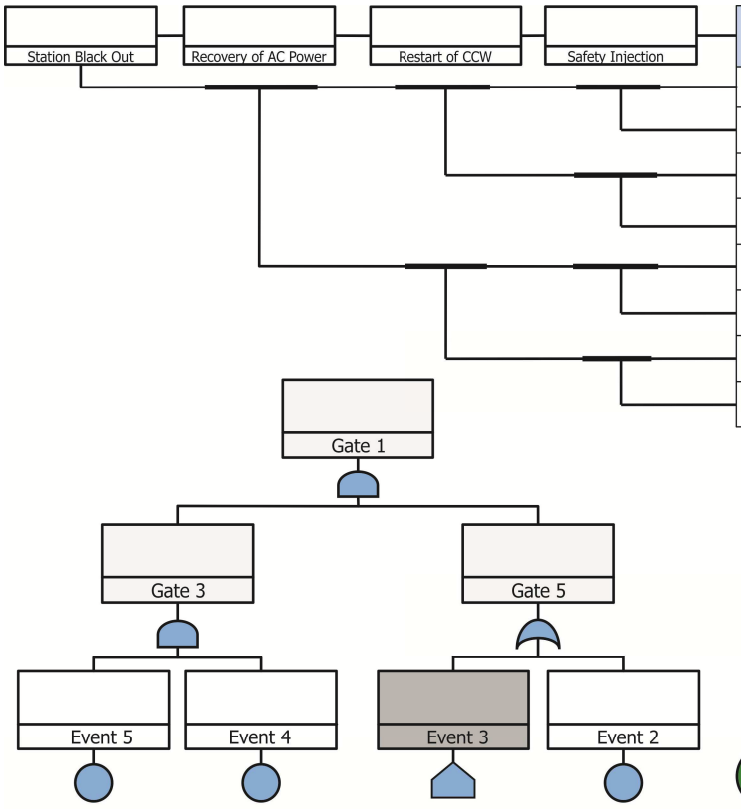
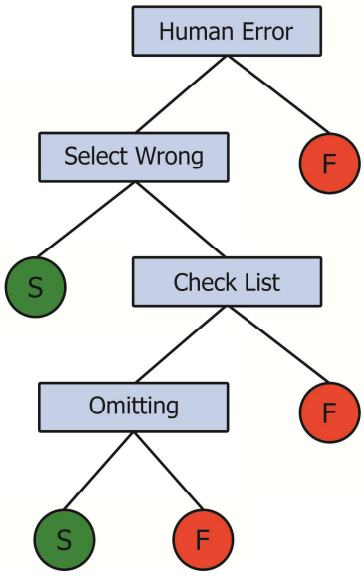
گزارش فنی کد محاسباتی تحلیل ایمنی احتمالاتی

PROBABILISTIC SAFETY ASSESSMENT
RELIABILITY LABORATORY TECHNICAL DOCUMENT
(RELAB 1.3)



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	



گزارش فنی کدRELAB 1.3

ویرایش ۰ – اسفند۱۳۹۶

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

۱- چکیده

کد (ReLab 1.0) نسخه یکپارچه و منسجم محاسبات ارزیابی احتمالاتی ایمنی[1] (PSA) است که مجهز به بخش‌های محاسباتی تحلیل درخت رویداد[2] (ETA)، تحلیل درخت خطا[3] (FTA)، دیاگرام تصمیم‌گیری دودویی[4] (BDD) و تحلیل خطای انسانی[5] (HRA) می‌باشد. گرچه تا حصول کد محاسباتی جامع تحلیل احتمالاتی ایمنی راه بسیار در پیش است، ولی در این نسخه سعی بر این شده تا با افزودن ماژول‌های BDD و HRA به ماژول‌های پیشین ETA و FTA، راه برای دستیابی به نسخه‌ای کامل‌تر هموار گردد. ماژول BDD تکنیکی برای دستیابی به مجموعه‌های برشی کمینه در مدت زمان کمتری نسبت به روش پیشین است؛ همچنین ماژول HRA جهت تحلیل و ارزیابی خطای انسانی در این نسخه تعبیه شده‌است. جزییات تمام بخش‌های کد و روش‌های محاسباتی آن در ادامه این گزارش به تفصیل بیان گردیده‌است.

۲- کلیدواژه

تحلیل درخت رویداد (ETA)، توالی رویداد، تحلیل درخت خطا (FTA)، مجموعه برشی کمینه، تحلیل میزان اهمیت، تحلیل خرابی‌های دارای علت مشترک، دیاگرام تصمیم‌گیری دودویی (BDD)، تحلیل خطای انسانی (HRA)، عوامل شکل‌دهنده عملکرد (PSF)، وابستگی.

1 Probabilistic Safety Assessment
2 Event Tree Analysis
3 Fault Tree Analysis
4 Binary Decision Diagram
5 Human Reliability Analysis

۳- اختصارات

عبارت	عبارت اختصاری	توضیح
Core Damage Frequency	CDF	فرکانس ذوب قلب راکتور
Failure Criteria	FC	معیار خرابی
Fault Tree Analysis	FTA	تحلیل درخت خطا
Event Tree Analysis	ETA	تحلیل درخت رویداد
Minimal Cut Set	MCS	مجموعه برشی کمینه
Rare Event Approximation	REA	تقریب رویداد نادر
Birnbaum Importance	BI	معیار اهمیت برنبام
Fussel-Vessly Importance	FV	معیار اهمیت فاسل-وسلی
Common Cause Failure	CCF	خرابی دارای علت مشترک
Min Cut Upper Bound	MCUB	باند بالای مجموعه برشی کمینه
Multiple Greek Letter	MGL	روش حروف چندگانه یونانی
Method for Obtaining Cut Sets	MOCUS	روش بدست آوردن مجموعه‌های برشی
Binary Decision Diagram	BDD	دیاگرام تصمیم‌گیری دودویی
Human Reliability Analysis	HRA	تحلیل قابلیت اعتماد انسانی
Complete Dependence	CD	وابستگی کامل
Error Factor	EF	عامل خطا
Human Error Probability	HEP	احتمال خطای انسانی
High Dependence	HD	وابستگی زیاد
Human Error Assessment and Reduction Technique	HEART	روش ارزیابی و کاهش احتمال خطا
Low Dependence	LD	وابستگی کم
Man-Machine Interface	MMI	رابط بین اپراتور و سیستم
Motor Operated Valve	MOV	روش شاخص احتمال موفقیت
Moderate Dependence	MD	وابستگی متوسط

عامل شکل‌دهنده عملکرد	PSF	Performance Shaping Factor
عملکرد مبتنی بر دستورات	RBA	Rule Based Action
عامل بازیابی	RF	Recovery Factor
روش استاندارد شده تحلیل قابلیت اعتماد انسانی در تحلیل ریسک	SPAR-H	Standardized Plant Analysis Risk Human Reliability Analysis
روش پیش‌بینی نرخ خطای انسانی	THERP	Technique for Human Error Rate Prediction
وابستگی صفر (عدم وابستگی کامل)	ZD	Zero Dependence
کد محاسباتی تحلیل احتمالاتی ایمنی	ReLab	Reliability Laboratory
ارزیابی احتمالاتی ایمنی	PSA	Probabilistic Safety Assessment

۴- مقدمه

تحلیل درخت رویداد و تحلیل درخت خطا دو ابزار اصلی در انجام PSA نیروگاه‌های هسته‌ای می‌باشد، که از تحلیل درخت رویداد به منظور مدلسازی روند پیشروی حوادث و از تحلیل درخت خطا برای مدلسازی خرابی سیستم‌ها و عملکردهای ایمنی استفاده می‌شود. با توجه به اینکه تحلیل درخت خطا یک روش قیاسی[1] است، برای مدلسازی خرابی سیستم‌ها مناسب می‌باشد، اما تحلیل درخت رویداد یک روش استنتاجی[2] بوده و در نتیجه برای تحلیل روند پیشروی حوادث مناسب می‌باشد [۱]. استفاده از ترکیب این دو روش در تحلیل PSA نیروگاه‌های هسته‌ای به این دلیل است که خواص و ویژگی‌های دو روش، آن‌ها را مکمل یکدیگر می‌سازد. ترکیب درخت خطا و درخت رویداد در تحلیل PSA، غالباً به یکی از دو روش لینک کردن درخت خطا[3] (FTL) یا لینک کردن درخت رویداد[4] (ETL) انجام می‌شود، که هرکدام از این دو روش دارای مزایا و محدودیت‌هایی می‌باشند. اغلب کدهای شناخته شده تحلیل PSA نیروگاه‌های هسته‌ای مانند SAPHIRE و Risk Spectrum، از روش اول و کدی مانند RISKMAN بر مبنای روش دوم توسعه داده شده‌اند. [۲]. نکته مهم در تحلیل این دو ماژول این است که کدهای تحلیل PSA، درخت‌های رویداد را نیز در نهایت تبدیل به درخت خطا نموده و محاسبات آن مشابه درخت خطا صورت می‌گیرد، بنابراین، تحلیل درخت خطا هسته اصلی یک کد PSA را تشکیل می‌دهد.

درخت خطا یکی از ابزارهای قدرتمند در مطالعات ایمنی می‌باشد به طوری که سنگ بنای مطالعات ایمنی به نحوی با آنالیز درخت خطا شروع می‌شود. ما از دو جهت مطالعات ایمنی را انجام می‌دهیم، یک آنالیز کیفی و دو آنالیز کمی، در اولی به دنبال علت و معلول‌ها هستیم و در دومی به دنبال احتمال وقوع رویدادها، تا بر پایه آن در مرحله ساخت، سیستمی کاملاً ایمن بسازیم و در مرحله راه‌اندازی و بهره‌برداری برای تمام رخدادهای نامطلوب چاره‌اندیشی کنیم و جلو وقوع آن‌ها را بگیریم. اما با پیچیده شدن و بزرگ شدن یک سیستم مانند یک نیروگاه هسته‌ای و بخش‌های مختلف آن زمان انجام محاسبات توسط درخت خطا به طور چشم‌گیری افزایش می‌یابد، اگرچه تمهیداتی برای این موضوع در نظر گرفته‌شده است اما باز هم مشکلات بر جای خود باقی می‌مانند. دیاگرام تصمیم‌گیری دوگانه به‌عنوان راه‌حلی مناسب برای این مشکلات معرفی‌شده‌اند. اولین نشانه‌های این مبحث در کارهای شانون[5] می‌باشد و نحوه نمایشی که وی برای توابع بولی ارائه داد. با تعریفی که وی از توابع بولی ارائه داد

---

1 deductive
2 inductive
3 Fault Tree Linking
4 Event Tree Linking
5 Claude Shannon

زمینه برای ورود درخت‌های تصمیم‌گیری به حوزه علوم مهندسی فراهم شد، به طوری که این مبحث به سرعت در علوم کامپیوتر و مدارهای مجتمع گسترش یافت و باعث افزایش سرعت و کارایی بسیاری در این حوزه‌ها شد. در مرجع شماره [۳] که در اوایل دهه ۹۰ میلادی معرفی شد یک روش مناسب برای تبدیل درخت خطا به درخت تصمیم‌گیری دوگانه و روشی برای آنالیز کمی و کیفی مطالعات ایمنی ارائه شد. بر پایه این مطالعه الگوریتم‌هایی برای تحلیل درخت خطا معرفی شد که با تبدیل آن به یک درخت تصمیم‌گیری کارایی این ابزار بیش از پیش مشخص شد. در پروژه پیش رو در چند بخش به معرفی این ابزار پرداخته شده‌است.

تحلیل قابلیت اعتماد انسانی یکی از مهم‌ترین بخش‌های هر تحلیل PSA در نیروگاه‌های هسته‌ای می‌باشد، زیرا خطای انسانی اثر قابل توجهی بر روی قابلیت اعتماد سیستم‌های ایمنی دارد. حوادث هسته‌ای مانند تری مایل آیلند[1] (TMI) و چرنوبیل و همچنین حوادث متعدد در سایر صنایع مانند حمل و نقل هوایی و کشتیرانی نشان می‌دهد چگونه خطای انسانی می‌تواند بر سیستم‌های ایمنی غلبه نموده و منجر به وقوع پیامدهای وخیم شود. حداقل ۷۰٪ از حوادث حمل و نقل هوایی و دریایی ناشی از عامل انسانی می‌باشد و ارقام مشابهی نیز در مورد صنایع فرآیندی وجود دارد. تحلیل ایمنی راکتورهای هسته‌ای تحت عنوان WASH-1400 که در سال ۱۹۷۵م. در آمریکا انجام شد، نشان داد که بیشتر از ۶۰٪ حوادث در صنایع هسته‌ای به نوعی با خطای اپراتور مرتبط هستند. به طور کلی نقش مستقیم عامل انسانی در پیشروی و پیامد حوادث حداقل به اندازه تجهیزات سخت‌افزاری اهمیت دارد [۴]. به دلیل اهمیت زیاد خطاهای انسانی در تحلیل PSA نیروگاه‌های هسته‌ای، در آخرین نسخه کدهای شناخته شده PSA مانند SAPHIRE و Risk Spectrum، قابلیت تحلیل خطای انسانی نیز به آنها افزوده شده است. ماژول تحلیل خطای انسانی در کد Risk Spectrum از روش‌های مختلفی مانند THERP، HEART و SPAR-H استفاده می‌کند. آخرین نسخه کد SAPHIRE نیز برای تحلیل خطای انسانی از روش SPAR-H استفاده می‌کند. در این پروژه به عنوان قدم اول در توسعه ماژول تحلیل خطای انسانی در کد ReLab، روش THERP به عنوان روش اصلی در نظر گرفته شده است. در مراحل بعد سایر روش‌های شناخته شده نیز به این ماژول افزوده خواهند شد.

