دور از ساحل، سطح افزونگی اجزای سیستم کنترل فرایند پایه بیشتر از در کنترل فرایند نرمال است. به کارگیری افزونگی احتمال خرابی هنگام نیاز (PFD) مدار سیستم کنترل فرایند پایه را کاهش خواهد داد.

سابقهٔ نرخ خرابی – به منظور محاسبه احتمال خرابی هنگام نیاز یک مدار سیستم کنترل فرایند پایه، ضروری است داده‌های نرخ خرابی حل‌گرهای منطقی، کارت‌های ورودی و خروجی، المان‌های کنترل نهایی، پاسخ انسانی و ... مورد بررسی و استفاده قرار گیرند.

نرخ تست مؤثر – قابلیت اطمینان یک سیستم کنترل فرایند پایه به فرکانس تست و اثربخشی تست نیز وابسته است.

سایر فاکتورها – سایر فاکتورهایی که باید لحاظ شوند شامل طراحی، ساخت، نصب و نگهداری هستند.

۷-۷-۲-۳- هشدارهای بحرانی و مداخلهٔ انسانی

این سیستم‌ها معمولاً با سیستم کنترل فرایند پایه فعال می‌شوند. یک کوره که مدار کنترل جریان سوخت گازی آن با فشار جبران نمی‌شود را در نظر بگیرید. سیستم کنترل فرایند پایه می‌تواند در فشار گاز بالا یک هشدار تولید کند. سپس اپراتور می‌تواند اقدام مناسب برای کنترل فشار گاز و یا خاموش کردن کوره انجام دهد. در اینجا لایهٔ حفاظت مستقل می‌تواند مدار سسیتم کنترل فرایند و اقدام اپراتور باشد.

فاکتورهای زیر باید در تعیین میزان اعتبار لازم برای اقدام انسانی به عنوان لایهٔ حفاظت مستقل، لحاظ شوند:

- آشکارسازی – شرایط چگونه آشکار خواهد شد؟ (مثلاً هشدار)
- تصمیم‌گیری – تصمیم بر اقدام چگونه اتخاذ خواهد شد؟
- اقدام – کدام اقدام برای جلوگیری از پیامد لازم است؟

۷-۷-۲-۴- سیستم ابزاردقیق ایمنی (SIS)

یک سیستم ابزاردقیق ایمنی ترکیبی از حسگرها، حل‌گرهای منطقی و المان‌های نهایی است. به این سیستم همچنین سیستم هماهنگ‌کننده نیز گفته می‌شود. یک سیستم ابزاردقیق ایمنی از لحاظ عملکردی از سیستم کنترل فرایند پایه مستقل است. قابلیت اطمینان یک سیستم ابزاردقیق ایمنی بر اساس احتمال خرابی هنگام نیاز و سطوح یکپارچگی ایمنی تعریف می‌شود.

۷-۷-۲-۵- حفاظت فیزیکی

حفاظت فیزیکی معمولاً به شیرهای اطمینان و تجهیزات مشابه مرتبط است. فاکتورهای زیر برای تعیین میزان اعتبار لازم برای حفاظت فیزیکی به عنوان لایهٔ حفاظت مستقل لحاظ شوند:

- تعیین اندازه (شامل حالت‌های کنترل‌کننده مانند آتش‌سوزی، خرابی توان و ...)،
- طراحی،
- نصب (مثلاً آرایش لوله‌کشی)،
- کیفیت تشخیص و نگهداری،
- تمیزی مایع فرایند (به عنوان مثال سرویس‌های خورنده)،

۷-۷-۲-۶- حفاظت پسا- انتشار

این حفاظ‌ها نوعاً به سدها و دیواره‌های صوتی مرتبط است. این لایه‌های حفاظت مستقل غیرفعال معمولاً قابلیت اطمینان بالایی دارند. همان ملاحظات لیست شده برای حفاظت فیزیکی باید برای این حفاظ‌ها نیز لحاظ شوند.

۷-۷-۲-۷- پاسخ اضطراری تأسیسات و پاسخ اضطراری جامعه

از آنجا که این پاسخ‌ها پس از انتشار اولیه فعال می‌شوند، به صورت عادی به عنوان لایه‌های حفاظت مستقل در نظر گرفته نمی‌شوند. آنچه که ممکن است به عنوان لایهٔ حفاظت مستقل لحاظ شده و یا تعیین شود، در واقع به هیچ وجه لایهٔ حفاظت مستقل نیست. با این حال، فاکتورهایی وجود دارند که به میزان زیادی لایه‌های حفاظت مستقل و احتمال خرابی هنگام نیاز را تحت تأثیر قرار می‌دهند که برخی از آنها در جدول شماره ۳۷ لیست شده‌اند.

جدول شماره ۳۷: عوامل مرتبط با لایه‌های حفاظت مستقل

عوامل	توضیحات
آموزش و مدرک	این فاکتورها در ارزیابی احتمال خرابی هنگام نیاز برای اقدامات اپراتور قابل استفاده هستند، ولی خود آنها لایه‌های حفاظت مستقل نیستند.
رویه‌ها	این فاکتورها در ارزیابی احتمال خرابی هنگام نیاز برای اقدامات اپراتور قابل استفاده هستند، ولی خود آنها لایه‌های حفاظت مستقل نیستند.
تست و تشخیص نرمال	این فعالیت‌ها برای همهٔ ارزشیابی‌های خطر فرض می‌شوند و مبنای قضاوت برای تعیین احتمال‌های خرابی هنگام نیاز هستند. تست و تشخیص نرمال احتمال خرابی هنگام نیاز لایه‌های حفاظت مستقل خاصی را تحت تأثیر قرار می‌دهد. طولانی کردن بازه‌های تست و تشخیص ممکن است احتمال خرابی هنگام نیاز یک لایهٔ حفاظت مستقل را افزایش دهد.
نگهداری	این فعالیت‌ها برای همهٔ ارزشیابی‌های خطر فرض می‌شوند و مبنای قضاوت برای تعیین احتمال‌های خرابی هنگام نیاز هستند. تست و تشخیص نرمال احتمال خرابی هنگام نیاز لایه‌های حفاظت مستقل خاصی را تحت تأثیر قرار می‌دهد.
ارتباطات	در یک تأسیسات وجود ارتباطات کافی مفروض است. ارتباطات ضعیف احتمال خرابی هنگام نیاز لایه‌های حفاظت مستقل خاصی را تحت تأثیر قرار می‌دهد.
علائم	علائم به خودی خود لایه‌های حفاظت مستقل نیستند. علائم ممکن است غیرواضح، نامفهوم بوده و یا چشم‌پوشی شوند. علائم می‌توانند احتمال خرابی هنگام نیاز لایه‌های حفاظت مستقل خاصی را تحت تأثیر قرار دهند.
حفاظت در برابر آتش	اثرگذاری حفاظت در برابر آتش به عنوان یک لایهٔ حفاظت مستقل به سناریوهای پسا- انتشار محدود است و در کاهش پیامدها و اثرات متوالی طی گسترش آتش به میزان زیادی سودمند است. تأسیسات ضدحریق می‌توانند به عنوان یک لایهٔ حفاظت مستقل برای برخی سناریوها با فراهم آوردن الزامات استانداردهای مربوطه استفاده شوند.
دسترسی و قابل فهم بودن اطلاعات	این یک الزام اساسی است و یک لایهٔ حفاظت مستقل را تشکیل نمی‌دهد.

۷-۷-۳- احتمال خرابی هنگام نیاز (PFD)

علل عدم موفقیت لایهٔ حفاظت مستقل می‌تواند ناشی از موارد زیر باشد:

- هنگام وقوع رویداد آغازگر، یک جزء از لایهٔ حفاظت مستقل حالت غیرایمن یا خراب داشته باشد (نوعاً این حالت انعکاسی از اقدامات نگهداری ضعیف است)،
- خرابی یک جزء هنگام انجام وظیفه (نوعاً ناشی از عدم کفایت طراحی، یا نقص در نگهداری و یا عیب‌های کارخانه)،
- مؤثر نبودن مداخله انسانی.

جدول جدول شماره ۳۸ مقادیر نوعی احتمال خرابی هنگام نیاز برای انواع مختلف لایه‌های حفاظت مستقل به کار رفته در تحلیل لایه‌های حفاظت را ارائه می‌کند.

جدول شماره ۳۸: مقادیر احتمال خرابی هنگام نیاز

IPL	Comments	PFD
BPCS	Can be credited as an IPL if not associated with the initiating event being considered (See IEC 61508 and IEF 61511 for additional discussion)	1×10^{-1} to 1×10^{-2} ($> 1 \times 10^{-1}$ allowed by IEC)
Safety Instrumented function	See Chapter 20	See Chapter 20
Dike	Will reduce the frequency of large consequence (widespread spill) of a tank overfill / rupture / spill / etc.	1×10^{-2} to 1×10^{-3}
Blast-wall / Bunker	Will reduce the frequency of large consequences of an explosion by confining blast and protecting equipment / buildings / etc.	1×10^{-2} to 1×10^{-3}
Human action with 10 minutes response time	Simple well-documented action with clear and reliable indications that the action is required	1.0 to 1×10^{-1}
Human response to BPCS indication or alarm with 40 minutes response time	Simple well-documented action with clear and reliable indications that the action is required (The PFD is limited by IEC 61511; IEC 2001)	1×10^{-1} ($> 1 \times 10^{-1}$ allowed by IEC)
Human action with 40 minutes response time	Simple well-documented action with clear and reliable indications that the action is required.	1×10^{-1} to 1×10^{-2}

۷-۸- کاربرد تحلیل لایه‌های حفاظت

۷-۸-۱- نحوهٔ اجرای تحلیل لایه‌های حفاظت

نحوهٔ اجرای تحلیل لایه‌های حفاظت در پاسخ به دو پرسش زیر خلاصه می‌شود.

۱. تحلیل لایه‌های حفاظت چه زمانی انجام می‌شود؟ طی مطالعهٔ PHA[۱] (مانند HAZOP یا What-if) و یا درست پس از آن،
۲. چه کسی می‌تواند تحلیل لایه‌های حفاظت را انجام دهد؟ یک تیم معمولاً کوچک‌تر از تیم PHA شامل تحلیل‌گر آشنا به روش‌شناسی تحلیل لایه‌های حفاظت و یک مهندس فرایند یا متخصص تولید. نتایج مطالعه می‌تواند توسط یک یا چند نفر به صورت مستقل با تخصص معادل و یا بیشتر بازنگری شود.

معیارهای انتخاب سناریوهای به‌کاررفته در تحلیل لایه‌های حفاظت – نوعاً بر شماری از فاکتورها مبتنی است:

- وخامتِ به اندازهٔ کافی زیاد پیامد و احتمال یک سناریو،
- نیاز به کاهش ریسک به سطوح قابل قبول معیار،
- عدم قطعیت فرکانس پیامدهای نهایی برای حالت‌های بحرانی،
- عدم قطعیت پیامدهای حالت‌های بحرانی،
- پیچیدگی سناریوها.

۷-۸-۲- اتخاذ تصمیمات ریسک

پس از تعیین سناریو و محاسبهٔ ریسک موجود، برای تعیین موارد زیر تصمیم‌گیری می‌شود.