1 Three Mile Island

۵- دامنه گزارش

در این گزارش به تشریح کلیه فرآیندهای محاسباتی ارزیابی احتمالاتی ایمنی به کار رفته در کد RELAB 1.0 می‌پردازیم. این فرآیندها شامل ماژول‌های محاسباتی تحلیل درخت رویداد، تحلیل درخت خطا، دیاگرام تصمیم‌گیری دوگانه و تحلیل خطای انسانی می‌باشد. هر ماژول در فصولی جداگانه در این گزارش بیان شده‌اند و در هر فصل به بررسی جزییات محاسباتی هر یک به تفصیل پرداخته شده‌است. فصل ۶ تحلیل درخت رویداد، فصل ۷ تحلیل درخت خطا، فصل ۸ کاربرد دیاگرام تصمیم‌گیری دودویی و در فصل ۹ تحلیل خطای انسانی ارائه گردیده‌است.

۶- تحلیل درخت رویداد

تحلیل درخت رویداد[1] (ETA) یکی از ابزارهای اصلی مورد استفاده در ارزیابی احتمالاتی ایمنی[2] (PSA) نیروگاه‌های هسته‌ای می‌باشد، و فرکانس ذوب قلب راکتور[3] با استفاده از ترکیب درخت رویداد و درخت خطا محاسبه می‌شود. در توسعه این ماژول، کد SAPHIRE به عنوان مرجع در نظر گرفته شده‌است، و در نهایت ماژول تحلیل ETA با قابلیت‌های مشابه این کد، به کد ReLab افزوده شده‌است. بدین منظور از دو روش Split Fraction و Delete Terms برای محاسبه فرکانس توالی‌های درخت رویداد استفاده شده‌است. این ماژول در کنار استفاده از روش‌های مذکور، از هسته[4] محاسباتی تحلیل مجموعه‌های برشی کمینه که در بخش تحلیل درخت خطا توضیح داده خواهد شد نیز بهره می‌برد. نتایج حاصل از کد ReLab به منظور اعتباربخشی با نتایج کد SAPHIRE مقایسه شده‌است، و این مقایسه حاکی از تطابق کامل در هر دو روش می‌باشد. تحلیل درخت رویداد یک روش استنتاجی در تحلیل حوادث می‌باشد، بدین معنی که این روش در زنجیره عِلّی[5] حادثه رو به جلو حرکت می‌کند. به بیان دیگر، در تحلیل درخت رویداد آنچه پس از وقوع یک رویداد نامطلوب به خصوص رخ می‌دهد مدنظر تحلیل‌گر می‌باشد، در حالی که در تحلیل درخت خطا هدف پیدا کردن عواملی است که منجر به یک رویداد نامطلوب می‌شود [۱]. مدلسازی ترتیب و توالی یک حادثه[6] در PSA نیروگاه‌های هسته‌ای مانند قطع تغذیه الکتریکی خارجی نیروگاه[7] (LOOP)، معمولاً با استفاده از تحلیل درخت رویداد انجام می‌شود. اما مدلسازی خرابی سیستم‌های ایمنی مانند دیزل ژنراتورهای اضطراری که برای مقابله با چنین حادثه‌ای در نظر گرفته شده، به وسیله درخت خطا صورت می‌گیرد. در نهایت ترکیب این دو روش مدل کامل PSA یک نیروگاه هسته‌ای را شکل می‌دهند.

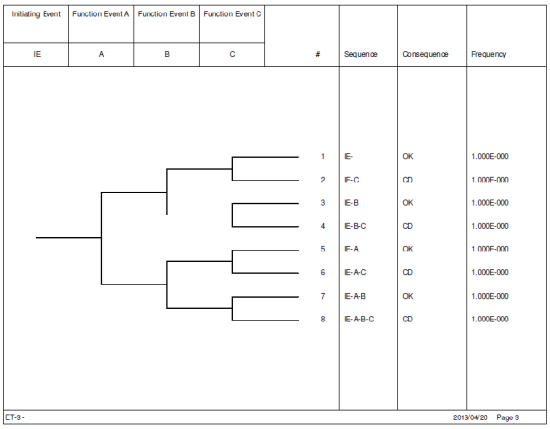
همانطور که در مقدمه گزارش نیز اشاره شده، ترکیب تحلیل درخت خطا و درخت رویداد در مدلسازی PSA نیروگاه‌های هسته‌ای به یکی از دو روش FTL یا ETL صورت می‌گیرد. در روش اول که در تحلیل PSA نیروگاه‌های هسته‌ای مرسوم‌تر می‌باشد، پیامد رویدادهای آغازگر به وسیله درخت رویداد مدل می‌شود و از درخت خطا نیز برای مدلسازی سیستم‌های ایمنی استفاده می‌شود. با توجه به اینکه در این روش کلیه اجزای

1 Event Tree Analysis
2 Probabilistic Safety Assessment
3 Core Damage Frequency
4 Kernel
5 Causal Chain
6 Accident Sequence
7 Loss Of Offsite Power

سیستم‌های ایمنی در درخت خطای آن در نظر گرفته می‌شود این روش نهایتاً منجر به تولید درخت‌های خطای بزرگی خواهد شد و از این رو به این راهبرد، روش درخت خطای بزرگ[1] نیز گفته می‌شود. اما در روش دوم بخش های مشترک در بین سیستم‌های ایمنی مختلف، به عنوان مثال سیستم‌های پشتیبان مانند تغذیه الکتریکی، خود در درخت‌های خطای جداگانه مدلسازی شده و درخت رویداد نیز بصورت مستقل وارد می‌شود. از آنجا که این روش در نهایت منجر به ایجاد درخت رویدادهای بزرگ خواهد شد به آن روش درخت رویداد بزرگ[2] نیز اطلاق می‌شود. پیش از ورود به مبانی ریاضی تحلیل درخت رویداد، تعدادی از مفاهیم پایه‌ای تحلیل درخت رویداد در بخش آتی شرح داده خواهند شد.

۶-۱ مفاهیم پایه‌ای تحلیل درخت رویداد

این بخش حاوی مروری کلی بر مفاهیم و تعاریف اصلی در تحلیل درخت رویداد می‌باشد، که در کد محاسباتی ReLab نیز از آن‌ها استفاده شده‌است. هر درخت رویداد دارای یک رویداد آغازگر[3] و تعدادی رویداد عملکرد[4] می‌باشد که رویداد آغازگر نشان‌دهنده دهنده وقوع یک رویداد نامطلوب و رویدادهای عملکرد نماینده سیستم یا عملکردهای ایمنی جهت جلوگیری از عواقب وخیم رویداد نامطلوب می‌باشند. وقوع یا عدم وقوع هر کدام از رویدادهای عملکرد نیز خرابی یا موفقیت آن عملکرد ایمنی را نشان می‌دهد.



شکل ۱: نمونه درخت رویداد رسم شده توسط کد SAPHIRE

1 Large Fault Tree
2 Large Event Tree
3 Initiating Event
4 Function Event

رسم یک درخت رویداد با تعیین رویداد آغازگر آن آغاز می‌شود، سپس در مرحله بعد عواملی که جهت جلوگیری از پیامدهای وخیم آن در نظر گرفته شده‌اند، تعیین می‌شود. این فرآیند تا زمانی ادامه می‌یابد که کلیه رویدادهای عملکرد تعیین شده 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 محاسبه احتمال وقوع توالی‌های مختلف در خت رویداد با توجه به رویدادهای عملکرد قابل انجام می‌باشد. شکل ۱ نمونه درخت رویداد رسم شده توسط کد SAPHIRE را نشان می‌دهد.

۶-۱-۱ رویداد آغازگر

در تحلیل درخت رویداد، به اولین متغیر ورودی درخت رویداد، رویداد آغازگر می‌گویند. رویداد آغازگر در درخت رویداد نشان‌دهنده وقوع یک رویداد نامطلوب می باشد که با ترکیب با خرابی تجهیزات، سیستم‌ها یا عملکردهای ایمنی منجر به یک پیامد نامطلوب شود. از آنجا که رویدادهای آغازگر نشان‌دهنده فرکانس وقوع یک رویداد می‌باشند، بنابراین برخلاف احتمال رویدادهای پایه، مقدار عددی آن محدودیتی ندارد و می‌تواند بزرگ‌تر از یک نیز باشد. رویداد آغازگر در شکل ۱، در قسمت بالا سمت چپ شکل با حروف اختصاری IE نشان داده شده‌است.

۶-۱-۲ رویداد عملکرد

رویداد عملکرد نشان‌دهنده تجهیزات، سیستم ها یا عملکردهای ایمنی می‌باشد که برای پیشگیری از وقوع پیامدهای نامطلوب یک رویداد آغازگر در نظر گرفته شده‌است. در رسم درخت رویداد معمولاً رویدادهای عملکرد را به ترتیب وارد عمل شدن آنها پس از وقوع رویداد آغازگر، وارد می‌کنند. در صورتی که وقوع یا عدم وقوع رویداد عملکرد تأثیر محسوسی در جلوگیری از پیامد نامطلوب رویداد آغازگر داشت ه 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 شکل ۱، در قسمت بالای شکل با حروف A، B و C نشان داده شده‌اند. ورودی یک رویداد عملکرد می‌تواند فقط یک رویداد پایه یا اینکه یک درخت خطا باشد.

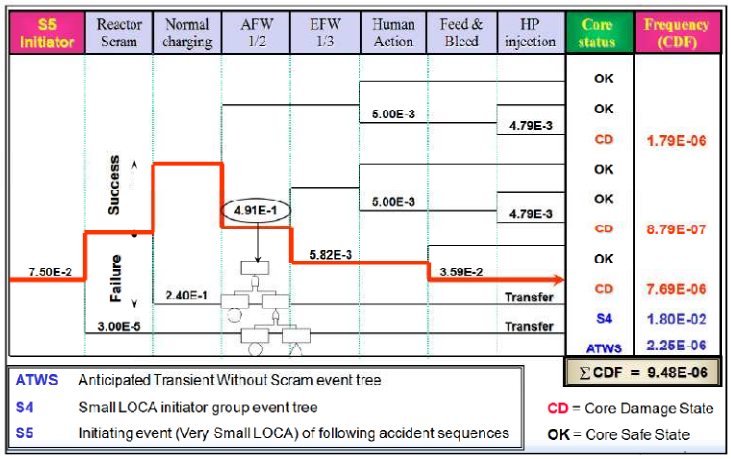
۶-۱-۳ توالی درخت رویداد

با توجه به آنچه در بخش پیش ذکر شد، هر کدام از مسیرهای درخت رویداد نشان‌دهنده عدم موفقیت تعدادی از سیستم‌ها یا عملکردهای ایمنی و موفقیت سایر سیستم ها پس از وقوع رویداد آغازگر می‌باشد. به هر کدام از این

مسیرهای درخت رویداد یک توالی حادثه[1] گفته می‌شود. توالی‌های مختلف درخت رویداد در شکل ۱، به ترتیب با اعداد ۱ تا ۸ مشخص شده‌اند. به عنوان مثال توالی شماره ۷ نشان دهنده خرابی سیستم‌های A و B و همچنین موفقیت سیستم C پس از وقوع رویداد آغازگر می‌باشد.

۶-۱-۴ پیامد درخت رویداد

هر کدام 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[2] می‌تواند یکی از دو حالت خاموشی راکتور یا ذوب قلب راکتور در نظر گرفته شود. به هر کدام از این وضعیت های نهایی یک پیامد درخت رویداد گفته می‌شود و در یک تحلیل PSA هدف اصلی پیدا کردن فرکانس یک پیامد خاص مانند ذوب قلب راکتور است که ممکن است از رویدادهای آغازگر مختلف ناشی شده باشد. این مسئله در شکل ۲ نشان داده شده‌است.



شکل ۲: درخت رویداد حادثه شکست بسیار کوچک مدار اول (Very Small LOCA)

همانطور که مشاهده می‌شود، رویداد آغازگر این درخت رویداد، شکست بسیار کوچک مدار اول راکتور[3] می‌باشد که با حروف اختصاری 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

---

1 Accident Sequence
2 End State
3 Very Small LOCA

نشان داده شده است که هدف پیدا کردن مجموع فرکانس ذوب قلب راکتور[1] است که با حروف اختصاری CD مشخص شده‌است. اما 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 رویداد دیگر مدلسازی شود. انتقال در درخت رویداد نیز مشابه انتقال در درخت خطا می‌باشد و برای هر کدام از توالی‌های انتقال یافته، یک درخت رویداد جداگانه رسم می‌شود.