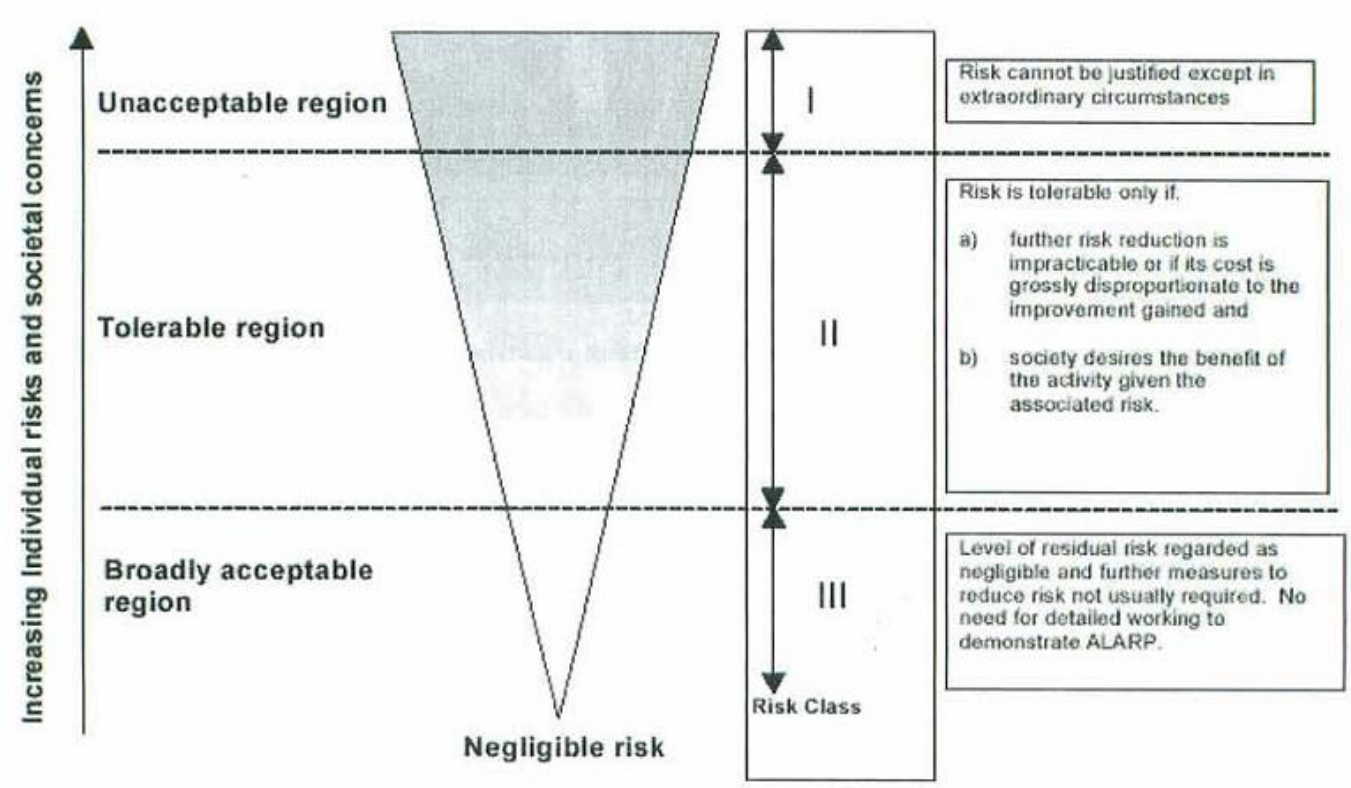
- آیا ریسک موجود قابل تحمل است؟
- آیا مهار ریسک موجود کافی است؟
- چه میزان کاهش ریسک برای کاهش ریسک به سطح قابل قبول لازم است؟

[۱] - Preliminary Hazard Analysis

برای پاسخ به سوالات فوق، لازم است رابطه بین ریسک و کاهش ریسک فهمیده شود. ماهیت مفاهیم ریسک و کاهش ریسک، تعیین هدف یا معیار ریسک قابل تحمل است. بدون معیار ریسک قابل تحمل، ممکن است یک تمایل برای افزودن حفاظ‌ها با این اعتقاد که منجر به افزایش ایمنی می‌شوند، وجود داشته باشد. این امر ممکن است منجر به برخی مسائل شود، از جمله:

- افزودن لایه‌های حفاظت مستقل غیرضروری،
- کاهش تمرکز بر لایه‌های حفاظت مستقل که برای حصول ریسک قابل تحمل ضروری هستند،
- لحاظ ارزش برای لایه‌های حفاظت مستقل که ممکن است مؤثر نباشد.

معیار حداقل میزان معقول عملی، بر اصل کاهش ریسک تا حد معقول عملی مبتنی است. هنگامی که یک ریسک بین نواحی غیرقابل پذیرش و قابل پذیرش قرار می‌گیرد، این اصل می‌تواند برای حصول یک ریسک قابل تحمل در یک کاربرد خاص به کار رود. در شکل ۷۶، سه ناحیه ریسک نشان داده شده است.



شکل ۷۶: ریسک قابل پذیرش و معیار حداقل میزان معقول عملی

به کارگیری اصل حداقل میزان معقول عملی ریسک مستلزم تعریف سه ناحیه بر اساس احتمال و پیامد یک رویداد است. جدول شماره ۳۹ مثالی برای نشان دادن کلاس‌های ریسک است که بر اساس احتمال و پیامد تعریف شده‌اند.

جدول شماره ۳۹: نمونهٔ دسته‌بندی ریسک رویدادها

احتمال	کلاس ریسک			
	پیامد وخیم	پیامد بحرانی	پیامد حدّی	پیامد قابل اغماض
احتمال زیاد	I	I	I	II
محتمل	I	I	II	II
ممکن	I	II	II	II
احتمال کم	II	II	II	III
غیرمحتمل	II	III	III	III
غیرمنتظره	II	III	III	III

جدول شماره ۴۰: شرح کلاس‌های ریسک

کلاس ریسک	شرح
کلاس I	ریسک غیرقابل تحمل
کلاس II	ریسک نامطلوب، و قابل تحمل تنها درصورتی که کاهش ریسک غیرعملی است و یا اگر هزینه‌ها به صورت زیادی با ارتقای ممکن متناسب نباید.
کلاس III	ریسک قابل چشم‌پوشی

رویکردهای نوعی برای مقایسه ریسک موجود با معیار ریسک قابل تحمل از پیش‌تعیین شده عبارتند از:

- روش ماتریس،
- روش معیار عددی،
- روش درجهٔ اعتبار لایهٔ حفاظت مستقل.

برای همهٔ روش‌های فوق، تحلیل هزینه – فایده می‌تواند به تصمیم‌گیری نهایی کاهش ریسک کمک کند.

۷-۸-۲-۱- روش ماتریس

روش ماتریس در مثال جداکننده ارائه شده است.

۷-۸-۲-۲- روش معیار عددی

معیار ریسک تعیین شده با استفاده از این رویکرد، مبتنی بر ریسک قابل تحمل بیشینه به ازای سناریو و مجموعه‌های متنوعی از پیامد مانند موارد زیر است:

- صدمه انسانی (مرگ و میر)،

- اثر محیطی،
- آسیب به خواص،
- زیاد تولید،
- انتشار مواد خطرناک،
- آتش‌سوزی،
- انفجار.

به عنوان مثال، ممکن است یک سازمان معیار ریسک قابل تحمل را به صورت فرکانس بیشینهٔ (به ازای سال یا به ازای ۱۰۰۰ ساعت) یک تلفات تعیین کند.

۷-۸-۲-۳- روش درجهٔ اعتبار لایهٔ حفاظت مستقل

این روش درجهٔ اعتبار لایهٔ حفاظت مستقل برای سناریوهای سطوح پیامد خاص و فرکانس را تعیین می‌کند. بنابراین، معیار قابل تحمل به صورت صریح در این روش نشان داده نمی‌شود. این روش مقدار احتمال خرابی هنگام نیاز برابر $۱۰^{-۲}$ را معادل ۱ درجه اعتبار برای لایهٔ حفاظت مستقل در نظر می‌گیرد. درجهٔ اعتبار تخصیص شده به یک سناریو وابسته به وخامت و فرکانس رویداد است. به عنوان مثال جدول شماره ۴۱ بر صدمه و مرگ و میر انسانی تمرکز دارد. رویکرد مشابهی برای انواع مختلف پیامدها مانند زیان تولید و اثرات زیست محیطی می‌تواند به کار رود. برای لحاظ انواع مختلف پیامدها، محاسبات تحلیل لایه‌های حفاظت نیازمند لحاظ ضرایب اصلاحی مانند فعال‌سازی احتمال‌های رویداد و بهبوددهندگان شرایط در محاسبات فرکانس است.

جدول شماره ۴۱: درجهٔ اعتبار لایهٔ حفاظت مستقل

	درجهٔ اعتبار لازم برای لایهٔ حفاظت مستقل	
فرکانس رویداد آغازگر	پیامد گروه چهار – یک خرابی	پیامد گروه پنج – خرابی‌های چندگانه
فرکانس $\leq ۱۰^{-۲}$	۲	۲/۵
$۱۰^{-۲} <$ فرکانس $\leq ۱۰^{-۳}$	۱/۵	۲
$۱۰^{-۳} <$ فرکانس $\leq ۱۰^{-۴}$	۱	۱/۵
$۱۰^{-۴} <$ فرکانس $\leq ۱۰^{-۶}$	۰/۵	۱
$۱۰^{-۶} <$ فرکانس	۰	۰/۵

۷-۹- مزایای استفاده از تحلیل لایه‌های حفاظت

مزایای استفاده از تحلیل لایه‌های حفاظت عبارتند از:

- نیاز به زمان و منابع کمتر نسبت به روش تحلیل ریسک کیفی داشته، ولی بسیار سخت‌تر از روش HAZOP است،
- سیستم‌های ایمنی فرایند بسیاری با هزینه‌های اضافی بیش از حد برای ایمنی، مهندسی شده‌اند و پیچیدگی غیرضروری دارند. تحلیل لایه‌های حفاظت به تمرکز بر منابع در اغلب سیستم‌های ایمنی بحرانی کمک می‌کند،
- با عمل‌کردن به عنوان یک ابزار اتخاذ تصمیم، به قضاوت سریع‌تر، حل مشکلات و فراهم آوردن پایه عمومی برای تشریح ریسک یک سناریو کمک می‌کند،
- ارتقای شناسایی سناریو با جفت‌سازی علت و پیامد از مطالعات PHA،
- کمک به مقایسه ریسک‌ها،
- کمک به تصمیم‌گیری اگر ریسک در تطابق با الزامات مقررات و یا استانداردها، به میزان حداقل معقول عملی باشد،
- شناسایی عملکردها، سیستم‌ها و فرایندهایی که حفاظت کافی ندارند،
- ایجاد مبنا برای تعیین لایه‌های حفاظت مستقل بر اساس IEC 61511،
- کمک به تصمیم‌گیری در این زمینه که حین عملکرد، نگهداری و آموزش مربوطه، بر کدام حفاظ باید تمرکز شود.
- پشتیبانی از برآوردن مقررات ایمنی فرایند.

۷-۱۰- معایب تحلیل لایه‌های حفاظت

- تحلیل لایه‌های حفاظت به زمان بیشتری نسبت به روش‌های کیفی مانند HAZOP و What-if برای رسیدن به یک تصمیم مبتنی بر ریسک نیاز دارد،
- در قیاس با روش‌های کیفی PHA، تحلیل لایه‌های حفاظت زمان و تلاش بیشتری برای یادگیری نیاز دارد،
- تحلیل لایه‌های حفاظت نیازمند داده‌های نرخ خرابی است. چنین داده‌هایی سخت یافت می‌شوند،
- تحلیل لایه‌های حفاظت برای سناریوهای پیچیده، مانند مواجهۀ اجزای خاموشی چندگانه با رویدادی (مانند آتش‌سوزی یا انتشار مواد سمی) که مستلزم خاموشی کامل تأسیسات است، مناسب نیست.
- تحلیل لایه‌های حفاظت یک ابزار شناسایی خطر نیست. شناسایی سناریوهای خطرناک توسط سایر ابزارها، مانند HAZOP که ارزشیابی ریسک نیمه کمّی فراهم می‌آورد، انجام می‌شود.

۸- جمع‌بندی

در این گزارش سرفصل‌های اصلی مبحث تحلیل ایمنی احتمالاتی ارائه شد. به عبارتی می‌توان گفت این اثر اولین گزارش تهیه شده در مبحث ایمنی احتمالاتی به زبان فارسی است که در آن مطالب اصلی معرفی شده‌اند. بدیهی است تکمیل و ویرایش مداوم یک اثر می‌تواند در ماندگاری و مفید بودن آن تأثیر بسزایی داشته باشد. از این رو در فعالیت‌های آتی برای پوشش‌دهی هر چه بیشتر نیاز کاربران و پرداختن به جزئیات و رفع کاستی‌ها و نارسایی‌های احتمالی ویراست‌های این نسخه تکامل خواهد یافت، به گونه‌ای که همهٔ مباحث خرد و کلان ایمنی احتمالاتی را شامل شود.

فهرست مراجع

1. Ivan Vrbanic, Ivan Kosutic, “Presentation of Common Cause Failures in Fault Tree Structure of Krško PSA: An Historical Overview”, International Conference Nuclear Energy for New Europe, Slovenia, September 8-11, 2003.
2. Nikolaos Limnios, “Fault Trees”, ISTE, 2007.
3. Ajit Kumar Verma, Srividya Ajit, Durga Rao Karanki, “Reliability and Safety Engineering”, Springer, 2010.
4. Mohammad Modarres, “Risk Analysis in Engineering; Techniques, Tools, and Trends”, Taylor & Francis, 2006.
5. Ali Mosleh, “Common Cause Failures: An Analysis Methodology and Examples”, Reliability Engineering and System Safety, 249-292, 1991.
6. “RiskSpectrum Analysis Tools Theory Manual”, Relcon Scandpower, 2008.