۶-۲ روش‌های تحلیل درخت رویداد

همانگونه که پیشتر اشاره شد، هدف اصلی در تحلیل درخت رویداد، محاسبه فرکانس پیامد نامطلوب ناشی از یک‌رویداد آغازگر می‌باشد. از آنجا که در یک درخت رویداد توالی‌های متعددی ممکن است منجر به پیامد نامطلوب‌شوند، بایستی ابتدا فرکانس هر کدام از این توالی‌ها محاسبه شود. بنابراین محاسبات تحلیل درخت رویداد در نهایت به محاسبه فرکانس توالی‌های مختلف آن کاهش می‌یابد. احتمال وقوع هر کدام از توالی‌های درخت رویداد نیز، احتمال اشتراک رویداد آغازگر و رویدادهای عملکرد در آن توالی می‌باشد. برای محاسبه احتمال/ فرکانس هرکدام از توالی‌های درخت رویداد و یا پیامدهای آن روش‌های مختلفی وجود دارد که سه مورد از این روش ها در بخش های آتی شرح داده می‌شود.

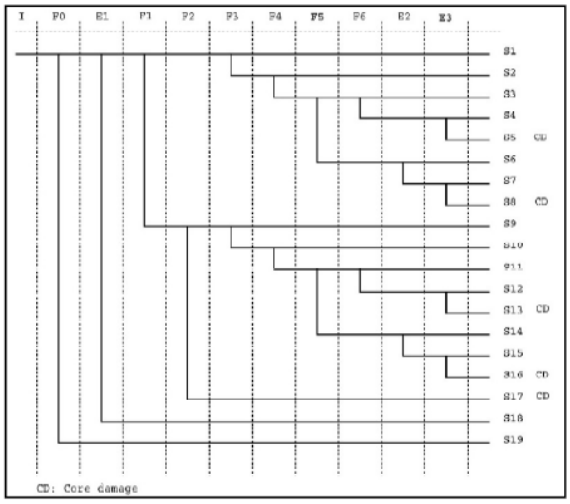
۶-۲-۱ روش Split Fraction

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، بنابر این 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 نظر گرفته می‌شود.

[1] Core Damage

۶-۲-۲ روش Delete Terms

همانطور که در بخش پیش ذکر شد، روش Split Fraction وابستگی بین رویدادهای عملکردی را در نظر نگرفته و فرض می‌کند که این این رویدادها از همدیگر مستقل می‌باشند. بنابراین نتایج حاصل از این روش تنها در صورتی معتبر است که رویدادهای عملکردی از همدیگر مستقل باشند. اما در تحلیل‌های مرسوم PSA معمولاً وابستگی‌های متعددی بین رویدادهای عملکردی 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 BWR [۱۲] در شکل ۳ داده شده‌است.



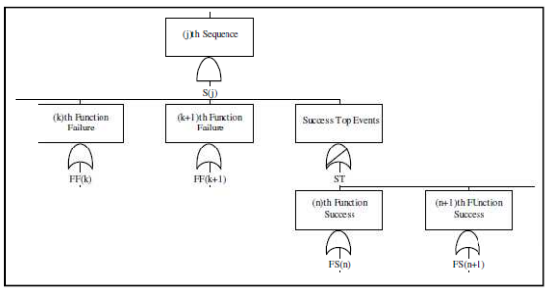
شکل ۳: درخت رویداد حادثه شکست بزرگ مدار اول یک راکتور BWR

ماتریس وابستگی‌های بین رویدادهای عملکردی این درخت رویداد نیز در جدل ۱ داده شده است، که اعداد درون جدول نشان دهنده تعداد رویدادهای پایه مشترک بین رویدادهای عملکردی می‌باشد.

جدول شماره ۱: 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 دقیق تر این مسئله، می توان هر کدام از توالی‌های یک درخت رویداد را مانند شکل ۴ به درخت خطای معادل آن تبدیل کرده، سپس با استفاده از مجموعه‌های برشی کمینه، فرکانس آن توالی را محاسبه نمود.



شکل ۴: درخت خطای معادل یک توالی درخت رویداد

همانگونه که در شکل ۴ مشاهده می‌شود، هر توالی به صورت یک گیت AND در نظر گرفته می‌شود که ورودی‌های آن وقوع یا عدم وقوع رویدادهای عملکردی می‌باشند. رویدادهای عملکرد ناموفق بطور مستقیم به گیت AND وارد می‌شوند، و رویدادهای عملکرد موفق به یک گیت NOR وارد می‌شوند، که خود به گیت AND اصلی وارد شده‌است.

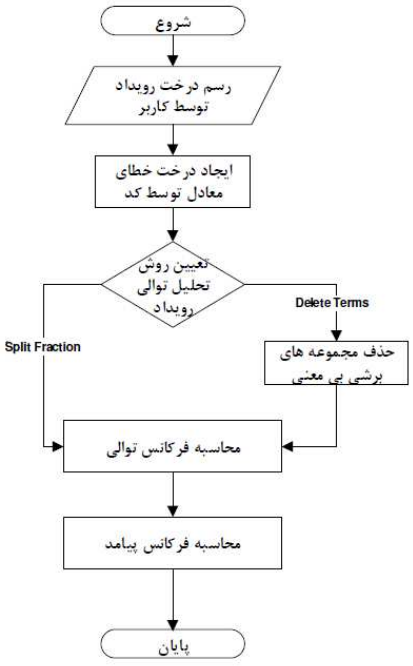
۶-۲-۳ روش دِمورگان

روش دقیق در نظر گرفتن شاخه‌های موفقیت درخت رویداد، استفاده از قوانین دمورگان می‌باشد. در این روش اثر گیت‌های متمم در یک توالی با استفاده از قوانین دمورگان در درخت خطای معادل آن اعمال می‌شود. قوانین دمورگان در تبدیل گیت‌های متمم شامل دو قانون زیر می‌شود:

$$\overline{(A+B)} = \overline{A}.\overline{B}\ or\ (A.NOR.B) = \overline{A}.AND.\overline{B} \qquad (۱-۶)$$

$$\overline{(A.B)} = \overline{A} + \overline{B}\ or\ (A.NAND.B) = \overline{A}.OR.\overline{B} \qquad (۲-۶)$$

بطور کلی در تبدیل دمورگان، گیت NAND و NOR به ترتیب به گیت OR و AND تبدیل شده و ورودی‌های آن‌ها نیز متمم می‌شوند. در صورتی که ورودی گیت متمم خود یک گیت باشد، نوع آن منفی شده و فرآیند تبدیل تا آخرین زیرشاخه‌های آن گیت ادامه پیدا می‌کند. با وجود اینکه روش دقیق مدلسازی شاخه‌های موفقیت درخت رویداد تبدیل دمورگان می‌باشد، به دلیل صرف زمان و حافظه زیاد کامپیوتر در تبدیل گیت‌های متمم، این کار در اکثر کدهای PSA انجام نمی‌شود. از آنجا که در کد SAPHIRE نیز که به عنوان مرجع در توسعه ReLab در نظر گرفته شده‌است از روش دمورگان استفاده نشده‌است. در شکل زیر فلوچارت تحلیل درخت رویداد کد ReLab آورده شده‌است.



شکل۵: فلوچارت تحلیل درخت رویداد در کد ReLab

۷- تحلیل درخت خطا

کد محاسباتی ReLab دارای قابلیت‌های تحلیل مجموعه‌های برشی کمینه، تحلیل خرابی‌های عامل مشترک و میزان اهمیت و حساسیت می‌باشد. این کد ابتدا با استفاده از مجموعه‌های برشی کمینه احتمال رویداد رأس درخت خطا را محاسبه می‌کند، سپس با استفاده از مجموعه‌های برشی کمینه بدست آمده و تغییر مقادیر پارامترها، تحلیل حساسیت و میزان اهمیت را انجام می‌دهد.

درخت خطا یک نمایش گرافیکی از یک عبارت بولی می‌باشد که با استفاده از قوانین جبر بولی قابل تبدیل و تغییر به فرم مجموعه‌های برشی کمینه می‌باشد. هدف از تحلیل مجموعه‌های برشی کمینه، بدست آوردن مجموعه‌های برشی درخت خطا و در نهایت محاسبه احتمال وقوع رویداد رأس[1] آن می‌باشد. در این فصل ابتدا عناصر اصلی تشکیل دهنده درخت خطا شامل رویدادهای پایه، گیت‌های منطقی و رویداد رأس، معرفی خواهند شد. سپس فرآیند تحلیل درخت خطا در کد محاسباتی ReLab، شامل بدست آوردن مجموعه‌های برشی کمینه و محاسبه احتمال وقوع رویداد رأس تشریح خواهد شد.

۷-۱ مفاهیم پایه‌ای تحلیل درخت خطا

این بخش حاوی مروری کلی بر مفاهیم و تعاریف اصلی در تحلیل درخت خطا می‌باشد، که در کد محاسباتی ReLab نیز از آنها استفاده شده است. هر درخت خطا دارای یک رویداد رأس و تعدادی رویداد پایه می‌باشد که ارتباط بین آنها توسط گیت‌های منطقی نمایش داده می‌شود. این ارتباط بیان کننده راه‌های مختلفی می‌باشد که وقوع رویدادهای پایه منجر به وقوع رویداد رأس درخت خطا خواهد شد. هر کدام از مفاهیم رویداد پایه، گیت منطقی و رویداد رأس در بخش‌های آتی شرح داده خواهند شد.

۷-۱-۱ رویدادهای پایه

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 در کد ReLab وجود دارد که عبارتند از : رویداد پایه، رویداد توسعه نیافته[2] و رویداد House.

---

1 Top Event
2 Undeveloped Event

۷-۱-۱-۱ رویداد پایه

این رویداد با یک علامت دایره نشان داده می‌شود، و در کد محاسباتی ReLab یک نام اختصاری[1] و یک عدد به آن اختصاص می‌یابد، که از کد اختصاری در انجام محاسبات استفاده می‌شود و عدد نیز احتمال وقوع آن می‌باشد.

۷-۱-۱-۲ رویداد توسعه نیافته

این رویداد که با علامت لوزی نشان داده می‌شود، براین شنان دادن شاخه‌هایی از درخت خطا که در مدل‌سازی بسط داده نشده‌اند به کار می‌رود. این رویداد نیز همانند رویداد قبلی می‌تواند یک کد اختصاری و یک احتمال وقوع به خود اختصاص دهد.

۷-۱-۱-۳ رویداد House

این رویداد 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 یک روی می‌دهد و Ignore (I) یعنی در تحلیل درخت خطا در نظر گرفته نشود.

۷-۱-۲ گیت‌های منطقی

روابط بین رویدادهای پایه و رویداد رأس درخت خطا، توسط گیت‌های منطقی ایجاد می‌شود. گیت‌ها 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.

۷-۱-۲-۱ 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.

۷-۱-۲-۲ 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.

[1] ID

۷-۱-۲-۳ 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.

۷-۱-۲-۴ گیت انتقال

این گیت که به صورت یک مثلث رو به بالا نشان داده می‌شود، نیاز به منطق خاصی برای وقوع خر وجی 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.

۷-۱-۲-۵ گیت NAND

این گیت از لحاظ منطقی متمم گیت AND می‌باشد و خروجی آن در صورتی روی می‌دهد که هرکدام از ورودی‌های گیت اتفاق نیفتند. این گیت را می‌تواند بایک گیت OR که تمام ورودی‌های آن منفی (متمم) شده‌اند مدل‌سازی کرد.

۷-۱-۲-۶ گیت NOR

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

۷-۱-۳ رویداد رأس

رویداد رأس در یک درخت خطا، اولین گیت آن درخت یا به عبارت دیگر گیتی است که ورودی هیچ گیت دیگری نیست. این رویداد نشان دهنده خرابی یک سیستم یا وقوع یک رویداد نامطلوب است که هدف از رسم درخت خطا، مدل‌سازی و محاسبه 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. این روند ادامه پیدا

می‌کند و در قدم بعدی بایستی منجر به رویدادهای مرحله قبل که رویدادهای میانی[1] نیز نامیده می‌شوند، تعیین گردد، تا زمانی که دیگر شاخه‌های درخت خطا قابل توسعه نباشند و بتوان به هر کدام از عوامل یک احتمال وقوع نسبت داد.

۷-۲ تحلیل مجموعه برشی کمینه

مجوعه برشی به ترکیبی از رویدادهای پایه در یک درخت خطا اطلاق می‌شود که وقوع همزمان آنها 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 مجموعه اصلی را باید حذف کرد و زیرمجموعه آن را باید در نظر گرفت. به این مجموعه‌های برشی که هیچکدام از آنها زیرمجموعه دیگری نیست، مجموعه برشی کمینه می‌گویند.

۷-۲-۱ بازآرایی درخت خطا

قبل از شروع تحلیل درخت خطا در کد محاسباتی ReLab، ابتدا یک سری اعمال بازآرایی بر روی درخت خطا صورت می‌گیرد تا آن را به شکلی درآورد که محاسبات آن ساده‌تر شود. این مراحل شامل پیدا کردن لوپ منطقی، تبدیل گیت‌های ترکیبی (N/M) و متمم (NAND و NOR)، تحلیل رویدادهای House و ادغام گیت‌های مشابه متوالی می‌باشد. در زمینه بازآرایی درخت خطا محدودیت خاصی وجود ندارد و می‌توان قبل از انجام محاسبات درخت خطا به هر تعداد ممکن از متدهای بازآرایی استفاده و ساختار درخت خطا را تا حد امکان ساده‌تر کرد.

۷-۲-۱-۱ 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 گیت‌اهی 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 در بخش‌های آتی می‌آید.

- گیت‌های ترکیبی

[1] Intermediate Event

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 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 M از رابطه (۷-۱) بدست می‌آید.

$$\binom{m}{n} = \frac{m!}{n!(m-n)!} \qquad (۷-۱)$$

به عنوان مثال یک گیت 2/3 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

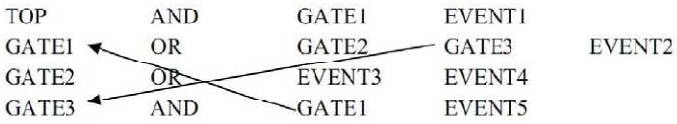
GATE 1-3 AND INPUT 2 INPUT 3

- گیت‌های متمم

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 [۴]. برای این کار گیت NAND به OR و گیت NOR به AND تبدیل شده و ورودی‌های آن نیز همگی منفی (متمم) می‌شوند.

۷-۲-۱-۲ خطای لوپ منطقی

خطای لوپ منطقی در درخت خطا در صورتی رودی می‌دهد که یک گیت به صورت مستقیم یا غیرمستقیم دوباره به خودش رجوع داده شود. کد ReLab در صورت وجود چنین مواردی در درخت خطا آن را پیدا کرده و با یک پیغام مسیر لوپ را نیز نشان می‌دهد. نمونه‌ای از خطای منطقی را در شکل ۶ مشاهده می‌کنید.



شکل ۶: لوپ منطقی در درخت خطا

۷-۲-۱-۳ ادغام گیت‌های مشابه متوالی

یکی دیگر از مراحل بازآرایی که طی آن می‌توان درخت خطار را ساده‌تر نمود، ادغام گیت‌های مشابه متوالی است. در صورتی که 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.

۷-۲-۲ بدست آوردن مجموعه‌های برشی کمینه

همانطور که در مقدمه اشاره شد، برای محاسبه احتمال وقوع رویداد رأس درخت خطا، ابتدا باید ساختار آن را به یک فرمت منطقی معادل تبدیل نمود که بتوان با استفاده از آن، تحلیل کمی درخت خطا را انجام داد. این فرمت معادل که برای کمی‌سازی درخت خطا به کار می‌رود مجموعه برشی کمینه[1] (MCS) نامیده می‌شود. یک مجموعه برشی ترکیبی از رویداد پایه است که وقوع همزمان آنها منجر به وقوع رویداد رأس درخت خطا می‌شود. مجموعه برشی کمینه، کوچک‌ترین ترکیب ممکن از رویدادهای پایه است که منجر به روی دادن رویداد رأس خواهد شد. بدین معنی که با حذف هر کدام از رویدادهای پایه از یک مجموعه برشی کمینه، مجموعه مورد نظر دیگر مجموعه برشی نخواهد بود و منجر به وقوع رویداد رأس نمی‌شود [۱۳]. مجموعه MCSها نشان دهنده تمامی حالات ممکن برای وقوع رویداد رأس ناشی از رویدادهای پایه می‌باشد.

علاوه بر محاسبه احتمال وقوع رویداد رأس، مقدار قابل توجهر از اطلاعات را تنها از ساختار MCSها می‌توان کسب کرد. به عنوان نمونه یک MCS که تنها دارای یک رویداد پایه باشد که منجر به روی دادن رویداد رأس می‌شود، نشان دهنده یکی از ضعف‌های طراحی سیستم می‌باشد. این گونه ضعف‌ها در ساختار سیستم‌ها معمولاً با استفاده از بالا بردن درجه افزونگی[2] یا تجهیزات با قابلیت اعتماد بالاتر قابل رفع شدن است. به عنوان یک نمونه

[1] Minimal Cut Set
[2] Redundancy

دیگر، یک MCS که در آن چند رویداد پایه مشابه وجود دارد نشان دهنده استعداد سیستم برای وقوع خرابی دارای علت مشترک[1] (CCF) می‌باشد [۴].

۷-۲-۲-۱ الگوریتم MOCUS

روش‌های مختلفی برای بدست آوردن مجموعه‌های برشی یک درخت خطا وجود دارند که هر کدام دارای مزایا و معایب خاص خود می‌باشند. در کد محاسباتی ReLab از الگوریتم MOCUS برای یافتن مجموعه‌های برشی استفاده شده است [۴]. این الگوریتم یکی از شناخته شده‌ترین روش‌ها در پیدا کردن مجموعه‌های برشی یک درخت خطا می‌باشد و بیشترین استفاده را در کدهای محاسباتی تحلیل درخت خطا داشته است. الگوریتم MOCUS با شروع از رویداد رأس در صورت برخورد به گیت AND ورودی‌های آن رادر ستون‌های جداگانه نوشته و برای هر کدام از ورودی‌های گیت OR یک سطر جدید ایجاد می‌کند.

۷-۲-۲-۲ حذف مجموعه‌های برشی غیرکمینه

پس از بدست آوردن مجموعه‌های برشی درخت خطا با استفاده از الگوریتم MOCUS، لازم است مجموعه‌های برشی تکراری و غیرکمینه حذف شوند. این کار با انجام مقایه دو به دو بین مجموعه‌های برشی و استفاده از قوانین خودتوانی[2] و جذب[3] در جبر بولی قابل انجام است. این دو قانون جبر بولی به ترتیب در روابط (۷-۲) و (۷-۳) نمایش داده شده‌اند.

$$A + A = A \qquad (۷-۲)$$

$$A + AB = A \qquad (۷-۳)$$

۷-۲-۳ محاسبه 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 مجموعه برشی کمینه مطابق رابطه (۷-۴) از حاصلضرب احتمال وقوع رویدادهای پایه عضو مجموعه برشی کمینه بدست می‌آید.

$$P(C_i) = \prod_{j=1}^{n} P_j \qquad (۷-۴)$$

---

1 Common Cause Failure
2 Idempotence
3 Absorption

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[1] (REA) و باند بالای مجموعه برشی کمینه[2] (MCUB) محاسبه کرد. مقدار تقریبی احتمال رویداد رأس درخت خطا با استفاده از تقریب REA مطابق رابطه (۵) محاسبه می‌شود. با توجه به رابطه (۷-۵) مشاهده می‌شود که فرض اصلی در این روش صرف‌نظر کردن از اشتراک بین مجموعه‌های برشی کمینه می‌باشد. این فرض در سیستم‌های قابل اعتماد[3] که احتمال مجموعه‌های برشی کمینه در آنها بسیار کوچک می‌باشد، فرض معقولی است.

$$T = \sum_{i=1}^{m} C_i \qquad (۷-۵)$$

تقریب MCUB که از بسط کامل سیلوستر- پوانکاره[4] استفاده می‌کند، منجر به نتایج دقیق‌تری برای احتمال رویداد رأس خواهد شد. نحوه محاسبه احتمال رویداد رأس درخت خطا با استفاده از تقریب MCUB در رابطه (۶) نمایش داده شده است.

$$T = \sum_{i=1}^{m} C_i - \sum_{i<j}^{m} C_i C_j + \cdots + (-1)^m C_1 C_2 \dots C_m \qquad (۷-۶)$$

این رابطه را می‌توان به شکل ساده‌تری نیز نوشت:

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

علی‌رغم اینکه در روش MCUB اشتراک بین مجموعه‌های برشی کمینه در نظر گرفته می‌شود، احتمال رویداد رأس در این روش نیز دقیق نیست. این روش تنها در حالتی منجر به مقدار دقیق احتمال رویداد رأس خواهد شد ک تمامی مجموعه‌های برشی کمینه درخت خطا از همدیگر مستقل باشند.

1 Rare Event Approximation
2 Min Cut Upper Bound
3 Reliable System
4 Sylvester-Poincare

۸- تحلیل دیاگرام تصمیم‌گیری دودویی (BDD)

۸-۱- جبر بولی

برای وارد شدن به مبحث دیاگرام تصمیم‌گیری دودویی یا دوگانه (BDD) نیاز به آشنایی با مباحث جبر بولی داریم، لذا در این بخش به معرفی اجمالی مفاهیم مورد نیاز برای درک بهتر موضوعات ارائه شده در این گزارش پرداخته می‌شود. در جبر بولی برخلاف جبر مقدماتی که متغیرها از نوع عدد می‌باشند، متغیرها از نوع صحیح و غلط هستند که مقادیر صفر یا یک به ترتیب برای مقادیر غلط و صحیح استفاده می‌شوند. درک این مطلب ساده اساس مبحث تصمیم‌گیری‌های دوگانه است، زیرا همیشه در مواجه با رویدادهایی که در دیاگرام‌های دوگانه با آن‌ها سروکار داریم دو حالت بیشتر نداریم، یا رویداد رخ می‌دهد یا اتفاق نمی‌افتد یعنی یک حالت صفر و یک داریم. عملگرهای اصلی در منطق بولی عبارت‌اند از: ۱- عطف منطقی[1] که نشانگر اشتراک دو رویداد است و تنها زمانی متغیر صحیح را اختیار می‌کند که هر دو رویداد اتفاق افتاده باشند،۲- فصل منطقی[2] یا همان اجتماع دو رویداد که تنها زمانی مقدار غلط را می‌گیرد که هر دو رویداد باهم اتفاق نیفتند، ۳- نقیض[3] که حالت یک رویداد را برعکس می‌کند یعنی برای مثال اگر تأثیر رخداد یک رویداد مورد بررسی باشد این عملگر تأثیر رخ ندادن رویداد را بازمی‌گرداند. برای نشان دادن یک فرمول جبری دو روش جمع حاصل‌ضرب‌ها و یا ضرب حاصل جمع‌ها به کار می‌رود، BDD درواقع نمایشی گرافیکی از یک فرمول جبری می‌باشد. در قسمت‌های بعد چگونگی نمایش عملگرهای منطقی و فرمول‌های جبری را توسط BDD خواهیم دید. ایده اولیه دیاگرام‌های تصمیم‌گیری به تجزیه شانون باز می‌گردد. فرض کنیم $X = \{x_1, x_2, \dots x_n\}$ مجموعه‌ای از n متغیر بولی باشد، یک انتصاب X تصویری از آن به مجموعه $\{0,1\}$ است. حال اگر تابع بولی مثل F که بر روی این مجموعه تعریف شده و x نیز عضوی از آن باشد، آنگاه بر طبق تجزیه شانون یک شکل نمایش F به‌صورت زیر خواهد بود:

$$F = \left(x \wedge F_{\{x=1\}}\right) \vee \left(\overline{x} \wedge F_{\{x=0\}}\right) \qquad (۱-۸)$$

نمایش فوق را به‌عنوان کلید مبحث دیاگرام‌های تصمیم‌گیری دوگانه در نظر می‌گیریم و در ادامه به معرفی آن می‌پردازیم.