پیوست الف: مبانی و ساختار کلی ایمنی هسته‌ای

اصول و اهداف ایمنی هسته‌ای

دو مدرک SF-1 و INSAG12 در زمینهٔ مفاهیم، اهداف و اصول ایمنی هسته‌ای منتشر شده‌اند. مدرک SF-1 شامل بیان اهداف بنیادی ایمنی هسته‌ای، بیان اصول بنیادی ایمنی هسته‌ای و بیان جایگاه آنها است. در مدرک INSAG12 استراتژی‌های ایمنی شامل دفاع در عمق و ملاحظات مربوط به سطوح مختلف آن بیان شده است.

معرفی مدرک SF-1

هدف این مدرک ایجاد و بیان اهداف، اصول و مفاهیم ایمنی است. این مدرک، مبنا و مرجعی برای سایر استانداردهای آژانس انرژی اتمی شامل الزامات و راهنمای ایمنی است.

دامنهٔ این مدرک، شامل اهداف بنیادی ایمنی و نیز ده اصل بنیادی ایمنی تبیین می‌شود. این اصول و اهداف ایمنی در تمامی فعالیت‌هایی که احتمال مخاطرهٔ پرتوگیری رادیواکتیو در آنها وجود دارد، باید اعمال گردد. این اصول بنیادی در طول عمر کلیهٔ تأسیسات و فعالیت‌های هسته‌ای کاربرد داشته و باید رعایت شوند.

ایمنی هسته‌ای به مجموعه‌ای از تمهیدات و اقداماتی اطلاق می‌شود که برای نیل به دو هدف اصلی در پروسه طراحی، ساخت، راه‌اندازی، بهره‌برداری و از کاراندازی تأسیسات هسته‌ای در نظر گرفته می‌شوند. این دو هدف اصلی عبارتند از:

۱. اطمینان از بهره‌برداری و کنترل ایمن تأسیسات هسته‌ای،
۲. اطمینان از حفاظت کارکنان، مردم جامعه و محیط زیست در برابر مخاطرات رادیولوژیک تأسیسات هسته‌ای.

در طبقه‌بندی آژانس بین المللی انرژی اتمی، اهداف ایمنی هسته‌ای خود به سه دسته (یک هدف اصلی و دو هدف تکمیلی) تقسیم می‌شوند:

۱. هدف عمومی ایمنی هسته‌ای، حفاظت از اشخاص، جامعه و محیط زیست از آسیب‌ها، با استقرار و نگهداری دفاع مؤثر در مقابل مخاطرات رادیولوژیکی در تأسیسات هسته‌ای است.
۲. هدف حفاظت در برابر پرتو، اطمینان از این موضوع است که در تمام شرایط بهره‌برداری، پرتوگیری در داخل تأسیسات یا به علت رها شدن مجاز مواد رادیواکتیو از تأسیسات، کمتر از حدود تعریف شده بوده و در حد کمترین

مقدار معقول و مجاز دست‌یافتنی، نگه داشته می‌شود، و نیز اطمینان از کاهش پیامدهای رادیولوژیکی هر حادثه‌ای است.

۳. هدف فنی ایمنی، در نظر گرفتن تمام اقدامات امکان‌پذیر و معقول برای جلوگیری از بروز حوادث در تأسیسات هسته‌ای، و درصورت بروز حوادث هسته‌ای، کاهش پیامدهای ناشی از آن‌ها می‌باشد.

در حال حاضر، آژانس بین المللی انرژی اتمی، با تعریف، تهیه و تدوین اصول و ارکان اساسی ایمنی هسته‌ای، مجموعه‌ای از اهداف، مفاهیم و اصول ایمنی هسته‌ای را تدوین کرده است. این مجموعه:

- مبنایی برای تنظیم ضوابط، مقررات و استانداردهای ایمنی هسته‌ای است،
- مبنای منطقی برای تدوین برنامه جامع و گسترده ایمنی هسته‌ای است،
- یک راهنمای مفید و قابل درک حتی برای افراد غیر متخصص در زمینهٔ ایمنی هسته‌ای (مدیران، مسئولان) است.

هدف بنیادی ایمنی هسته‌ای

حفاظت از افراد (مردم جامعه و پرسنل تأسیسات هسته‌ای) و محیط زیست در برابر تأثیرات مضر و مخرب پرتوهای یون‌ساز است، به گونه‌ای که:

- بدون محدود کردن بی‌مورد فعالیت‌های تأسیسات باشد،
- محدود کردن عملیاتی باشد که ریسک‌های پرتوگیری را افزایش می‌دهند.

در جهت اطمینان از بهره‌برداری ایمن از تأسیسات، اقدامات زیر بایستی صورت پذیرد:

- کنترل پرتوگیری افراد (مردم جامعه و پرسنل تأسیسات) و رهاسازی مواد رادیواکتیو به محیط زیست،
- محدود کردن احتمال وقوع رویدادهایی که ممکن است به از دست دادن کنترل قلب راکتور هسته‌ای، واکنش هسته‌ای زنجیره‌ای، منبع و چشمه رادیواکتیو یا دیگر منابع تشعشع منجر شود،
- مهار پیامدهای رویدادهای بالا، درصورتی‌که حادث شوند.

ایمنی به هر دو مورد ریسک‌های تشعشع در شرایط بهره‌برداری عادی و ریسک‌های تشعشع حاصل از پیامدهای سوانح مرتبط است. همچنین ایمنی به دیگر پیامدهای مستقیم و محتمل از دست دادن کنترل موارد زیر نیز مرتبط است:

- قلب راکتور هسته‌ای،

- واکنش هسته‌ای زنجیره‌ای،
- منبع و چشمه رادیواکتیو،
- دیگر منابع و چشمه‌های تشعشع.

شمول اصول بنیادی ایمنی هسته‌ای عبارت است از:

۱- تأسیسات:

- تأسیسات هسته‌ای،
- تأسیسات کار با پرتوها،
- برخی تأسیسات استخراج و فرآوری مواد خام هسته‌ای، مانند معادن اورانیوم و تأسیسات مدیریت پسمان‌های رادیواکتیو،
- سایر مکان‌هایی که در آنها مواد رادیواکتیو، تولید، فرآوری، استفاده، جابجایی، ذخیره یا دفن می‌شوند و یا جاهایی که مولدهای پرتو نصب می‌شوند.

۲- فعالیت‌ها:

- تولید، استفاده، واردات و صادرات چشمه‌ها برای کاربردهای صنعتی، تحقیقاتی و پزشکی،
- حمل و نقل مواد رادیواکتیو،
- برچیدن تأسیسات، فعالیت‌های مدیریت پسمان‌ها مانند رهاسازی مواد آلوده،
- برخی جنبه‌های بازسازی ساختگاه‌های آلوده به پسمان‌های مربوط به فعالیت‌های گذشته.

اصول بنیادی ایمنی هسته‌ای

نیل به اهداف ایمنی هسته‌ای در ده اصل بنیادی بیان شده است. این ده اصل، پایه و اساس پی‌ریزی سیستم ایمنی هسته‌ای و مدیریت آن در پروژه‌ها و طرح‌های هسته‌ای بوده و از لحاظ حقوقی و فنی الزام‌آور است.

- اصل ۱: مسئولیت ایمنی

مسئولیت اول در ارتباط با ایمنی بر عهدهٔ شخص یا سازمان متولی تأسیسات و فعالیت‌های هسته‌ایی است که ریسک‌های پرتوگیری را افزایش می‌دهند.

سازمان بهره‌بردار مسئولیت‌های زیر را بر عهده دارد:

- ✓ بررسی طراحی مناسب و کیفیت کافی در تأسیسات و تجهیزات وابسته،
- ✓ فراهم نمودن شایستگی‌های مورد نیاز جهت بهره‌برداری،
- ✓ فراهم نمودن اطلاعات و آموزش‌های مورد نیاز،
- ✓ فراهم نمودن دستورالعمل‌ها و ترتیبات نگهداری ایمنی در تمامی شرایط،
- ✓ کنترل‌های مورد نیاز برای مواد رادیواکتیو،
- ✓ کنترل پسماندهای تولیدی رادیواکتیو در تأسیسات.

- اصل ۲: نقش دولت

یک چارچوب مؤثر قانونی و دولتی برای ایمنی همراه با یک نهاد قانونی مستقل باید دایر شده و مورد حمایت قرار گیرد. نقش دولت عبارت است از:

- تصویب قوانین لازم در مجلس جهت احداث و بهره‌برداری از تأسیسات هسته‌ای،
- تأسیس نظام ایمنی هسته‌ای ملی در جهت نظارت بر تأسیسات هسته‌ای با مشخصه‌های ذیل:
  - ✓ دارای اختیارات قانونی با بودجه مستقل و نیروهای خبره و آموزش دیده کافی،
  - ✓ مستقل از سازمان‌های بهره‌بردار،
  - ✓ دارای تمهیدات و یا سیستم‌هایی به منظور تبادل اطلاعات ایمنی با جامعه و دیگر گروه‌های علاقه‌مند،
  - ✓ مشاوره با نخبگان و یا دیگر گروه‌ها در جامعه در یک فضای باز، در یک فرایند فراگیر.

- اصل ۳: رهبری و مدیریت ایمنی

رهبری و مدیریت مؤثر ایمنی باید در سازمان مرتبط، تأسیسات و فعالیت‌هایی که ریسک تشعشع را افزایش می‌دهند، دایر شده و مورد حمایت قرار گیرد.

اصول رهبری و مدیریت ایمنی عبارتند از:

- ✓ رهبری در موضوعات ایمنی باید در بالاترین سطح سازمان نشان داده شود،
- ✓ ایمنی باید با یک سیستم مدیریت مؤثر برآورده شده و باقی نگه‌داشته شود،
- ✓ مسائل ایمنی نباید با موارد دیگر از جمله مسائل فنی و یا اقتصادی مصالحه شود،

- ✓ سیستم مدیریت ایمنی باید فرهنگ ایمنی و ارزیابی‌های منظم ایمنی را ارتقا داده و از تجارب دیگر تأسیسات هسته‌ای استفاده نماید.

- اصل ۴: توجیه‌پذیری تأسیسات و فعالیت‌ها

تأسیسات و فعالیت‌هایی که ریسک تشعشع را افزایش می‌دهند، باید در نهایت دارای یک منفعت باشند. تأسیسات هسته‌ای و یا فعالیت‌هایی که خطر ریسک تشعشع دارند باید دارای منفعتی باشند که بر خطرات آن رجحان داشته و آنرا توجیه کند. به منظور ارزیابی ریسک و یا منفعت‌های آن، بایستی تمام پیامدهای با اهمیت در بهره‌برداری تأسیسات و یا آن فعالیت در نظر گرفته شود.

در بسیاری از موارد این تصمیمات در بالاترین سطح دولت گرفته می‌شود، مانند احداث نیروگاه هسته‌ای، و در برخی موارد تصمیم بر عهده نظام ایمنی است.

پرتودهی بیماران در مراکز تشخیصی - درمانی یک نمونه استثناء است که منفعت‌های آن برای بیماران است. توجیه این مراکز با توجه به مسائل فنی پرتودهی (حفاظ سازی، آموزش و ...) و دستورالعمل‌های خاص آنها مورد بررسی قرار می‌گیرند.

- اصل ۵: بهینه‌سازی حفاظت

حافظت باید به منظور فراهم آوردن بالاترین سطح ایمنی که موجّه و قابل حصول است، بهینه شود. بهینه‌سازی حفاظت مستلزم قضاوتی است که بستگی به موارد زیر دارد:

- ✓ تعداد نفراتی (کارکنان و عموم مردم جامعه) که ممکن است تحت تأثیر قرارگیرند،
- ✓ میزان احتمال تحت تابش قرار گرفتن،
- ✓ مقدار و توزیع دُزی که دریافت می‌کنند،
- ✓ ریسک ناشی از حوادث قابل پیش‌بینی،
- ✓ فاکتورهای اقتصادی، اجتماعی و محیطی.