---

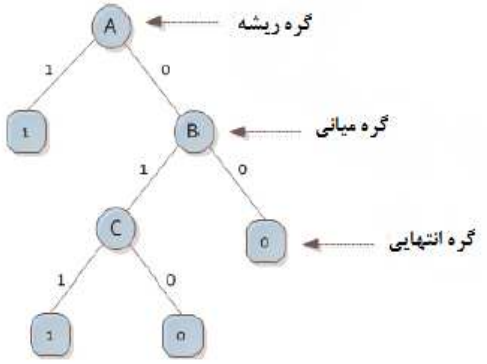
1 Conjuction
2 Disjunction
3 Negation

۸-۲- مباحث مقدماتی BDD

درخت خطا رایج‌ترین روش برای بررسی ایمنی سیستم‌های صنعتی می‌باشد که دو هدف اصلی معمولاً در این مطالعات موردتوجه است، ۱- مطالعات کیفی، ۲- مطالعات کمی. در مطالعات کیفی هدف مشخص شدن راه‌هایی است که منجر به بروز رخدادی می‌شوند، برای مثال در مطالعات ایمنی نیروگاه ما به دنبال عواملی هستیم که باعث بروز حادثه ذوب قلب می‌شوند به این عوامل اصطلاحاً کمینه‌های برشی[1]گوییم. برای این منظور ابتدا تمامی عواملی که در رویداد رأس موثرند را پیدا می کنیم و سپس درخت خطا را تشکیل می دهیم و از رویدادهای پایه شروع به تحلیل می‌کنیم تا روابط بولی بین رویدادهای پایه بر اساس گیت های منطقی درخت خطا مشخص شود تا درنهایت تابع منطقی رویداد رأس به دست آید که در این مرحله باید این رابطه را به صورت جمع حاصل‌ضرب‌های متغیرها تبدیل کرد تا مجموعه‌های برشی رویداد رأس به دست آید، اما برای به دست آوردن کمینه‌های برشی باید الگوریتم‌های کاهش و به دست آوردن کمینه‌ها را بر روی جمع حاصل ضرب‌ها اعمال کنیم که چنانچه سیستم بزرگ باشد بسیار زمان‌بر است. در مطالعات کمی هدف به دست آوردن احتمال اتفاق افتادن یک رویداد است، برای مثال ما به دنبال به دست آوردن احتمال ذوب شدن قلب در مطالعات ایمنی هستیم. استفاده از درخت خطا در این بخش نیز در صورت بزرگ بودن سیستم بسیار زمان‌بر است، اگرچه در این بخش با قرار دادن یک حد مشخص برای احتمال رویدادهایی که در بروز رویداد مدنظر مؤثرند، فقط احتمال‌هایی را در نظر می‌گیریم که ازاین حد بزرگ‌تر باشند و بدین ترتیب بخشی از محاسبات را کاهش داده تا از زمان انجام محاسبات کاسته شود، اما با این روش احتمال دقیق رخ دادن رویداد مدنظر دیگر به دست نمی‌آید لذا با تمام مزیت‌هایی که درخت خطا دارد نیاز به روشی مؤثرتر برای انجام مطالعات است. دیاگرام‌های تصمیم‌گیری دوگانه (BDD) بدون اینکه ماهیت مسئله را عوض کنند به‌صورت مؤثرتری اهداف ما را در مطالعات ایمنی برآورده می‌کنند و زمان انجام محاسبات را کاهش می‌دهند. BDD دو خاصیت مهم دارد: ۱- گراف‌هایی فشرده هستند که این خاصیت از تقسیم شدن گراف به زیر گراف‌های معادل به دست می‌آید ۲- در این روش هر عملیات یک بار انجام و ذخیره می‌شود و در نتیجه اجرای هر عمل فقط یک بار صورت می‌گیرد و لذا در زمان انجام محاسبات بسیار صرفه‌جویی می‌شود. دو شکل نمایش برای BDD را سعی می‌کنیم همزمان توضیح دهیم. ابتدا نمایش گرافیکی درخت تصمیم‌گیری و سپس نمایش رسمی آن، که در این پروژه الگوریتم‌های معرفی شده به نمایش رسمی آن مربوط می‌شود. درخت‌های تصمیم‌گیری گراف‌هایی مستقیم و بدون حلقه‌اند[2]و دارای سه نوع گره هستند. ۱- گره ریشه که دارای

[1] Minimal Cutset
[2] directed acyclic graph

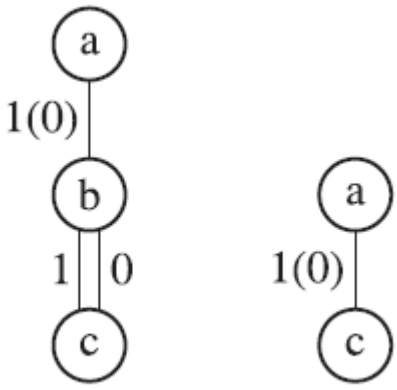
دوشاخه (فرزند) صفر و یک است و دارای والد نیست. ۲- گره‌های میانی که دارای دوشاخه (فرزند) صفر و یک هستند و هر گره میانی دارای یک والد است. ۳- گره‌های انتهایی که تنها یک والد دارند. با این تقسیم‌بندی مشخص است که سرچشمه یک درخت تصمیم‌گیری گره ریشه منحصر به فرد است که خود دارای دو فرزند است که می‌توانند گره میانی یا انتهایی باشند. شکل زیر نمایانگر این مفاهیم است.



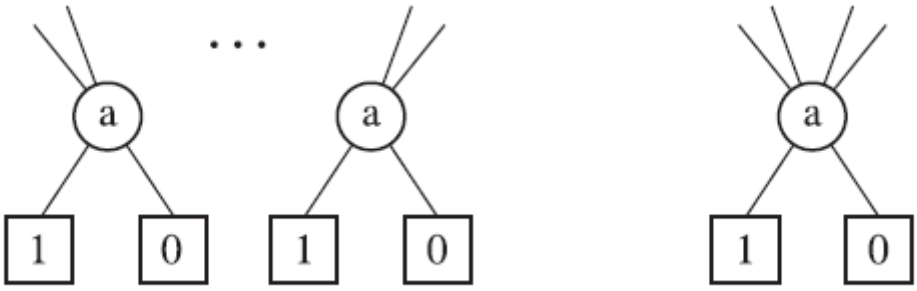
شکل ۷: دیاگرام تصمیم‌گیری دودویی

با توجه به شکل، هر گره دارای یک متغیر است که نام آن درون رأس نوشته می‌شود و فرزندان صفر و یک هر گره با شاخه متناظر صفر یا یک نمایش داده می‌شوند. در درخت‌های خطا هر رویداد پایه متناظر با یک گره ریشه یا گره میانی است و دو حالت رخ دادن یا ندادن هر رویداد پایه با شاخه یک یا صفر نمایش داده می‌شود و ارتباط بین متغیرها با توجه به گیت‌های منطقی درخت خطا تعیین می‌شود. البته BDD که برای آنالیز درخت‌های خطا مورد استفاده قرار می‌گیرد دارای متغیرهایی با رتبه یا ترتیب[1] ثابت هستند و تا جایی که امکان داشته باشد درخت تصمیم‌گیری ساده شده می‌شود که اصطلاحاً به چنین درخت‌های تصمیم‌گیری، درخت تصمیم‌گیری کاهش‌یافته با رتبه ثابت[2] گوییم. همان‌طور که گفته شد درخت‌های تصمیم‌گیری فشرده هستند این کار با حذف رئوسی که مناسب نیستند انجام می‌شود. این رئوس در دو حالت حذف می‌شوند: ۱- اگر هر دو فرزند یک رأس به یک یا دو رأس کاملاً مشابه ختم شوند. ۲- زمانی که رأس مشابه رأس دیگر داشته باشیم. این دو مطلب در شکل زیر مشخص‌شده‌اند.

1 order
2 Reduced Ordered Binary Decision Diagram



شکل ۸: حذف گره در حالت اول



شکل ۹: حذف گره در حالت دوم

حال که مختصر با این نحوه نمایش آشنا شدیم به نمایش رسمی دیاگرام تصمیم‌گیری دوگانه می‌پردازیم، اساس BDD از ساختار «If Then Else» که در ادامه ما آن را به‌اختصار ITE می‌نامیم تشکیل‌شده است، همان‌طور که پیش‌تر ذکر شد نکته جذاب در مورد BDD این است که ساختار ITE از فرمول شانون مشتق شده است. درنتیجه اگر $f(x)$ یک تابع بولی برای رویداد رأس یک درخت خطا باشد بر اساس فرمول شانون می‌توانیم بنویسیم:

$f(x) = X_1.f_1 + \overline{X_1}.f_2$ ، ساختار ITE مطابق با این فرمول $ITE(X_1, f_1, f_2)$ خواهد شد، معنای این جمله این است که اگر رویداد X_1 رخ دهد آنگاه f_1 برقرار است و در غیر این صورت f_2 برقرار خواهد بود، برای هر رویداد در درخت خطا می‌توان چنین ساختاری را نسبت دهیم. لذا قدم اول برای یک BDD این است که از درخت خطا شروع و آن را تبدیل به درخت تصمیم‌گیری کنیم. البته اندازه این درخت حاصل بسته به ترتیبی که برای متغیرها انتخاب می‌کنیم تغییر خواهد کرد و مسلماً هر چه این درخت کوچک باشد زمان انجام محاسبات و حافظه اشغال شده کمتر می‌شود. برای انتخاب ترتیب مناسب باید تمام رویدادهای پایه رده[1] مناسب را اختیار کنند، اما انتخاب هر چه باشد نتایج به دست آمده یکسان هستند و تنها تفاوت در زمان انجام محاسبات و میزان فضای اشغال‌شده از حافظه است، روش انتخاب رده مناسب برای رویدادهای پایه به‌تفصیل توضیح داده خواهد شد. هرکدام از عملگرهای بولی را می‌توان با ساختار ITE نمایش داد در ذیل ساختار سه عملگر اصلی آمده است:

$$f \wedge g = ITE(f, g, 0) \qquad (۲-۸)$$

$$f \vee g = ITE(f, 1, g) \qquad (۳-۸)$$

$$\bar{f} = ITE(f, 0, 1) \qquad (۴-۸)$$

فرض کنیم $J = ITE(x, F_1, F_2)$ و $H = ITE(y, G_1, G_2)$ و op یک عملگر بولی باشد، در این صورت نحوه تأثیر این عملگر بر روی ساختارهای BDDمطابق رویه زیر است:

$H < op > J = ITE(y, G_1, G_2) < op > ITE(x, F_1, F_2)$ ،حال اگر $x < y$ آنگاه :

$H < op >$

$$ITE(x, F_1 < op > ITE(y, G_1, G_2), F_2 < op > ITE(y, G_1, G_2)) \qquad (۵-۸)$$

و چنانچه $x = y$ آنگاه:

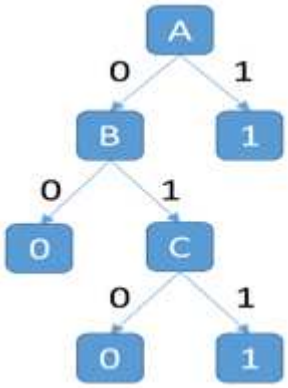
$$H < op > J = ITE(x, F_1 < op > G_1, F_2 < op > G_2) \qquad (۶-۸)$$

[1] ترتیب یا اولویت برای رویداد پایه

برای روشن شدن مطلب رابطه $f = A + (B.C)$ را در نظر می‌گیریم، در تابع f سه متغیر داریم فرض کنیم ترتیب آن‌ها بدین شکل باشد: $A < B < C.$ برای به دست آوردن دیاگرام تصمیم‌گیری این تابع ابتدا برای متغیرها ساختار BDD را نوشته و سپس دو اپراتور تابع را بر ساختارهای متغیرها اعمال می‌کنیم:

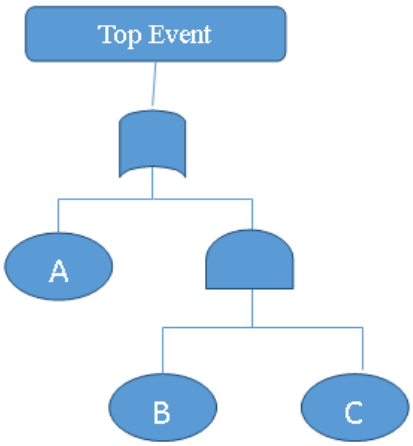
$$f = ITE($$

نمایش گرافیکی درخت تصمیم‌گیری تابع f مطابق شکل زیر است:



شکل ۱۰: نمایش تابع f

درخت خطا برای این ساختار مطابق شکل زیر است که آنالیز کمیت و کیفیت توسط BDD را برای این مثال ساده به طور مختصر شرح می‌دهیم.



شکل ۱۱: درخت خطا

با توجه به درخت خطا، در درخت تصمیم‌گیری به‌دست‌آمده برای رخ دادن رویداد رأس باید مسیرهایی را دنبال کنیم که از گره ریشه شروع و به گره‌های انتهایی یک ختم می‌شوند. لذا دو مسیر داریم ۱- A ، ۲- $\bar{A}.B.C$ ، حال با توجه به اینکه برای هر متغیر داریم: $p_i + q_i = 1$ لذا احتمال رخ دادن رویداد رأس برابر است با:

$$p_{TopEvent} = p_A + q_A.p_B.p_C = p_A + (1 - p_A).p_B.p_C \qquad (۷-۸)$$

در آنالیز کیفیت به دنبال مجموعه‌های برشی هستیم، این مجموعه‌ها درواقع همان دلالت‌کننده‌ها[1] برای یک تابع بولی هستند لذا در مسیرهایی که به گره یک ختم می‌شوند تنها متغیرهایی که رخ می‌دهند را در نظر می‌گیریم با توجه به این مطلب در BDD مثال ما دو مجموعه برشی داریم که درواقع کمینه نیز هستند و عبارت‌اند از: ۱- A ، ۲- $B.C$ [۵][۶][۷][۸]. ورودی این ماژول در کد RELAB 1.0 درخت خطا است و خروجی آن درخت تصمیم‌گیری دودویی، احتمال رخداد رویداد رأس و کمینه‌های برشی هستند که هدف اصلی در آنالیز درخت خطا می‌باشند.

[1] implicant

۹- تحلیل خطای انسانی (HRA)

۹-۱- تعاریف اساسی در قابلیت اعتماد انسانی

رفتار انسانی از لحاظ قابلیت مدل‌سازی ریاضی بسیار پیچیده است و بررسی متون و ادبیات علمی در زمینه تحلیل قابلیت اعتماد انسانی نشان می‌دهد که یک اجماع کلی بر روی تعیین بهترین روش مدل‌سازی قابلیت اعتماد انسانی وجود ندارد. همچنین فرضیات، مکانیسم‌ها و راهبردهای استفاده شده در هر روش، لزوماً قابل استفاده برای همه خطاهای انسانی نیست. خطاهای انسانی در تمامی مراحل طراحی، تولید، ساخت و بهره‌برداری سیستم‌های پیچیده ممکن است اتفاق بیفتد. خطاهای در مراحل طراحی، تولید و ساخت نیز، ممکن است باعث بسیاری از خطاهای در مرحله بهره‌برداری شوند. مهم‌ترین خطاهای انسانی، خطاهایی هستند که موجب خرابی همزمان چند سیستم ایمنی و از دست رفتن افزونگی موجود در سیستم‌ها می‌شود، که به آنها خرابی‌های وابسته[1] نیز می‌گویند. برای جلوگیری از وقوع اینگونه خطاها معمولاً برنامه‌های کنترل و تضمین کیفیت طراحی و پیاده‌سازی می‌شوند.

پیش از اینکه وارد مباحث مربوط به بررسی و مقایسه روش‌های مختلف مدل‌سازی در تحلیل قابلیت اعتماد انسانی شویم، برخی از مهم‌ترین تعاریف و مفاهیم بنیادی در این زمینه در این بخش شرح داده می‌شود. این تعاریف در بیشتر روش‌های تحلیل قابلیت اعتماد انسانی مشترک می‌باشند.

۹-۱-۱ قابلیت اعتماد انسانی

قابلیت اعتماد انسانی برابر است با احتمال اینکه یک فرد، اولاً اعمال مورد نیاز برای یک سیستم را در یک بازه زمانی مشخصی با موفقیت انجام دهد (در صورتی که محدودیت زمانی برای انجام کار تعیین شده باشد)، ثانیاً هیچ اقدام اضافی دیگری که عملکرد سیستم را دچار اختلال می‌کند، انجام ندهد [۹]. تحلیل قابلیت اعتماد انسانی (HRA) نیز به روش و فرآیند مورد استفاده در تخمین میزان قابلیت اعتماد انسانی می‌گویند، که معمولاً در چهارچوب یک تحلیل جامع‌تر، مانند تحلیل احتمالاتی ایمنی (PSA) انجام می‌شود.

1 Dependent Failure

۹-۱-۲ واسط بین انسان و ماشین

در تمامی سیستم‌هایی که یک اپراتور نقش پایش فرآیندهای صورت گرفته توسط سیستم را بر عهده دارد، ارتباط و تعامل بین سیستم و اپراتور وجود خواهد داشت. عبارت واسط بین انسان و سیستم[1] (MMI) به نقاط اندرکنش و تعامل بین سیستم و اپراتور اشاره می‌کند. بنابراین به یک نمایشگر، یک کنترل دستی[2]، دستورات مکتوب، یا هر چیز دیگری که اپراتور برای ارتباط با سیستم از آن استفاده می‌نماید، MMI گفته می‌شود.

۹-۱-۳ نمایشگرها، کنترل‌های دستی و دستورالعمل‌های مکتوب

نمایشگر[3] در مبحث قابلیت اعتماد انسانی به هر گونه ابزار یا وسیله‌ای گفته می‌شود که اطلاعات صوتی یا تصویری از طریق آن به اپراتور ارائه می‌شود. نمایشگرها خود به دو گروه تقسیم می‌شوند: نمایشگرهای دارای هشدار[4] که با هشدارهای صوتی همراه هستند، و نمایشگرهای بدون هشدار[5] که فقط اطلاعات بصری را به اپراتور انتقال می‌دهند.

کنترل‌های دستی به تجهیزات و ابزارهایی گفته می‌شود که اپراتور خروجی حاصل از تصمیم‌گیری خود را، از طریق آن به عنوان ورودی به سیستم انتقال می‌دهد. انواع کنترل‌های دستی در نیروگاه‌های هسته‌ای شامل انواع سوئیچ‌ها، دکمه‌ها، تنظیم‌کننده سطح، کلیدها و غیره می‌شود.

دستورالعمل‌های مکتوب در سه دسته کلی جای می‌گیرند: دسته اول دستورالعمل‌های مکتوب رسمی هستند که ممکن است به دفعات مورد استفاده قرار گیرد. دسته دوم دستورالعمل‌های تهیه شده برای شرایط خاص[6] هستند که معمولاً به صورت غیر رسمی، و برای یک بار استفاده در شرایط خاص، تهیه می‌شود. و در نهایت دسته سوم یادداشت‌های ثبت شده هستند که به دستورالعمل‌هایی گفته می‌شود که در زمان ارائه دستورات شفاهی، توسط اپراتور یادداشت شده است.

1 Man-Machine Interface
2 Manual Control
3 Display
4 Annunciated Displays
5 Unannunciated Displays
6 Ad hoc Procedures

۹-۱-۴ وظیفه و عناصر تشکیل‌دهنده آن

در مباحث قابلیت اعتماد انسانی، به سطحی از رفتار شغلی فرد که انجام یک عملکرد شغلی معنادار را دربرمی‌گیرد، یا هر واحد رفتاری فرد که برای رسیدن به هدف یا عملکرد کلی سیستم بایستی انجام شود، وظیفه[1] می‌گویند. هر وظیفه از عناصر[2] کوچک‌تری تشکیل می‌شود که به تنهایی موجب نیل به هدف سیستم نخواهند شد.

۹-۱-۵ عوامل شکل دهنده عملکرد

در مدل‌سازی قابلیت اعتماد انسانی در چهارچوب تحلیل PSA، لازم است عواملی که بیشترین تأثیر را بر روی عملکرد اپراتور دارند، در نظر گرفته شوند.در سیستم‌های پیچیده‌ای که انسان با سیستم سروکار دارد، مانند نیروگاه‌های هسته‌ای، عواملی زیادی بر روی عملکرد اپراتور تأثیر می‌گذارند، که تعدادی از آنها نسبت به اپراتور عامل خارجی و تعدادی نیز داخلی هستند. عوامل خارجی شامل محیط کار به طور کلی، به خصوص نحوه طراحی سیستم‌ها و تجهیزات، دستورالعمل‌های کتبی یا دستورات شفاهی یادداشت شده می‌باشد. عوامل داخلی نیز شامل ویژگی‌های شخصی اپراتور مانند مهارت‌ها، انگیزه‌ها و انتظارات می‌شود که هر کدام به نحوی بر روی عملکردش تأثیر می‌گذارند.

استرس‌های روانی و جسمی ناشی از شرایط محیط کار و سناریوی حادثه، وابستگی بین عملکرد اپراتورهای مختلف، و کلیشه‌های جمعیتی[3] از مهم‌ترین عوامل شکل دهنده عملکرد اپراتور[4] (PSF) هستند که در تحلیل‌های قابلیت اعتماد انسانی در نظر گرفته می‌شوند. کلیشه‌های جمعیتی در بخش بعد شرح داده خواهد شد.

۹-۱-۶ کلیشه‌های جمعیتی

کلیشه‌های جمعیتی به مجموعه انتظارات گروهی از افراد در یک جامعه، نسبت به نحوه عملکرد یک کنترل، یا حالت‌های نمایش در یک نمایشگر، و نتایج و معانی حاصل از آن اطلاق می‌شود. به عنوان نمونه ما قویاً انتظار داریم در صورتی که یک شیر آب را در خلاف جهت عقربه‌های ساعت بچرخانیم، شیر آب باز شده و در صورت ادامه این کار مقدار جریان آب بیشتر شود. در حالی که در مورد کنترل‌های تنظیم صدا، وقتی کنترل را در خلاف

1 Task
2 Elements
3 Populational Stereotype
4 Performance Shaping Factor

جهت عقربه‌های ساعت می‌چرخانیم، انتظار داریم صدا کم شده و در نهایت قطع شود. نمونه‌ای از کلیشه‌های جمعیتی متفاوت بین فرهنگ‌ها، در مورد کلیدهای روش و خاموش کردن لامپ‌ها می‌باشد. در آمریکا جهت بالا برای روشن شدن لامپ در نظر گرفته می‌شود، در حالی که در اروپا بر عکس آن اجرا می‌شود. جهت خواندن متون نیز نمونه‌ای دیگر از کلیشه‌های جمعیتی است. نحوه تأثیر کلیشه‌های جمعیتی بر روی عملکرد اپراتور به این شکل است که اگر در طراحی یک سیستم این مسئله رعایت نشود، احتمال خطای اپراتور نیز بالا خواهد رفت.

۹-۲ روش پیش‌بینی نرخ خطای انسانی[1] (THERP)

روش THERP توسط سواین[2] و گاتمن[3] توسعه داده شد و اولین بار در سال ۱۹۷۵م. در تحلیل قابلیت اعتماد انسانی در پروژه WASH-1400 مورد استفاده قرار گرفت. این روش در سال ۱۹۸۳ با عنوان کتابچه راهنمای قابلیت اعتماد انسانی و در قالب NUREG-1278 منتشر شد [۹]. روش THERP بعدها تکامل یافته و به صورت روش SPAR-H درآمد [۱۰]، اما در این پروژه به عنوان قدم اول، از روش THERP برای تحلیل قابلیت اعتماد انسانی بهره گرفته شده است. سایر روش‌های تحلیل خطای انسانی در آینده به ماژول تحلیل خطای انسانی افزوده خواهند شد. فرآیند محاسبه احتمال خطای اپراتور در روش THERP شامل ۶ مرحله اصلی می‌باشد که به ترتیب انجام می‌شوند. مراحل اصلی در این فرآیند به ترتیب عبارتند از [۱۱]:

۱. تجزیه یک وظیفه به عناصر تشکیل دهنده
۲. مدل‌سازی وظیفه با استفاده از رسم درخت رویداد HRA
۳. اختصاص مقادیر احتمال نامی به هر کدام از عناصر درخت رویداد
۴. تعیین اثر عوامل شکل دهنده عملکرد (PSF) بر روی هر عنصر
۵. محاسبه اثر وابستگی[4] بین وظایف
۶. محاسبه احتمال خطای انسانی مربوط به کل وظیفه

هر کدام از این مراحل در بخش‌های آتی شرح داده خواهند شد.

1 Technique for Human Error Rate Prediction
2 Swain
3 Guttman
4 Dependency

۹-۲-۱ تجزیه یک وظیفه به عناصر تشکیل‌دهنده

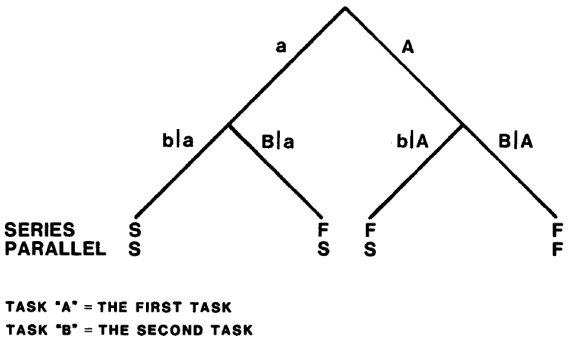
اولین قدم در روش THERP تجزیه یک وظیفه به عناصر تشکیل‌دهنده آن می‌باشد، که بر اساس طبقه‌بندی[۱] وظایف در این روش صورت می‌گیرد. به عنوان مثال اگر برای انجام یک وظیفه ایمنی به خصوصی، باید پنج عملکرد مجزا توسط دو اپراتور در دو مکان مختلف صورت بگیرد، این وظیفه ابتدا به پنج عنصر تشکیل دهنده آن تجزیه می‌شود، سپس هر کدام از این پنج عنصر به تنهایی مورد تحلیل و بررسی قرار می‌گیرند. یکی از تعاریف اساسی در روش THERP، که در واقع مبنای تقسیم یک وظیفه ایمنی به عناصر آن نیز می‌باشد، مفهوم واحد ادراکی[۲] است. برای انجام هر کدام از عناصر یک وظیفه ایمنی، اپراتور لزوماً فقط با یک کنترل یا تجهیز سر و کار نخواهد داشت، و ممکن است یک عمل مشابه را به طور همزمان یا در فاصله زمانی کوتاهی، بر روی دو یا چند کنترل انجام دهد. به عنوان نمونه اگر قرار است اپراتور وضعیت دو کلید را بصورت همزمان و در یک جهت تغییر دهد، مجموعه دو کلید تشکیل یک واحد ادراکی می‌دهد. یعنی اگر اپراتور وضعیت یکی از این دو کلید را تغییر ندهد، دیگری را نیز تغییر نخواهد داد.

در روش THERP، طبقه‌بندی انواع خطاهای اپراتور در جداولی ارائه شده است، که جهت تعیین نوع و احتمال وقوع هر یک از عناصر یک وظیفه کلی، باید از این جداول استفاده نمود. تقسیم‌بندی خطاهای اپراتور در این جداول با توجه به شرایط بهره‌برداری سیستم (کارکرد نرمال یا شرایط حادثه)، نوع وظیفه اپراتور (تشخیص[۳] شرایط یا عمل بر اساس دستورالعمل‌ها[۴])، نوع واسط بین اپراتور و سیستم[۵] (نمایشگرها، شیرها یا دستورالعمل‌های مکتوب[۶]) و همچنین نوع خطای اپراتور (Omission یا Commission) می‌باشد. اما استفاده از این جداول و تعیین اینکه احتمال هر خطا با استفاده از کدام جدول بایستی تعیین شود طبق روال خاصی انجام می‌شود که به آن روش جستجو[۷] اطلاق می‌شود. در روش جستجو تحلیل‌گر با پاسخ دادن به تعدادی سوال به صورت متوالی در نهایت نوع وظیفه و احتمای خطای اپراتور در انجام آن را تعیین می‌کند. این روش به طور مفصل در بخش‌های آتی شرح داده خواهد شد.