- اصل ۶: محدودسازی ریسک‌ها برای افراد

اقدامات کنترل مخاطرات تشعشع باید این اطمینان را ایجاد کند که هیچ مورد خاصی موجب به وجود آمدن ریسک غیرقابل قبولی از آسیب نمی‌شود. توجیه و بهینه‌سازی حفاظت نمی‌تواند در ذات خود تضمین کند که هیچ شخصی یک ریسک

غیرقابل قبول از خطر دریافت نمی‌کند. محدودیت‌های دُز و ریسک نشانگر یک حد مجاز تعیین شده است که به تنهایی برای حفاظت کافی نیستند، بلکه هم بهینه‌سازی حفاظت و هم محدودیت‌های دوز و ریسک برای نیل به سطح ایمنی مورد نظر ضروری هستند.

- اصل ۷: حفاظت از نسل‌های امروز و آینده

افراد و محیط زیست، در زمان حال و آینده، باید در برابر ریسک‌های تشعشع محافظت شوند. ریسک تشعشعات ممکن است از مرزها فرار رفته و همچنین برای دورهٔ زمانی طولانی باشد. نتایج احتمالی آن در حال حاظر و آینده باید مبنای قضاوت برای کافی بودن تمهیدات کنترل ریسک ناشی از تشعشعات باشد. به ویژه، استانداردهای ایمنی اعمال شده نه فقط برای جمعیت محلی، بلکه برای جمعیت گذرا در تأسیسات و فعالیت‌ها در نظر گرفته شود.

- اصل ۸: پیشگیری از حوادث

تمام تلاش‌های ممکن برای پیش‌گیری و مهار حوادث هسته‌ای و رادیولوژیکی باید انجام شوند. بیشترین پیامدهای مضر که از تأسیسات و فعالیت‌های هسته‌ای حاصل می‌شوند، مربوط به:

- ✓ عدم کنترل قلب راکتور هسته‌ای
- ✓ عدم کنترل واکنش زنجیره‌ای
- ✓ عدم کنترل چشمه‌های رادیواکتیو و دیگر منابع تابش‌های هسته‌ای

می‌باشند. بنابراین، برای کاهش احتمال حوادثی از نوع باید تمهیداتی به قرار زیر در نظر گرفته شود:

- جلوگیری از وقوع نقص و یا ایجاد شرایط غیرعادی
- جلوگیری از گسترش شرایط غیرعادی و نقص‌ها
- جلوگیری از عدم کنترل منابع رادیواکتیو و یا دیگر چشمه‌های تشعشع

ابزار مقدماتی برای این کار، اعمال استراتژی دفاع عمقی در طراحی می‌باشد. فلسفه دفاع عمقی با ترکیب مناسبی از تمهیدات زیر به وجود می‌آید:

- ایجاد یک سیستم مدیریت مؤثر با تعهد قوی به فرهنگ ایمنی

- انتخاب سایت مناسب به همراه طراحی و مهندسی خوب با توجه به مرزهای ایمنی و الزامات قابلیت اطمینان که می‌توان شامل موارد زیر باشد:
  - ✓ طراحی، تکنولوژی و مواد با بالاترین کیفیت و قابلیت اطمینان
  - ✓ کنترل، سیستم‌های حفاظتی و تمهیدات نظارت و مراقبت
  - ✓ یک ترکیب مناسب از تمهیدات ایمنی ذاتی و مهندسی (سیستم‌های ایمنی)
- دستورالعمل‌ها و قواعد مهندسی جامع برای بهره‌برداری و مدیریت حوادث
- اصل ۹: آمادگی و واکنش اضطراری

باید برنامه‌هایی برای آمادگی و واکنش اضطراری در برابر سوانح هسته‌ای و رادیولوژیکی تهیه شوند. اهداف ابتدایی از داشتن برنامهٔ اضطراری:

- ✓ حصول اطمینان از آمادگی برای پاسخ به حوادث در سطوح سایت، منطقه و ملی،
- ✓ حصول اطمینان از اینکه برای رخدادهای قابل پیش‌بینی و منطقی ریسک‌های تشعشعات خیلی پایین خواهد بود،
- ✓ برای هر رخدادی که حادث شود، تمهیدات عملی برای مهار نتایج آن به افراد، جامعه و محیط زیست فراهم شود.

وظیفه سازمان بهره‌بردار با همکاری نظام ایمنی، مسئولین محلی و دولت است که این برنامه‌های اضطراری را در سه سطح محلی، منطقه و ملی فراهم نمایند. دامنه و وسعت این برنامه‌های اضطراری به موارد ذیل بستگی دارد:

- ✓ احتمال وقوع حوادث و نتایج آن،
- ✓ مشخصه‌های ریسک‌های تشعشعات،
- ✓ ماهیت و محل احداث تأسیسات و یا فعالیت‌های پرتویی.
- اصل ۱۰: اقدامات حفاظتی برای کاهش ریسک‌های تشعشع غیرقانونی

اقدامات حفاظتی برای کاهش ریسک‌های تشعشع غیرقانونی (که تحت نظارت‌های قانونی نیستند) یا موجود، بایستی توجیه شده و بهینه شوند. ریسک تشعشعات ممکن است در محل‌هایی رخ دهد که در کنترل نظام ایمنی نباشد. در چنین موقعیت‌هایی اگر ریسک تشعشعات بالا باشد، توجهات لازم و یا عملیات حفاظتی باید به طور منطقی برای کاهش این‌گونه ریسک نیز انجام شود. به عنوان مثال، یک نمونه ریسک ناشی از منبع طبیعت، پرتوگیری از گاز رادون در برخی معادن و نمونهٔ دیگر، تأسیسات معدن‌کاری رها شده که قبلاً در حال کار بوده است، می‌باشد.

استراتژی دفاع عمقی

مفهوم دفاع عمقی در ایمنی هسته‌ای، عبارت است از فراهم کردن حفاظت‌های مستقل چندگانه (سدهای ایمنی) در برابر وقوع حوادث و گسترش آنها، به طوریکه اگر یکی از آنها در ایفای نقش خود ناموفق باشد، حداقل دیگری بتواند نقش خود را به درستی ایفا کند، درحالی‌که سد دوم مستقل از عملکرد سد اولی باشد. دفاع عمقی بر مبنای چهار سد اصلی در برابر رهایش محصولات رادیواکتیو به خارج از نیروگاه استوار است:

- ✓ شبکه سوخت،
- ✓ غلاف سوخت،
- ✓ مدار اولیه تحت فشار خنک‌کننده راکتور،
- ✓ محفظهٔ ایمنی.

دفاع عمقی شامل پنج سطح دفاعی است که به منظور بهترین استفاده از این سدها به کار می‌روند. سطوح دفاعی در استراتژی دفاع عمقی و تمهیدات فنی و اجرایی ایمنی هر سطح در جدول شماره ۴۲ و جدول شماره ۴۳ ارائه شده‌اند.

جدول شماره ۴۲: سطوح دفاعی در استراتژی دفاع عمقی

سطح دفاعی	هدف	ابزارهای لازم
سطح ۱	پیش‌گیری از وقوع عملکرد غیرعادی و خرابی‌ها	طراحی محافظه‌کارانه و کیفیت بالای ساخت و بهره‌برداری
سطح ۲	کنترل عملکرد غیرعادی و کشف خرابی‌ها	سیستم‌های کنترلی، محدودکننده و حفاظتی، و مشخصات نظارتی دیگر
سطح ۳	کنترل حوادث لحاظ شده در مبنای طراحی	سیستم‌های ایمنی و دستورالعمل‌های حادثه
سطح ۴	کنترل حوادث شدید و شرایط نیروگاه، شامل پیش‌گیری از پیشرفت حادثه و مهارکردن پیامدهای حادثه	اقدامات اضافی و مدیریت حادثه
سطح ۵	مهارکردن پیامدهای رادیولوژیکی مربوط به رهاسازی قابل توجه محصولات رادیواکتیو	برنامه اضطراری خارج از سایت

جدول شماره ۴۳: تمهیدات فنی و اجرایی ایمنی در سطوح مختلف دفاع عمقی (۴. کلاس بندی)

سطح دفاعی	تمهیدات فنی و اجرایی
سطح ۱: جلوگیری از ایجاد اختلال در عملکرد عادی تأسیسات هسته‌ای	مکان‌یابی برای احداث تأسیسات تعیین محدوده تحت حفاظت و کنترل در اطراف سایت

	طراحی تأمین کیفیت لازم برای تجهیزات و فعالیت‌ها بهره‌برداری از تأسیسات طبق الزامات موجود در دستورالعمل‌های فنی و بهره‌برداری حفظ سیستم‌ها و تجهیزات مهم برای ایمنی در وضعیت سالم (بازرسی، عیب یابی، تعویض قطعات و ...) آموزش کارکنان (تأمین سطوح لازم علمی و عملی پرسنل برای بهره برداری در رژیم‌های مختلف و ایجاد فرهنگ ایمنی)
سطح ۲: جلوگیری از وقوع حوادث لحاظ شده در مبنای طراحی به کمک سیستم‌های بهره‌برداری نرمال	تعیین انحراف از عملکرد عادی و رفع آن کنترل و هدایت سیستم‌ها در بهره‌برداری در حالت انحراف
سطح ۳: جلوگیری از وقوع حوادث ورای طراحی به کمک سیستم‌های ایمنی	جلوگیری از تبدیل رویدادهای اولیه به حوادث مبنای طرح و تبدیل حوادث مبنای طرح به حوادث ماورای طراحی به کمک سیستم‌های ایمنی کاهش عواقب ناشی از حوادثی که مهار آن حاصل نشده است، به روش محصور کردن محصولات رادیواکتیو ناشی از شکافت
سطح ۴: هدایت و کنترل حوادث ورای طراحی	جلوگیری از گسترش حادثه و کاهش عواقب آن حفاظت محفظه ایمنی بازگرداندن تأسیسات هسته‌ای به وضعیت قابل کنترل (واکنش زنجیره‌ای متوقف شده، خنک‌سازی سوخت به صورت مداوم انجام شده و مواد رادیواکتیو در محدوده مشخص محصور شوند)
سطح ۵: برنامه‌ریزی مقابله با حوادث	آماده‌سازی و اجرای برنامه مقابله با حوادث در داخل و خارج سایت

از میان مقرراتی که برای اطمینان از پیاده‌سازی صحیح سطح دفاعی ۱ ضروری است، می‌توان به موارد زیر اشاره کرد:

- ✓ تعریف روشن از شرایط بهره‌برداری عادی و غیرعادی،
- ✓ تعیین حاشیه‌های ایمنی کافی در طراحی سیستم‌ها و تجهیزات، شامل حاشیه‌هایی که به استحکام و مقاومت آنها در حوادث مرتبط است،
- ✓ مشخصات ایمنی ذاتی نیروگاه، مانند پایداری هسته‌ای و ترموهیدرولیکی و اینرسی حرارتی سیستم خنک‌کننده،

- ✓ وضع مقررات طراحی به منظور فراهم‌کردن زمان کافی برای بهره‌برداران جهت عکس‌العمل به رویدادها و اطمینان از ارتباط مناسب انسان و ماشین، شامل ابزارهای پشتیبانی بهره‌برداری به منظور تسهیل امور،
- ✓ انتخاب دقیق مواد و استفاده از فرایندهای تولیدی مناسب، همراه با به کار گیری گسترده آزمایش‌های فنی،
- ✓ انتخاب صحیح و آموزش کامل و جامع کارکنان بهره‌برداری، نگهداری، مهندسی و مدیریت. کسب اطمینان از رفتار این کارکنان مطابق با فرهنگ ایمنی ضروری است،
- ✓ ایجاد دستورالعمل‌های بهره‌برداری مناسب و کنترل مطمئن وضعیت نیروگاه و شرایط بهره‌برداری آن،
- ✓ ثبت، ارزیابی و استفاده از تجربیات بهره‌برداری،
- ✓ نگهداری پیش‌گیرانه کامل، همراه با رعایت اولویت‌هایی که بر مبنای اهمیت ایمنی و الزامات قابلیت اطمینان سیستم‌ها مشخص شده است.