1 Taxonomy
2 Perceptual Unit
3 Diagnosis
4 Rule Based Action (RBA)
5 Man-Machine Interface (MMI)
6 Written Material
7 Search Scheme

۹-۲-۲ مدل‌سازی در درخت رویداد خطای انسانی

پس از تجزیه یک وظیفه به عناصر تشکیل دهنده 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[1] نامیده می‌شود قرار داده می‌شوند. این درخت رویداد روند منطقی انجام عناصر مختلف توسط اپراتورها را نمایش می‌دهد. مدل‌سازی در این درخت از اولین عنصر یک وظیفه که باید قبل از بقیه عناصر انجام شود، شروع می‌شود. این عنصر اولین گره درخت تصمیم دودویی را می‌سازد و دو یال متصل به آن نشان دهنده دو حالت موفقیت و عدم موفقیت در انجام آن می‌باشد. مطابق شکل ۱۲، برای هر عنصر وظیفه دو مسیر موفقیت و خطا وجود دارد، که مسیر سمت چپ (a) مربوط به موفقیت و مسیر سمت راست (A) مربوط به خطا می‌باشد.



شکل ۱۲: درخت رویداد تحلیل HRA

در ادامه هر کدام از مسیرهای موفقیت یا خطای هر گره، عناصر دیگر وظیفه به ترتیب منطقی و زمانی در نظر گرفته خواهند شد. برای هر کدام از این عناصر نیز مشابه قبلی عمل می‌شود. در نهایت هر کدام از این مسیرها بایستی به یکی از دو وضعیت موفقیت[2] (S) یا خرابی[3] (F) کل سیستم منتهی بشوند. در رسم درخت دودویی خطای انسانی باید دو نکته مهم درنظر گرفته شود. نکته اول اینکه چپ‌ترین مسیر این درخت، یعنی مسیری که در آن همه عناصر وظیفه با موفقیت انجام شده است، قطعا به موفقیت سیستم منجر می‌شود. نکته دوم نیز این

1 HRA Event Tree
2 Success
3 Failure

است که در انتهای یال راست گره‌ها حالت موفقیت امکان‌پذیر نیست، چون این بدین معنی است که خطای اپراتور منجر به موفقیت سیستم شده است.

آنچه که در نهایت مدنظر تحلیل‌گر می‌باشد، احتمال مربوط به مسیرهایی می‌باشد که به خرابی سیستم منجر شده است. پس از تقسیم عملکرد اپراتور به اجزای آن و مدل‌سازی در درخت رویداد، باید مقادیر احتمال هر کدام از یال‌های درخت رویداد محاسبه شود. برای این کار ابتدا باید نوع هر کدام از این خطاها با توجه به تقسیم‌بندی اعمال اپراتور در روش THERP تعیین شود، سپس از جداول مربوطه مقدار احتمال آن استخراج شود.

۹-۲-۳ تقسیم‌بندی انواع اعمال اپراتور

عناصر مربوط به یک وظیفه در روش THERP را می‌توان به طور کلی به دو دسته عملکرد تشخیص[1] خرابی توسط اپراتور، و عمل مبتنی بر دستورالعمل[2] (RBA) تقسیم نمود. در عملکرد تشخیص، اپراتور باید با توجه به پارامترهای فیزیکی فرآیند و از طریق اعلان‌ها و هشدارها وضعیت سیستم را تشخیص دهد، تا بر اساس آن تصمیم لازم گرفته شود. به طور کلی به فرآیند یافتن محتمل‌ترین علل شرایط غیرعادی نیروگاه و در نتیجه تشخیص سیستم‌های لازم برای مقابله با این شرایط، تشخیص می‌گویند. عمل مبتنی بر دستورالعمل نیز به مجموعه رفتارهایی توسط اپراتور گفته می‌شود که بر اساس دستورات مکتوب یا دستورات شفاهی یادداشت شده انجام می‌شوند. نمونه‌هایی از عمل بر اساس دستورالعمل کالیبره کردن یک ابزار یا تغییر وضعیت تعدادی شیر دستی از روی یک چک لیست می‌باشد.

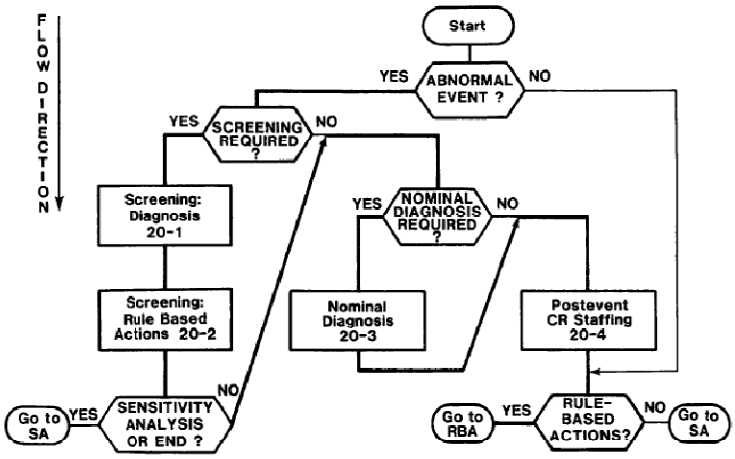
خطاهای RBA نیز خود به دو دسته خطاهای Omission و Commission تقسیم می‌شوند. خطاهای Omission به آن دسته از خطاها اطلاق می‌شود که ناشی از غفلت و فروگذاری اپراتور از انجام دادن یک وظیفه می‌باشند، که باید در زمان و شرایط مشخصی انجام شوند. خطاهای Commission برخلاف دسته قبلی، به خطاهای ناشی از عملکرد اشتباه اپراتور اطلاق می‌شود که به بدتر شدن روند حادثه منجر می‌شوند.

همانطور که در بخش قبل نیز اشاره شد، در روش THERP دستورالعمل تقسیم یک وظیفه به عناصر تشکیل‌دهنده آن، طبق روال مشخصی تحت عنوان روش جستجو انجام می‌شود. در فلوچارت روش جستجو، با استفاده از تعدادی سوال و جواب به صورت زنجیره‌ای و متوالی، نوع عنصر مورد بررسی با توجه به طبقه‌بندی

1 Diagnosis
2 Rule Based Action

اعمال اپراتور در روش THERP تعیین می‌شود. در ادامه، سوالاتی که به منظور تعیین احتمال خطای اپراتور باید پاسخ داده شوند، مشابه مرجع [۹] ارائه می‌شود.

۱. اولین سوالی که در این فلوچارت باید پاسخ داده شود این است که آیا رویداد نامطلوبی رخ داده است؟ در صورت مثبت بودن پاسخ، ابتدا نیاز به تشخیص رویداد نامطلوب توسط اپراتور وجود دارد، و سپس عمل اپراتور پس از تشخیص شرایط، بررسی می‌شود. در صورت عدم وقوع رویداد نامطلوب، باید مستقیماً بررسی کرد که آیا نیاز به عملکرد اپراتور وجود دارد یا خیر؟



شکل ۱۳: فلوچارت تعیین نوع اعمال اپراتور در روش THERP

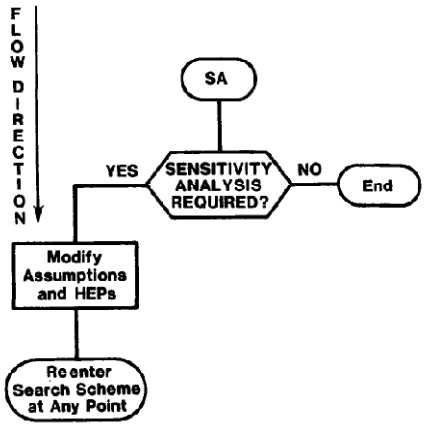
۲. در صورت مثبت بودن پاسخ در مرحله پیش، پرسش بعدی این است که آیا تحلیل HRA در مرحله غربالگری[1] صورت می‌گیرد یا خیر؟ در مرحله غربالگری مقادیر احتمال بسیار بالایی به خطاهای اپرتور نسبت داده می‌شود، و در صورتی که مقادیر بالای احتمال خطای اپراتور در محاسبات تحلیل سیستم تأثیر قابل توجهی نداشته باشد، این خطا از محاسبات حذف شده و در نظر گرفته نمی‌شود. این مرحله در واقع ارتباط مستقیم با تحلیل سیستم با استفاده از درخت خطا دارد.

1 Screening

۳. در صورتی که تحلیل HRA در مرحله غربالگری باشد، امکان انتخاب از بین دو نوع خطای تشخیص، یا عمل بر اساس دستورات (RBA) وجود دارد. مقادیر احتمال خطاهای تشخیص و RBA در حالت تحلیل غربالگری، از دو جدول جداگانه ۲۰-۱ و ۲۰-۲ مرجع [۹] استخراج می‌شوند.

۴. در مواردی ممکن است تحلیل HRA پس از اختصاص مقادیر غربالگری خاتمه یابد، یا اینکه پس از اختصاص مقادیر غربالگری تحلیل حساسیت[1] صورت گیرد. در هر دو صورت در پاسخ به سوال Sensitivity Analysis or End? در شکل ۱۳، بایستی مسیر مربوط به پاسخ مثبت دنبال شود. این مسیر منتهی به شکل ۱۴ خواهد شد. اما در صورت پاسخ منفی، ادامه مسیر همانند پاسخ منفی به سوال ۲ است.

۵. اگر پس از اختصاص مقادیر غربالگری، لازم شد تحلیل دقیق‌تری صورت گیرد، بایستی مسیر مربوط به پاسخ منفی در سوال قبلی دنبال شود. همانگونه که در شکل ۱۵ نیز مشاهده می‌شود، اولین پرسش در این مسیر این است که آیا نیاز به تشخیص اپراتور وجود دارد؟ در صورت مثبت بودن پاسخ، مقادیر احتمال از جدول ۲۰-۳ مرجع [۹] انتخاب خواهد شد. محدودیت‌های مربوط به بازه زمانی تشخیص حادثه توسط اپراتور، در چهارچوب تحلیل PSA و توسط کارشناسان تحلیل سیستم تعیین می‌شود.



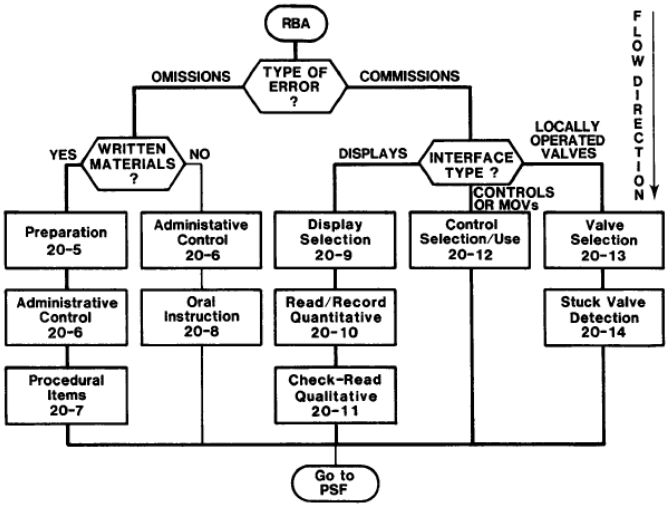
شکل ۱۴: فلوچارت تحلیل حساسیت در روش THERP

1 Sensitivity

۶. پس از تشخیص حادثه و قبل از تعیین نوع عمل اپراتور برای جلوگیری از پیشروی حادثه و تعیین احتمال عدم موفقیت در انجام آن، بهتر است تعداد و ترکیب افراد در اتاق کنترل و ارتباط بین آنها از لحاظ وابستگی مشخص شود. جدول ۲۰-۴ مرجع [۹] فرضیات مربوط به تعداد اپراتورها در اتاق کنترل بر حسب زمان پس از تشخیص شروع حادثه را نشان می‌دهد. این فرضیات به تحلیل‌گر اجازه می‌دهد روابط بین اپراتورها پس از شروع حادثه را به صورت ساخت یافته در نظر بگیرد. روابط بین اپراتورها از لحاظ سطح وابستگی یکی از عوامل شکل‌دهنده عملکرد (PSF) می‌باشد، که در بخش‌های بعدی گزارش بطور مفصل مورد بحث قرار خواهد گرفت. البته لازم به ذکر است که این مسئله در صورتی حائز اهمیت است که بعد از تشخیص شرایط غیر عادی نیازی به عملکرد اپراتور باشد.

۷. پرسش بعدی مربوط به این است که آیا لازم است پس از تشخیص حادثه، عملی توسط اپراتور صورت بگیرد؟ در صورت پاسخ منفی به این سوال، تحلیل‌گر بایستی در مورد انجام تحلیل حساسیت یا پایان تحلیل HRA تصمیم بگیرد، که مشابه حالت تحلیل غربالگری، به شکل ۱۵ وارد می‌شود.