اصول طراحی زیر، به منظور اطیمنان از وجود یک سطح قابلیت اطمینان بالا در سیستم‌های ایمنی نیروگاه (سطح ۳)، در پروسه طراحی در نظر گرفته می‌شوند:

- ✓ رعایت افزونگی در سیستم‌ها،
- ✓ پیش‌گیری از خرابی‌های با عامل مشترک ناشی از رویدادهای خارجی و داخلی از طریق جداسازی فیزیکی یا فضایی و محافظ‌های سازه‌ای،
- ✓ پیش‌گیری از خرابی‌های با عامل مشترک ناشی از طراحی، تولید، ساخت، راه‌اندازی، نگهداری و یا دیگر خطاهای انسانی از طریق تنوع یا افزونگی عملکردی،
- ✓ خودکارسازی به منظور کاهش آسیب‌پذیری ناشی از خطاهای انسانی، حداقل در مرحله آغازین یک رویداد غیرعادی و یا یک حادثه،
- ✓ معماری کاملی که تست‌های متناوب را به منظور اطمینان از کارایی سیستم‌ها و کارکرد سیستم‌ها در موقع نیاز، تسهیل نماید،
- ✓ کیفیت سیستم‌ها، تجهیزات و سازه‌ها برای کار در شرایط محیطی خاص که ممکن است به علت وقوع یک حادثه یا رویداد خارجی به وجود آمده باشند،
- ✓ افزایش قابلیت اطمینان سیستم‌های کمکی و پشتیبان، تا سطح مورد نیاز سیستم‌های ایمنی نیروگاه در طراحی، ساخت، راه‌اندازی و بهره‌برداری.

اهداف ضروری مدیریت حادثه (سطح ۴) که شامل تمهیدات پیش‌گیرانه و محافظتی است، عبارتند از:

- ✓ پایش پارامترها و مشخصات اصلی وضعیت نیروگاه،
- ✓ کنترل وضعیت زیربحرانی بودن قلب،
- ✓ خنک‌سازی مجدد قلب و حفظ فرایند خنک‌سازی بلندمدت،
- ✓ محافظت از یکپارچگی محفظهٔ ایمنی (شامل مشخصات نشت)، اطمینان از برداشت حرارت و پیش‌گیری از وارد شدن بارها و تأثیرات خطرناک بر روی محفظهٔ ایمنی و تمام نقاطی که امکان نشت از آنجا وجود دارد، در حالتی که آسیب جدی به قلب وارد شده است و یا حادثه وخیم‌تر شده است.
- ✓ به دست آوردن مجدد کنترل نیروگاه به منظور جلوگیری از آسیب‌های بیشتر.

کلاس‌بندی سیستم‌های ایمنی از لحاظ نوع کارکرد

سیستم‌های ایمنی از لحاظ نوع کارکرد به صورت زیر کلاس‌بندی می‌شوند:

- **سیستم‌های محافظت‌کننده:** توقف مطمئن راکتور در زمان حادثه و برقراری شرایط زیربحرانی در تمام رژیم‌های کاری از جمله حوادث مبنای طراحی،
- **سیستم‌های محصورکننده:** حفظ مواد رادیواکتیو و اشعه در محدودهٔ مرزهای مشخص هنگام حادثه،
- **سیستم‌های تأمین‌کننده (پشتیبان):** تأمین‌کنندهٔ انرژی، سیال کاری و شرایط مورد نیاز کار سیستم‌های ایمنی،
- **سیستم‌های هدایت‌کننده و کنترل‌کننده:** هدایت و کنترل سیستم‌های ایمنی.

کلاس‌بندی سیستم‌های ایمنی از لحاظ تأثیر اجزای مختلف به صورت زیر انجام می‌شود:

کلاس ایمنی ۱

- سوخت،
- اجزایی که خرابی آنها می‌تواند باعث رویدادهای آغازگری شود که حوادث ورای طراحی را در پی دارند (با وجود عملکرد طبق طراحی سیستم‌های ایمنی) و منجر به آسیب به اجزای سوخت و نقض حدود تعیین شده برای حوادث مبنای طراحی می‌شوند.

کلاس ایمنی ۲

- اجزایی که خرابی آنها باعث وقوع رویدادهای آغازگر منجر به آسیب به سوخت در محدودهٔ تعیین شده در حوادث مبنای طراحی می‌شود، مشروط به اینکه سیستم‌های ایمنی به صورت مناسب عمل کنند،
- اجزای سیستم‌های ایمنی که خرابی منفرد (single failure) آنها موجب ناکارامدی عملکرد سیستم‌های مرتبط می‌شود.

کلاس ایمنی ۳

- سیستم‌های مهم برای ایمنی که در کلاس‌های ۱ و ۲ قرار ندارد،
- اجزای حاوی مواد پرتوزا که نشت آنها در اثر خرابی به محیط، از جمله فضاهای سایت، باعث عدول از مقادیر تعیین شده در استانداردهای ایمنی پرتویی می‌شود.

کلاس ایمنی ۴

- اجزایی که مربوط به کار در شرایط نرمال بوده و بر ایمنی تأثیرگذار نیستند و در کلاس‌های ایمنی ۱ تا ۳ گنجانده نشده‌اند.

مراحل مختلف احداث نیروگاه هسته‌ای

مراحل مختلف احداث نیروگاه هسته‌ای عبارت است از:

- امکان سنجی (Feasibility Study)،
- انتخاب و ارزیابی سایت (Site Selection And Evaluation)،
- طراحی مفهومی، پایه و تفصیلی، (Conceptual, Basic and Detailed Design)،
- خرید تجهیزات (Procurement)،
- ساخت و نصب تجهیزات (Construction and Installation)،
- راه‌اندازی (Commissioning)،
- بهره‌برداری (Operation)،
- ازکاراندازی (Decommissioning).

نقش نظام ایمنی هسته‌ای در مراحل ساخت نیروگاه هسته‌ای

- ✓ نظام ایمنی هسته‌ای، ضوابط، مقررات و الزامات ایمنی را تهیه و تدوین نموده و ابلاغ می‌نماید.
- ✓ نظام ایمنی در تمامی مراحل احداث نیروگاه بر فرایند کارها، از طریق بازررسی و صدور مجوز، نظارت می‌کند.
- ✓ نظام ایمنی از برنامه‌های تحقیقاتی مداوم ایمنی حمایت می‌کند که این برنامه‌ها هم به صورت بومی و هم به صورت بین‌المللی می‌توانند اجرا شوند.
- ✓ هر نیروگاه قدرت باید اطلاعات تفصیلی برای تضمین ایمن بودن طراحی، ساخت و بهره‌برداری از آن نیروگاه، برای کارکنان، افراد جامعه و محیط زیست را برای اخذ یک مجوز، تهیه نماید.
- ✓ پس از اخذ مجوز، برنامهٔ بازرسی از نیروگاه توسط نظام ایمنی هسته‌ای، توجه مداوم به ایمنی و سلامتی افراد جامعه، حفاظت از محیط زیست و امنیت مواد و تأسیسات هسته‌ای را تضمین می‌کند.
- ✓ نظام ایمنی هسته‌ای بازررسی‌های عادی را هدایت می‌کند.
- ✓ نظام ایمنی به هر نوع حادثه، رویداد غیرعادی یا حتی ادعاهای رویدادهای غیرعادی که ممکن است در خلال بهره‌برداری از نیروگاه قدرت اتفاق بیفتد، رسیدگی می‌کند.
- ✓ نظام ایمنی بازرسی‌های مستقر در هر نیروگاه هسته‌ای قدرت، فعالیت‌های دارنده مجوز را مورد مشاهده و پایش قرار می‌دهند.
- ✓ نظام ایمنی نسبت به رویدادهای بهره‌برداری در هر نیروگاه واکنش یا پاسخ لازم را صادر می‌کند.

استانداردها و راهنماها

- ✓ یک ساختار قانونی، باید برای تنظیم کردن فعالیت‌های هسته‌ای تصویب شود.
- ✓ نهاد قانون‌گذار باید قوانینی را وضع کند که مسئولیت اصلی ایمنی را به تشکیلات بهره‌بردار اختصاص دهد.
- ✓ نهاد قانون‌گذار باید یک نظام ایمنی تأسیس کند که مسئول صادر کردن پروانه کنترلی منظم فعالیت‌های هسته‌ای باشد.
- ✓ نهاد قانون‌گذار یک کشور باید در اصطلاحات عمومی، سطوح ایمنی را تعریف کند. برای مثال طبقه‌بندی‌های تأسیسات هسته‌ای، بزرگی دامنه، مقدار و احتمال بیشینهٔ رهایش مواد رادیواکتیو در حادثه با یک دید متعادل شده نسبت به خطرات و منافع.
- ✓ مسئولیت نظام ایمنی: ۱- تهیه و تدوین اهداف و استانداردهای ایمنی تفصیلی، ۲- نظارت بر حسن اجرای آنها.

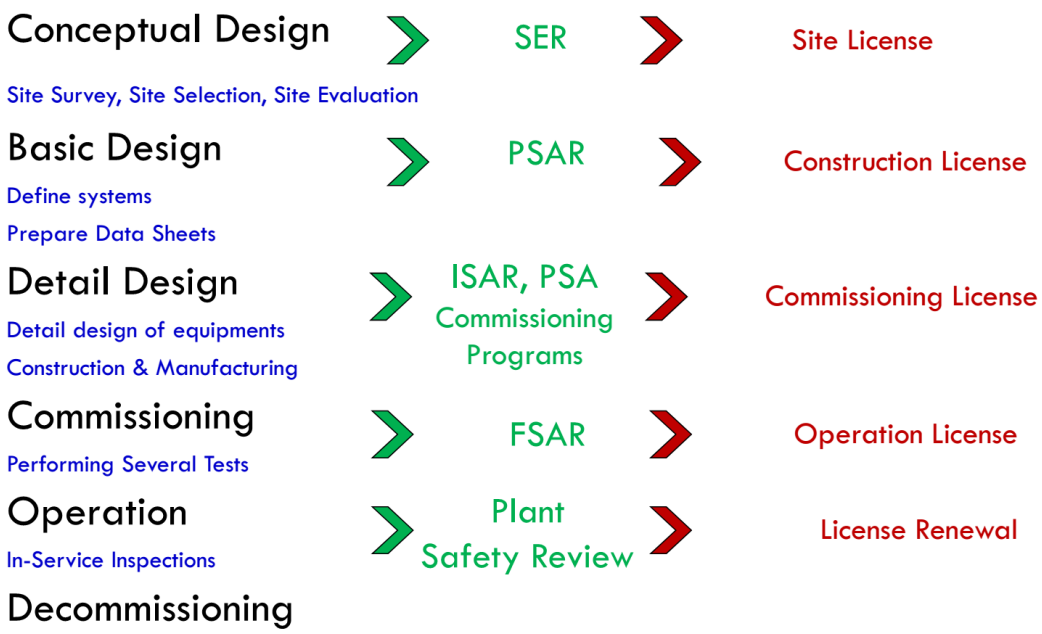
- ✓ به منظور اطمینان از عدم فشارهای غیرضروری، نظام ایمنی از تشکیلاتی که فعالیت‌های هسته‌ای را توسعه می‌دهند، به صورت مؤثری مستقل باشد.
- ✓ یک وظیفهٔ مهم نظام ایمنی اطلاع‌رسانی در خصوص ایمنی و مخصوصاً تصمیمات مهم و قانونی به مردم است.

انواع مدارک ایمنی اخذ پروانه

مدارک اصلی مرتبط با ایمنی نیروگاه بر طبق شرایط خاص هر کشور متفاوت است.

مدارک مهم برای اخذ پروانه‌های مختلف از نظام ایمنی هسته‌ای که باید توسط بهره‌بردار تهیه و تدوین شوند، عبارتند از:

- گزارش تحلیل ایمنی (SAR: Safety Analysis Report)،
- گزارش ارزیابی ایمنی احتمالاتی (PSA: Probabilistic Safety Analysis)،
- گزارش ازریابی اثر زیست محیطی (SER: Site Evaluation Report)،
- برنامهٔ اضطراری خارجی (Offsite Emergency Plan)،
- دستورالعمل عملیات، شامل روش‌های کار اضطراری،
- مدرک سازماندهی عملیات،
- برنامه تست قبل راه اندازی نیروگاه،
- مشخصات فنی برای کار نیروگاه،
- بازدیدهای دوره‌ای ایمنی،
- مدارک تضمین کیفیت (QA: Quality Assurance)،



شکل ۷۷: مراحل طراحی نیروگاه و تهیه گزارش‌ها و مجوزهای مربوطه

گزارش تحلیل ایمنی

گزارش تحلیل ایمنی یک مدرک اصلی برای شرح این است که طراحی و ساخت یک نیروگاه هسته‌ای به نحوی است که نیروگاه می‌تواند بدون ریسک قابل توجه برای کارگران و عموم جامعه کار کند. گزارش تحلیل ایمنی یک مدرک زنده است که به مرور زمان رشد کرده و با زمان تغییر می‌کند. فاکتورهای اصلی این تغییر عبارتند از: پیشرفت طراحی تفصیلی، تغییرات طراحی تصمیم گرفته شده در طول ساخت و عملکرد نیروگاه و نیاز به تطبیق با پیشرفت مبحث ایمنی.

مراحل اصلی گزارش تحلیل ایمنی عبارتند از:

- گزارش تحلیل ایمنی پایه: باید بعد از اتمام طراحی پایه برای دریافت مجوز ساخت نیروگاه ارائه شود.
- گزارش تحلیل ایمنی میانی: باید بعد از اتمام طراحی تفصیلی برای دریافت مجوز راه‌اندازی نیروگاه ارائه شود.
- گزارش تحلیل ایمنی نهایی: باید بعد از اتمام فاز راه‌اندازی برای دریافت مجوز بهره‌برداری نیروگاه ارائه شود.

استانداردها و راهنماها برای تهیه و بازبینی مدارک در جدول شماره ۴۴ ارائه شده است.

جدول شماره ۴۴: استانداردها و راهنماها برای تهیه و بازبینی مدارک

استاندارد و راهنما برای تهیه‌کنندگان مدارک: طراحان (مهندسان طراح) + نهادها یا افراد درگیر در راه‌اندازی (کارشناسانی که کار تست و راه‌اندازی را انجام می‌دهند)	استاندارد و راهنما برای بازبینی‌کنندگان مدارک : نهادهای حکومتی (دولت و مجلس) + نهادهای قانونی (سازمان انرژی اتمی و نظام ایمنی هسته‌ای) + نهادهای نظارتی (آژانس بین‌المللی انرژی اتمی و ...)
International: SAFETY GUIDE No. GS-G-4.1: IAEA Safety Standards Series "Format and Content of the Safety Analysis Report for Nuclear Power Plants" National: RG-1.70 "Standard Format and Content of Safety Analysis Reports for NPPS" RG-1.206 "Combined License Applications For Nuclear Power Plants"	National: NUREG-0800 "Standard Review Plan"

سرفصل‌های گزارش تحلیل ایمنی

- ✓ فصل اول: مقدمه و توصیف کلی نیروگاه،
- ✓ فصل دوم: مشخصات سایت،
- ✓ فصل سوم: طراحی سازه‌ها، ساختمان‌ها، سیستم‌ها و تجهیزات،
- ✓ فصل چهارم: راکتور،
- ✓ فصل پنجم: سیستم خنک‌کننده راکتور و سیستم‌های مرتبط،
- ✓ فصل ششم: سیستم‌های ایمنی،
- ✓ فصل هفتم: سیستم‌های کنترل و ابزار دقیق،
- ✓ فصل هشتم: سیستم‌های الکتریکی،
- ✓ فصل نهم: سیستم‌های کمکی،
- ✓ فصل دهم: سیستم‌های تبدیل قدرت و بخار،
- ✓ فصل یازدهم: مدیریت پسمان‌های رادیواکتیو،
- ✓ فصل دوازدهم: حفاظت در برابر پرتو،
- ✓ فصل سیزدهم: تشکیلات بهره‌برداری و هدایت آن،
- ✓ فصل چهاردهم: برنامه‌های تست اولیه و راه‌اندازی،

- ✓ فصل پانزدهم: تحلیل حوادث،
- ✓ فصل شانزدهم: مشخصات فنی (حدود و شرایط بهره‌برداری)،
- ✓ فصل هفدهم: تضمین کیفیت،
- ✓ فصل هجدهم: مهندسی فاکتورهای انسانی،
- ✓ فصل نوزدهم: ارزیابی ایمنی احتمالاتی و ارزیابی حوادث وخیم،
- ✓ فصل بیستم: ازکاراندازی و جنبه‌های پایان عمر نیروگاه.

بررسی و ارزیابی ایمنی هسته‌ای

- ارزیابی

ریسک پرتویی نسبت به کارکنان، افراد جامعه و محیط زیست که در اثر استفاده از مواد پرتوزا و بهره‌برداری از تأسیسات هسته‌ای ناشی شود، باید ارزیابی و درصورت لزوم کنترل شود.

کاربردهای مواد پرتوزا شامل استفاده‌های پزشکی و صنعتی از چشمه‌های مواد پرتوزا می‌شود. همچنین بهره‌برداری از راکتورهای هسته‌ای (قدرت و تحقیقاتی)، تولید، حمل و نقل مواد پرتوزا و سوخت هسته‌ای، مدیریت پسمانهای پرتوزا و سوخت مصرف شده نیز در زمره فعالیت‌هایی هستند که ریسک پرتو و ایمنی آنها باید مورد ارزیابی قرار گیرد.

- نظارت

نظارت بر ایمنی هسته‌ای و پرتویی یک وظیفه ملی است، ولی از آنجا که ریسک پرتویی بدون مرز است، همکاری‌های بین‌المللی برای ارتقای جهانی ایمنی از ابتدای استفاده از پرتوها شکل گرفته است. این همکاری‌ها برای کنترل و محدودسازی ریسک پرتویی در حالت‌های عادی کارکرد تأسیسات، پیش‌گیری از وقوع حوادث، آمادگی و مقابله در برابر حوادث، کاهش اثرات زیانبار و مدیریت حوادث وخیم است.

در واقع ارزیابی ایمنی ابزاری برای بررسی تطابق تأسیسات و فعالیت‌های هسته‌ای با الزامات ایمنی و پرتویی و نیز، تعیین اقداماتی است که باید برای حصول اطمینان از ایمنی انجام شوند.

- مبحث ارزیابی ایمنی

ارزیابی ایمنی یک فرایند سیستماتیک و مستمر است که در سراسر عمر تأسیسات هسته‌ای (مراحل انتخاب سایت، طراحی، ساخت و نصب، راه‌اندازی، بهره‌برداری، ازکاراندازی و خروج از کنترل‌های قانونی) و تمام طول فعالیت‌های هسته‌ای و پرتویی با هدف حصول اطمینان و برآورده شدن اصول و الزامات مربوطه ادامه پیدا می‌کند.

سازمان‌های دارنده مجوز/پروانه که مسئول نهایی ایمنی تأسیسات و فعالیت‌های هسته‌ای و پرتویی می‌باشند، باید ارزیابی ایمنی را انجام داده و آن را مستندسازی نمایند. این ارزیابی باید جهت بررسی و راستی‌آزمایی مستقل به واحد قانونی هسته‌ای ارسال گردند.

ارزیابی ایمنی بخش اصلی فرایند صدور مجوز/پروانه می‌باشد. ممکن است برای راستی‌آزمایی و مشاهده برخی از مواردی که در گزارشات ارزیابی بدانها اشاره شده است، بازرسی نیز صورت گیرد.

هر زمانی که باید در مورد موضوعات مرتبط با ایمنی تأسیسات و یا فعالیت‌های هسته‌ای و پرتویی تصمیم‌گیری شود (از قبیل اعمال تغییرات مرتبط با ایمنی در تأسیسات، تمدید اعتبار مجوز/پروانه، وقوع رخدادها و حوادث و ...)، نیاز به ارزیابی ایمنی می‌باشد. بنابراین، اطلاعات کافی و ضروری در مورد تجهیزات، سیستم‌ها و یا اقدامات مزبور و چگونگی برآورده شدن الزامات مربوطهٔ ایمنی، باید به صورت مکتوب و تحت عنوان گزارش ارزیابی ایمنی ارائه گردند.

فرایند ارزیابی ایمن به طور کامل یا جزئی با در نظر گرفتن رویکرد اولویت‌بندی در خلال بهره‌برداری از تأسیسات و یا انجام فعالیت‌های هسته‌ای و پرتویی در موارد زیر تکرار می‌شود:

- اعمال تغییرات مهم از نظر ایمنی در طراحی تجهیزات و سیستم‌ها،
- تغییرات در الزامات واحد قانونی،
- اعمال تجارب بهره‌برداری،
- بررسی اثرات استهلاک تجهیزات،
- بررسی امکان تمدید پروانه/مجوزهای صادر شده برای بهره‌برداری طولانی‌تر،
- وقوع رویدادها یا حوادث در تأسیسات.

برای حصول اطمینان از استمرار بهره‌برداری ایمن از تأسیسات و انجام فعالیت‌های هسته‌ای و پرتویی، بررسی دوره‌ای ایمنی انجام می‌شود. بازه زمانی این ارزیابی‌ها به وضعیت تأسیسات و سازمان بهره‌بردار آنها بستگی داشته و بنا به تشخیص واحد قانونی تعیین می‌گردد.

ابزار اولیه حصول اطیمنان حداکثری از ایمنی، اجرای اصل دفاع عمقی می‌باشد. توجه و رعایت این اصل در ارزیابی ایمنی، ضروری است.

میزان وارد شدن به جزئیات در ارزیابی ایمنی باید بر اساس رویکرد اولویت بندی باشد. در این رویکرد، برای ارزیابی تأسیسات و فعالیت‌های هسته‌ای و پرتویی، پیچیدگی و کمال آنها باید در نظر گرفته شود. استفاده از فناوری آزموده شده، سابقه و تجارب قبلی در زمینهٔ فعالیت مورد نظر، ساخت و بهره‌برداری موفقیت‌آمیز از تأسیسات مشابه، در دسترس بودن سازندگان و تولید کنندگان تجهیزات در آینده از جمله موارد قابل ذکر در به کمال رسیدن تأسیسات و فعالیت‌های هسته‌ای و پرتویی می‌باشند. همچنین، میزان پیچیدگی سیستم‌ها، تجهیزات و فعالیت‌هایی که در یک نیروگاه هسته‌ای قدرت وجود دارد، به مراتب بیشتر از یک راکتور تحقیقاتی با توان حرارتی چند مگاوات بوده و این موضوع در حجم کار ارزیابی ایمن یآنها تأثیر به سزایی دارد.

مدارکی که مشمول بررسی و ارزیابی ایمنی می‌شوند:

- گزارش‌های مقدماتی و نهایی تحلیل ایمنی (SAR)،
- گزارش‌های مقدماتی و نهایی ارزیابی اثرات محیطی (ER & EIA)،
- مدرک شرایط و محدوده‌های بهره‌برداری (OLC)،
- برنامه تضیمن کیفیت (QA) و دستورالعمل‌های ضمیمه آن،
- گزارش تحلیل ایمنی احتمالاتی (PSA)،
- گزارش‌های حوادث و رویدادهای مؤثر بر ایمنی تأسیسات،
- برنامه راه‌اندازی و ازکاراندازی،
- گزارش‌های دروه‌ای تحلیل ایمنی،
- برنامه‌های آمادگی و مقابله با شرایط اضطراری درون و بیرون سایت،
- گزارش‌های مانیتورینگ محیطی.

تأسیسات و فعالیت‌هایی که مشمول بررسی و ارزیابی ایمنی می‌شوند:

- نیروگاه‌های هسته‌ای،
- راکتورهای تحقیقاتی،

- تأسیسات چرخه سوخت هسته‌ای (معادن اورانیوم، کارخانه تغلیظ و فرآوری اورانیوم، کارخانه ساخت سوخت، تأسیسات غنی‌سازی اورانیوم)،
- تأسیسات پسمانداری مواد پرتوزا (آمایش، حمل و نقل، انبارکردن موقت و دائمی، دفن و دورریزی).

روند کلی بررسی و ارزیابی ایمنی مدارک در گروه ارزیابی ایمنی:

پس از ارجاع مدارک از مدیریت ایمنی هسته‌ای مرکز نظام ایمنی به گروه ارزیابی ایمنی، فعالیت‌های زیر صورت می‌گیرد:

- ✓ بررسی کلیات مدارک و کافی بودن مطالب ارائه شده و مطابقت شکلی آنها با الزاماتی که به نهادهای سازنده و بهره‌بردار معرفی شده است،
- ✓ بررسی و ارزیابی محتویات ارائه شده در خصوص برآورده شدن معیارها، الزامات و استانداردهای ایمنی،
- ✓ بررسی صلاحیت علمی و فنی کارکنان نهادهای سازنده و بهره‌بردار و مطابقت آموزش‌های ارائه شده به ایشان با مقررات و الزامات ایمنی هسته‌ای (بررسی گواهینامه‌ها)،
- ✓ برگزاری جلسات و انجام ممیزی برای رفع ابهام در مواردی که هنگام بررسی مدارک سیستم مدیریت کیفیت ضروری تشخیص داده شده است،
- ✓ تهیه گزارش ارزیابی ایمنی و ارسال نتایج و یافته‌های ارزیابی مدارک ایمنی به بخش صدور پروانه و مجوز از طریق مدیر کل ایمنی هسته‌ای،
- ✓ همکاری در تدوین شرایط اعتبار پروانه و مجوز.

برخی الزامات برای تهیه گزارش‌های تحلیل ایمنی، ارزیابی اثرات محیطی و برنامه اضطراری تأسیسات

۱. مدرک US RG 1.70 تحت عنوان:

Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)

به عنوان مرجع تهیه گزارش تحلیل ایمنی نیروگاه بوشهر،

۲. مدرک IAES Safety Standards No. SSG-20 تحت عنوان:

Safety Assessment for Research Reactors & Preparation of the Safety Analysis Report

به عنوان مرجع تهیه و بررسی گزارش تحلیل ایمنی راکتور تحقیقاتی تهران،

۳. مدرک US RG 3.39 تحت عنوان:

Standard Format and Content of License Applications for Plutonium Processing and Fuel Fabrication Plants

به عنوان مرجع تهیه و بررسی گزارش تحلیل ایمنی کارخانه ساخت سوخت (FMP)،

۴. مدرک US RG 3.25 تحت عنوان:

Standard Format and Content of Safety Analysis Reports for Uranium Enrichment Facilities

به عنوان مرجع تهیه و بررسی گزارش تحلیل ایمنی تأسیسات غنی‌سازی اورانیوم (FEP).

۵. مدرک DOE-5480.23 و NUREG 1520 تحت عنوان:

Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility

به عنوان مرجع تهیه و بررسی گزارش تحلیل ایمنی تأسیسات فرآوری اورانیوم (UCF)،

۶. مدارک IAEA EPR 2003 و US RG 3.67 تحت عنوان:

Methods for Developing Arrangements for Response to a Nuclear or Radiological Emergency,

Standard format and Content for Emergency Plans for Fuel Cycle and Materials Facilities

به عنوان مرجع تهیه و بررسی برنامه‌های اضطراری درون سایت و خارج از سایت نیروگاه‌های هسته‌ای و تأسیسات چرخه سوخت،

۷. مدرک US RG 4.9 تحت عنوان:

Preparation of Environmental Reports for Commercial Uranium Enrichment Facilities

به عنوان مرجع تهیه و بررسی گزارش محیطی تأسیسات چرخهٔ سوخت.

انواع و تقسیم‌بندی در ارزیابی ایمنی:

شاخه‌های فنی درگیر در ارزیابی:

- ✓ مخاطرات داخلی و خارجی،

- ✓ فیزیک هسته‌ای،
- ✓ یکپارچگی (سوخت، مدار اولیه، محفظهٔ ایمنی و سایر سازه‌های عمرانی، سایر اجزای مهم ایمنی)
- ✓ مهندسی مکانیک (دینامیک و ارتعاشات، پرتابه و ...)
- ✓ ترموهیدرولیک
- ✓ شیمی
- ✓ کنترل و ابزاردقیق
- ✓ توان الکتریکی
- ✓ حفاظت در برابر آتش
- ✓ حفاظت در برابر اشعه
- ✓ مهندسی فرایند
- ✓ مدیریت و عامل انسانی

کاربرد تحلیل ایمنی یقینی در مراحل طول عمر تأسیسات:

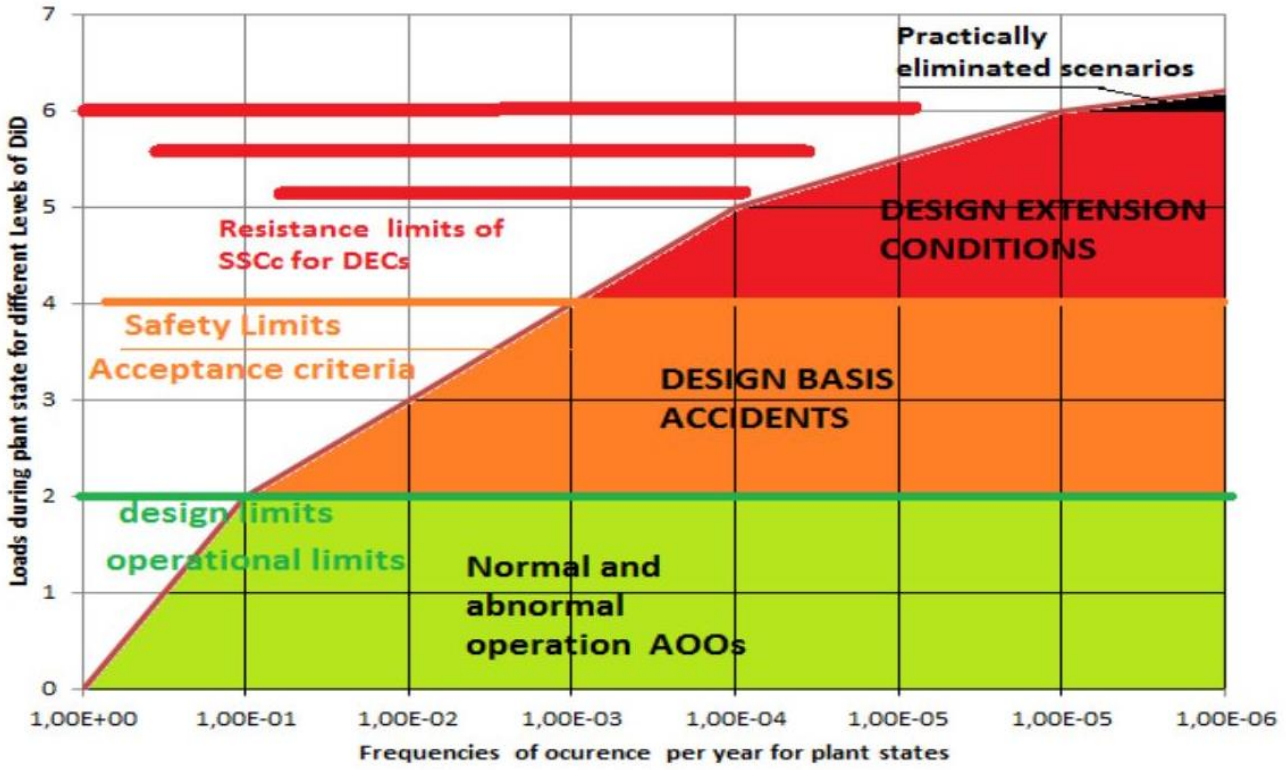
- ✓ طراحی
- ✓ نصب
- ✓ راه‌اندازی و خاموش سازی
- ✓ ارتقای طراحی یا عملکرد
- ✓ بازنگری دوره‌ای ایمنی،
- ✓ توسعهٔ عمر تأسیسات.

کاربرد تحلیل ایمنی یقینی برای همه حالت‌های تأسیسات:

- عملکرد عادی،
- عملکرد غیرعادی،
- حوادث مبنای طرح،
- شرایط توسعه طراحی بدون ذوب قلب،

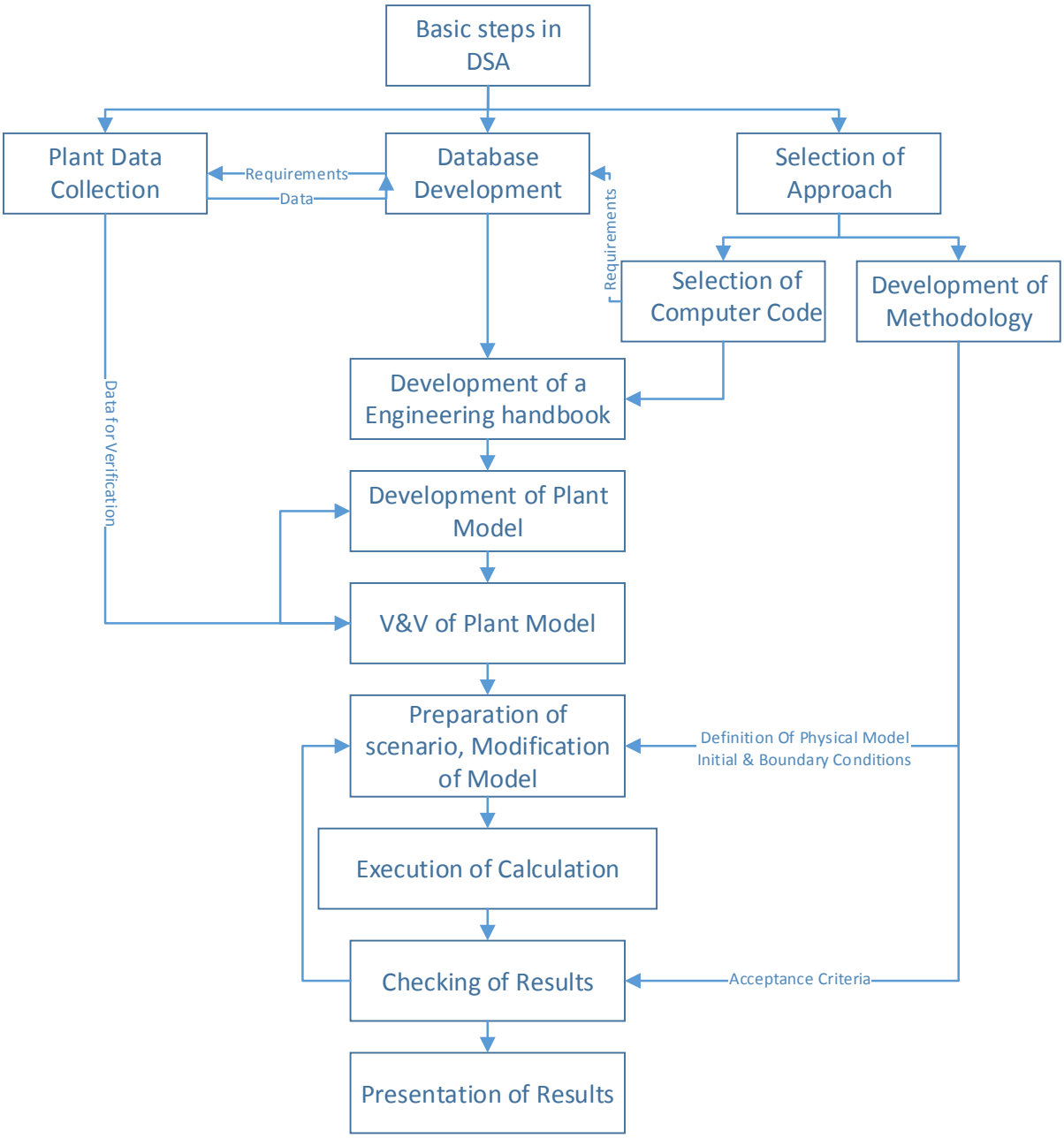
- شرایط توسعه طراحی با ذوب قلب.

دسته‌بندی شرایط گذره‌ها و حوادث بر اساس فرکانس وقوع آنها در شکل ۷۸ ارائه شده است.



شکل ۷۸: دسته‌بندی شرایط در ارزیابی ایمنی

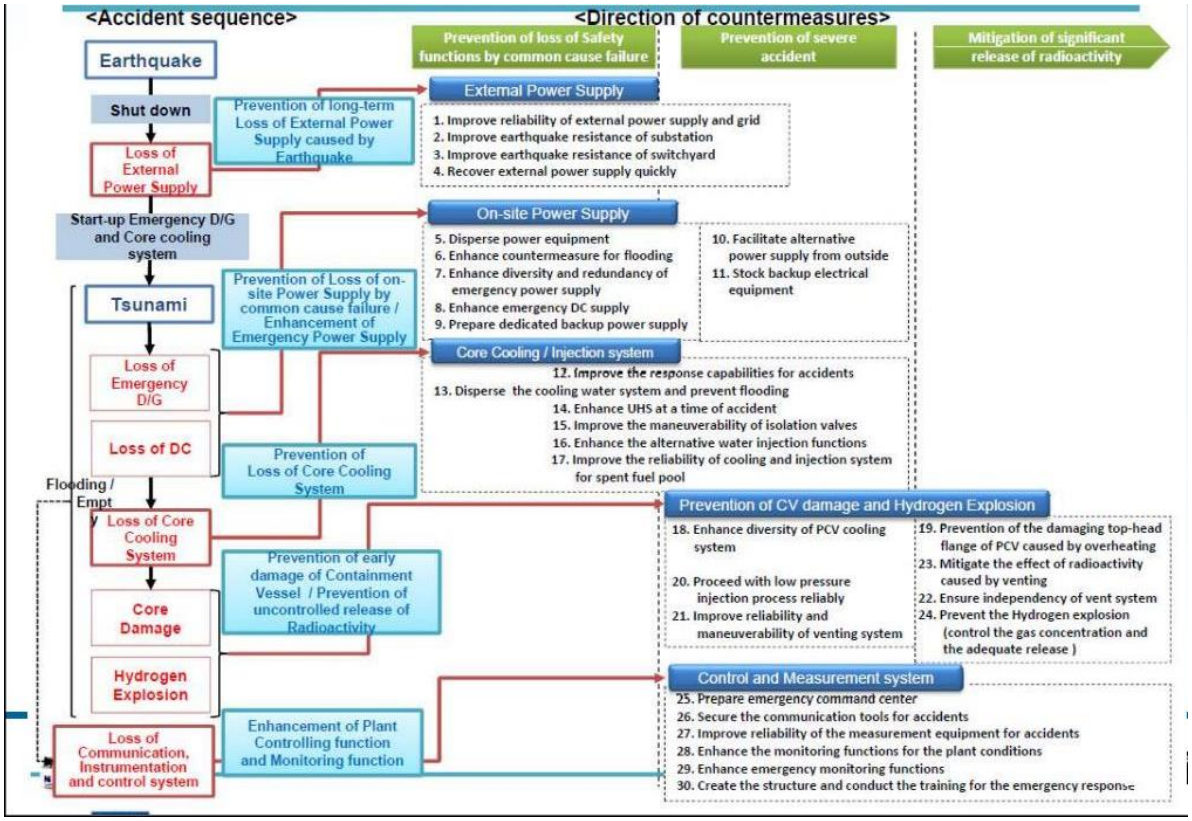
الگوریتم حاوی مراحل انجام تحلیل ایمنی یقینی در نیروگاه‌های هسته‌ای در شکل ۷۹ ارائه شده است.



شکل ۷۹: مراحل تحلیل ایمنی یقینی

درس‌آموخته‌های (تجارب حاصل از) حادثه فوکوشیما

حادثه فوکوشیما در اثر زلزله‌ای با قدرت ۸/۹ ریشتر در فاصلهٔ ۱۷۸ کیلومتری نیروگاه در ۱۱ مارس سال ۲۰۱۱ به وقوع پیوست. نیروگاه برای تحمل زلزله با قدرت ۸/۲ ریشتر طراحی شده بود. امواج سونامی با ارتفاع ۹ یا ۱۳ متر و شوک‌های پس از زلزله از عواملی هستند که پس از وقوع زلزله (حدود یک ساعت بعد) باعث تشدید وضعیت می‌شوند. این در حالی است که نیروگاه برای مقاومت در برابر امواج ۶/۵ متر طراحی شده بود.



شکل ۸۰: توالی رویدادها در حادثه فوکوشیما

فوکوشیما، رویداد بدون مشابه

مشخصات منحصر به فرد حادثه فوکوشیما شامل سه مورد زیر است:

- مرگ و میر هزاران نفر در اثر زلزله و سونامی،
- ویرانی صدها میلیاردی در زیرساخت‌ها و خواص،
- پیچیده شدن مشکلات با وقوع حوادث راکتور هسته‌ای.

این حادثه نشان داد که خرابی عامل مشترک قطع کامل برق ایجاد شده در اثر حوادث طبیعی بر ریسک تخمین زده شده توسط تحلیل ایمنی احتمالاتی نیروگاه‌های موجود غالب است.

پیامدهای حوادث

- در این حادثه مرگ و میر آنی ناشی از نیروگاه گزارش نشده است،
- اغلب هسته‌های پرتوزای منتشر شده از سوخت (ید و سزیم)، در داخل آب استخر فرونشانی ظاهر شد.
- برخی شرایط خارجی (در اثر جهت باد و باران محلی) بیش از مقدار میانگین شناسایی شد.
- اثرات نهان بلند مدت هنوز قابل دسترسی نمی‌باشند.

سوالات بسیاری باقی مانده است که سرانجام پاسخ داده خواهد شد. داده‌های قابل توجهی جمع آوری خواهد شد که می‌تواند به موارد زیر کمک کند:

- رفع آسیب‌پذیری نیروگاه‌های موجود،
- طراحی راکتورهای بهتر و ایمن‌تر.

ارزیابی بهتر شواهد تاریخی برای فرکانس‌ها و دامنه‌های پدیده‌های طبیعی لحاظ شده در مبنای طراحی و لحاظ پیامدهای بالای پدیده‌های طبیعی (زلزله‌ها، سیل‌ها، آتش‌سوزی‌ها و ...) با فرکانس پایین از جمله اموری است که در ادامه حیات نیروگاه‌های هسته‌ای باید لحاظ شوند. همچنین راکتورهای جدید باید به گونه‌ای طراحی شوند که از خرابی‌های با عامل مشترک طبیعی یا مخاطرات ناشی از انسان ممانعت کنند.

ارتقای تکنولوژی سطوح بالاتری از استاندارد فراهم می‌سازد. در این راستا اقدامات زیر قابل انجام است:

- طراحی‌های غیرفعال و ارتقایافته،
- تغییرات ممکن برای حذف آسیب‌پذیری نیروگاه‌های موجود پس از حوادث وخیم (منافذ فیلتری، منابع آب غیرفعال، سیستم‌های نگهداری آوار قلب، تجهیزات سیار و غیره)،
- ملاحظات مرتبط با قطع کامل توان و از دست رفتن چاه حرارتی برای مدت طولانی‌تر از مقدار معین فعلی (۲۴ تا ۷۲ ساعت)،

- فراهم کردن قابلیت‌های شبیه‌سازی با زمان واقعی و مرتبط با حوادث وخیم و شرایط اضطراری به عنوان کمک به آموزش بهتر،
- به کارگیری ابزارهای ارتقایافته و به اندازه کافی قابل اطمینان با کیفیت مناسب برای شرایط حادثه.

تحلیل ایمنی احتمالاتی و حادثهٔ فوکوشیما

ممکن است این سوال پیش آید که آیا روش تحلیل ایمنی احتمالاتی با حادثه فوکوشیما دچار تزلزل شده است؟ اگر تحلیل ایمنی احتمالاتی بسیار عالی است، چرا ریسک «قابل قبول» است، اما تاکنون ۵ حادثه ذوب قلب در کل جهان داشته‌ایم؟ برخی چیزها حس ایجاد نمی‌کند.

موضوع ایمنی احتمالاتی مبتنی بر این فرض است که هیچ سازه‌ای کاملاً ایمن نیست. هر سازه‌ای دارای یک احتمال خرابی است. در سال ۲۰۱۰ راکتورهای ژاپنی مستقر در ساحل اقیانوس آرام، حدود ۵۰۰ راکتورسال تجربه بهره‌برداری داشته‌اند. با فرض اینکه احتمال وقوع حادثه ورای طراحی سونامی ۱ بار در هر ۱۰۰ سال است، ۵ رویداد ویرانی قلب قابل پیش‌بینی است. با فرض اینکه احتمال وقوع حادثه ورای طراحی سونامی ۱ بار در هر ۱۰۰۰ سال است، ۰/۵ رویداد ویرانی قلب قابل پیش‌بینی است.

مدیریت حوادث

برنامه اضطراری برای خارج از نیروگاه یکی از مدارک ایمنی اخذ پروانه است. برنامه‌ریزی اضطراری خارج از نیروگاه بخشی از برنامه جامع مدیریت حوادث برای یک نیروگاه است. وقوع برخی سوانح هسته‌ای منجر به بازنگری در بسیاری از اصول و شیوه‌های برنامه‌ریزی اضطراری شد. تعهدات، مسئولیت‌ها و نیازهای اساسی در شرایط اضطراری در قالب سندی با عنوان استانداردهای بین‌المللی ایمنی برای محافظت از پرتوهای یون‌ساز و ایمنی در برابر منابع پرتوزا تدوین شده است. برنامه‌ریزی پاسخ اضطراری باید در دو سطح اصلی انجام شود:

- سطح اول مربوط به کاربر دارای مجوز بوده و با هدف کاهش عواقب احتمالی وقوع سانحه در چشمه و اعلام خطر به مسئولین بیرون سایت تهیه می‌شود.
- سطح دوم مربوط به مسئولین بیرون سایت بوده و به منظور کنترل و کاهش اثرات سانحه برای عموم مردم آماده می‌شوند.

اساس پاسخ به یک سانحه رادیولوژیک، مشابه هر سانحهٔ همراه با مواد زیان‌آور است. آنچه سوانح رادیولوژیک را از سایر سوانح متمایز می‌کند آن است که سایر سوانح را می‌توان با برخی از حواس خود نظیر بینایی، شنوایی و بویایی حس کرد، اما در سوانح رادیولوژیک چنین امکانی وجود ندارد. بنابراین لازم است شرایطی فراهم گردد تا خطرات رادیولوژیک احتمالی شناسایی شده و عموم مردم و کارکنان اضطراری از اقدامات لازم آگاه گردند. با این وجود، لازم است برنامه‌های رادیولوژیک در فهرست برنامه‌های مربوط به مواد زیان‌آور گنجانده شوند.

اهداف کلی برنامه‌ریزی اضطراری عبارتند از:

- الف) کاهش خطر سانحه یا تخفیف عواقب آن در چشمه منشأ آن،
- ب) جلوگیری از وقوع اثرات قطعی زیان‌آور بر سلامتی افراد (مانند مرگ)،
- ج) کاهش اثرات احتمالی زیان‌آور برای سلامتی افراد (مانند سرطان).

مسئولیت کاربر مواد پرتوزا، تلاش برای رسیدن به هدف اول می‌باشد. این مورد شامل جلوگیری یا کاهش نشت این مواد و ممانعت از قرارگرفتن کارکنان و عموم مردم در معرض این خطر است. دو هدف بعدی شامل مسئولیت مشترک کاربران و سازمان‌های بیرون سایت است که ملزم به اجرای اقدامات حفاظتی می‌باشند.

طبقه‌بندی عوامل و فعالیت‌های مورد نیاز در قالب پنج طبقه برنامه‌ریزی جهت پاسخ اضطراری است که هر یک با توجه به وسعت و مدت زمان وقوع، دارای فصول مشترکی هستند. این طبقه‌بندی تنها به عنوان شیوه‌ای مناسب در تهیه راهنمای برنامه‌ریزی استفاده شده و در حین وقوع سانحه نمی‌توان از آنها بهره گرفت. این پنج طبقه در جدول شماره ۴۵ ارائه شده‌اند.

جدول شماره ۴۵: طبقه‌بندی مناطق جامعه ذیل برنامهٔ پاسخ اضطراری هنگام حادثه

طبقه	شرح مناطق در هر طبقه
۱	مراکزی که احتمال نشت مقادیر زیادی مواد پرتوزا را دارند، به طوری که منجر به وقوع اثرات قطعی (زیان‌آور) بر سلامتی افراد در منطقه بیرون سایت می‌شود. همچنین، این طبقه، نواحی نزدیک به این منطقه که باید برای انجام اقدامات حفاظتی فوری آماده شوند را نیز در بر می‌گیرد.
۲	مراکزی که احتمال نشت مواد پرتوزا را دارند، (به طوری که پرتوگیری درمناطق بیرون‌سایت بالاتر از آستانه مداخله عمومی فوری شود)، در آن جا وجود دارد ولی هیچ‌گونه خطر کشنده‌ای نداشته و در مجموع خطر کمی پیش‌بینی می‌شود. همچنین مناطقی که باید برای انجام اقدام حفاظتی در پاسخ به سانحه آماده شوند نیز در این طبقه جای می‌گیرد.
۳	مراکزی که خطر قابل توجهی برای بیرون سایت ندارند ولی مستعد وقوع سوانحی هستند که اثرات قطعی (زیان‌آور) بر سلامتی افراد در درون سایت خواهند داشت. همچنین نواحی استحفاظی که برای انجام پشتیبانی‌های پزشکی، پلیس و آتش‌نشانی این مراکز مهیا می‌شوند را نیز در بر می‌گیرد.
۴	مناطقی که تهدید مشخصی نداشته و یا خطر کمی دارند. این سطح برنامه‌ریزی برای هر کشوری لازم است، زیرا احتمال وقوع سوانحی در حمل و نقل مواد پرتوزا و مفقود شدن یا سرقت چشمه پرتوزا در همه جا وجود دارد.
۵	مناطقی که به احتمال زیاد به هنگام وقوع سوانحی در خارج کشور نیاز به اجرای مداخله در امور تغذیه آن‌ها وجود خواهد داشت.