۸. اما در صورتی که بعد از تشخیص شرایط بهره‌برداری غیرعادی، نیاز به عملکرد اپراتور نیز باشد، تحلیل‌گر بایستی نوع عملی را که اپراتور قرار است انجام دهد تعیین کند. در واقع پرسش بعدی پاسخ بلی و خیر ندارد، بلکه در آن نوع خطای اپراتور تعیین می‌شود. همانطور که پیشتر نیز گفته شد، خطاهای اپراتور در انجام یک عمل مبتنی بر دستورات به دو دسته خطاهای Omission و Commission تقسیم می‌شود. اگر خطای اپراتور از نوع غفلت از انجام یک کار است مسیر مربوط به Omission دنبال می‌شود، و در صورتی که نوع خطای اپراتور انجام ندادن درست یک وظیفه باشد مسیر Commission دنبال خواهد شد.



شکل ۱۵: فلوچارت تعیین نوع اعمال مبتنی بر دستورالعمل (RBA) در روش THERP

۹. در صورت انتخاب گزینه خطای Omission، پرسش بعدی مربوط به وجود یا عدم وجود دستورات مکتوب است. دستورالعمل‌های مکتوب شامل مواردی مانند دستورالعمل‌های رسمی[۱]، دستورالعمل‌های تهیه شده برای شرایط خاص[۲] یا دستورات شفاهی[۳] یادداشت شده می‌باشد.

- در صورت وجود دستورات رسمی مکتوب، با استفاده از جداول ۲۰-۵، ۲۰-۶ و ۲۰-۷ مرجع [۹]، به ترتیب احتمال خطا در آماده‌سازی دستورالعمل‌ها جهت استفاده، خطا در اجرای دستورالعمل‌ها[۴]، و غفلت[۵] از انجام یک دستورالعمل را می‌توان تعیین نمود.
- عدم وجود دستورات نوشته شده، بدین معنی است که اپراتور با اتکا به حافظه‌اش عمل خواهد کرد. جدول ۲۰-۶ مرجع [۹]، مقادیر احتمال خطا در اجرای دستورالعمل‌ها توسط اپراتور و جدول ۲۰-۸ نیز مقادیر احتمال خطا در انجام دستورات شفاهی بر اساس تعداد مواردی که لازم است اپراتور به یاد آورد، ارائه نموده است.

۱۰. اما در صورتی که خطای اپراتور از نوع Commission باشد، پرسش بعدی مربوط به نوع واسط بین اپراتور و سیستم (MMI) است. واسط‌های بین اپراتور و سیستم به سه دسته کلی نمایشگرها، کنترل‌ها یا شیرهای کنترلی[۶] (MOV)، و شیرهای با عملکرد کنترل محلی[۷] تقسیم شده است.

در مورد نمایشگرهای بدون هشدار که در اینجا در نظر گرفته می‌شوند، سه نوع خطای اشتباه در انتخاب نمایشگر، خطا در خواندن و ثبت اطلاعات کمی نمایشگر، و خطای خواندن و بررسی اطلاعات کیفی نمایشگر وجود دارند، که مقادیر خطاهای مرتبط با آنها به ترتیب در جداول ۲۰-۹، ۲۰-۱۰ و ۲۰-۱۱ مرجع [۹] داده شده است.

در مورد کنترل‌ها یا شیرهای کنترلی (MOV) جدول ۲۰-۱۲ احتمال انواع خطاهای مرتبط با انتخاب و استفاده از آنها را ارائه می‌کند.

1 Formal Procedures
2 Ad hoc Procedures
3 Oral Instructions
4 Administrative Control
5 Omission
6 Motor Operated Valve
7 Locally Operated Valves

در مورد شیرهایی نیز که اپراتور بایستی در محل آنها عمل کنترل را انجام دهد، مقادیر احتمال خطا در انتخاب شیرها، و خطا در تشخیص خرابی شیرها به ترتیب در جداول ۲۰-۱۳ و ۲۰-۱۴ داده شده است.

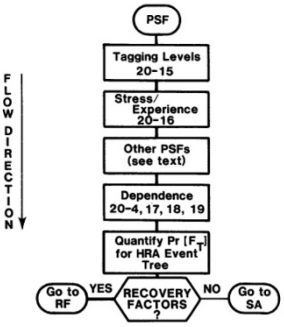
مقادیر احتمال خطای انسانی داده شده در جداولی که تا کنون از آنها نام برده شد، مقادیر عمومی می‌باشند، بدین معنی که مقادیر آنها را می‌توان با تقریب خوبی در تحلیل HRA هر نیروگاه یا سیستمی استفاده نمود. اما خطاهای انسانی همیشه در شرایط یکسانی رخ نمی‌دهند، بنابراین باید اثر شرایطی که اپراتور با توجه به آن عمل می‌کند، بر روی مقادیر یادشده اعمال شود. به عنوان مثال کیفیت دستورالعمل‌ها یا میزان تجربه اپراتور نقش به سزایی در تعیین نحوه عملکرد او دارد. این مسئله به تفصیل در بخش بعد مورد بررسی قرار گرفته است.

۹-۲-۴ فاکتورهای شکل دهنده عملکرد اپراتور

مقادیر نامی احتمال خطاهای اپراتور بسیار کلی بوده و نشان دهنده وضعیت دقیق یک نیروگاه خاص از لحاظ عملکرد اپراتور نمی‌باشد. واضح است که با توجه به شرایط خاص یک نیروگاه از لحاظ فاکتورهای شکل‌دهنده عملکرد اپراتور، مانند کیفیت آموزش اپراتورها، کیفیت دستورالعمل‌ها و نحوه طراحی واسط اپراتور و سیستم، احتمال خطای اپراتور می‌تواند نسبت به یک نیروگاه دیگر پایین‌تر یا بالاتر باشد. در تحلیل‌های مرسوم PSA، تعیین اثر PSFها بر اساس شناخت کیفی خود تحلیل‌گر از شرایط سناریو شامل تحلیل وظیفه[1] و همچنین بررسی محیط انجام وظیفه مانند اتاق کنترل نیروگاه، صورت می‌گیرد.

بررسی تعیین اثر PSF بر روی افزایش یا کاهش احتمال خطای اپراتور در روش THERP، در شکل ۱۶ نشان داده شده است. همانطور که مشاهده می‌کنید عوامل اثرگذار بر روی عملکرد اپراتور بطور کلی در چهار مورد خلاصه شده است، و پس از تعیین آنها می‌توان احتمال خطای اپراتور را محاسبه نمود. از این چهار عامل، میزان وابستگی بین عناصر مختلف که در شکل آمده است، به صورت مستقل در بخش بعد مورد بررسی قرار خواهد گرفت. سه عامل دیگر عبارتند از: سطح برچسب‌گذاری[2]، استرس و تجربه، و سایر عوامل PSF.

[1] Task Analysis
2 Tagging Level



شکل ۱۶: اثر فاکتورهای شکل‌دهنده عملکرد بر روی مقادیر نامی احتمال خطا

برچسب‌گذاری فرآیندی در بهره‌برداری از نیروگاه هسته‌ای می‌باشد که طی آن جهت اطلاع از وضعیت هر کدام از سیستم‌ها و تجهیزات ایمنی از یک برچسب[1] و یک لیست جهت ثبت این برچسب‌ها استفاده می‌شود. بنابراین با استفاده از این برچسب‌ها و لیست آنها در هر لحظه اپراتور متوجه می‌شود که چه سیستمی در دسترس است و کدام سیستم به دلایلی از دسترس خارج شده است. در روش THERP، سطح برچسب‌گذاری به طور مستقیم در احتمال خطا تأثیر ندارد و فقط بر روی توزیع عدم قطعیت احتمال خطا تأثیر می‌گذارد. بنابراین با توجه به اینکه تحلیل عدم قطعیت در حال حاضر به صورت سیستماتیک در کد ReLab پیاده‌سازی نشده است، در این پروژه نیز این عامل در نظر گرفته نخواهد شد.

مهم‌ترین عامل شکل‌دهنده عملکرد اپراتور در روش THERP، اثر استرس و تجربه می‌باشد. این PSF در واقع اثر مجموع سه عامل اساسی شکل‌دهنده عملکرد اپراتور را باهم در خود دارد. این سه عامل اساسی عبارتند از:

- سطح استرس، که با پیچیدگی سناریوی حادثه ارتباط مستقیم دارد
- مهارت اپراتور، که با کیفیت آموزش ارتباط دارد
- کیفیت دستورالعمل‌های مدیریت حادثه

نحوه تأثیر این سه عامل بر روی تغییر احتمال خطای اپراتور در جدول شماره ۲ نشان داده شده است. در این جدول ستون دوم سطوح مختلف استرس را نشان می‌دهد که به چهار سطح خیلی پایین، متوسط، نسبتاً بالا و خیلی بالا تقسیم شده‌اند. ستون بعدی این جدول نشان دهنده نوع دستورالعمل‌های مورد استفاده در تأسیسات

[1] Tag

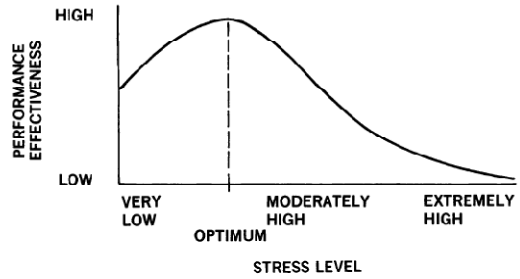
مورد نظر می‌باشد، که در دو دسته کلی دستورالعمل‌های مرحله- به- مرحله[1] و دستورالعمل‌های پویا[2] تقسیم می‌شوند. در نهایت دو ستون بعدی با توجه به مهارت اپراتور، که به دو سطح مبتدی[3] و ماهر[4] تقسیم شده است، و ترکیبی از دو عامل انتخاب شده از ستون‌های قبل، یعنی میزان استرس و نوع دستورالعمل‌ها، ضریب اعمال شده بر روی احتمال اپراتور را نشان می‌دهد. به عنوان مثال در صورتی که سطح استرس ناشی از سناریو نسبتاً بالا، نوع دستورالعمل‌ها پویا و اپراتور نیز ماهر باشد، عدد خام تعیین شده برای احتمال خطای اپراتور در مراحل قبل، در عدد ۵ ضرب خواهد شد.

جدول شماره ۲: تغییر احتمال خطای اپراتور در اثر عوامل شکل‌دهنده عملکرد (PSF)

Item	Stress Level	Procedure Type	Skilled Op.	Novice Op.
1	Very Low	-	x2	x2
2	Optimum	Step-by-Step	x1	x1
3		Dynamic	x1	x2
4	Moderately High	Step-by-Step	x2	x4
5		Dynamic	x5	x10
6	Extremely High	Step-by-Step	x5	x10
7		Dynamic	0.25	0.50

یکی از نکات جالبی که در جدول شماره ۲ مشاهده می‌شود این است که در حالت استرس خیلی پایین، احتمال خطای اپراتور در ضریب دو ضرب خواهد شد، در حالی که در حالت استرس بهینه به جز در یک حالت (اپراتور مبتدی و دستورالعمل‌های پویا)، احتمال خطای اپراتور تغییر نمی‌کند. این مسئله از اینجا ناشی می‌شود که استرس همیشه عاملی در جهت افزایش احتمال خطا نمی‌باشد و برای عملکرد بهینه اپراتور یک سطح حداقلی از استرس لازم است. این موضوع در شکل ۱۷ به خوبی نشان داده شده است.

1 Step-by-Step
2 Dynamic
3 Novice
4 Skilled



شکل ۱۷: ارتباط بین سطح استرس و عملکرد اپراتور

مرحله بعد نیز فقط از این جهت در نظر گرفته شده است، که اثر سایر عوامل در یک نیروگاه بر روی عملکرد اپراتور در نظر گرفته شود. هر نیروگاهی معمولاً دارای تعدادی عوامل خاص خودش می‌باشد که ممکن است در سایر نیروگاه‌ها وجود نداشته باشد، و بر روی عملکرد اپراتورها نیز تأثیر می‌گذارد. این عوامل در این مرحله در نظر گرفته می‌شود، و مقادیر و ضرایب لازم در این مرحله توسط تحلیل‌گر تعیین می‌شود.

۹-۲-۵ وابستگی بین عناصر

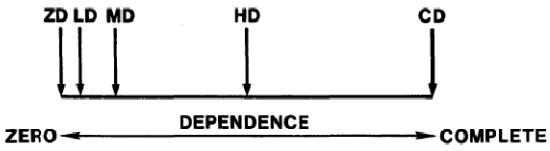
انجام چند عنصر عملکردی توسط اپراتورهای مختلف در جهت انجام یک عملکرد کلی ایمنی معمولاً از یکدیگر مستقل نمی‌باشند. در نظر گرفتن وابستگی بین این عناصر از این لحاظ حائز اهمیت می‌باشد، که ممکن است عملکرد یک اپراتور در انجام یک وظیفه بر روی عملکرد اپراتور دیگر تأثیر منفی یا مثبت بگذارد. در حالت‌های حدی ممکن است انجام یک کار اشتباه توسط یک اپراتور، انجام کار دیگری توسط اپراتور بعدی را غیرممکن سازد یا بر عکس. دو رویداد در صورتی مستقل از همدیگر هستند که احتمال شرطی وقوع یکی از آنها، در صورت وقوع یا عدم وقوع رویداد دیگر هیچ تغییری نکند. این عبارت به زبان احتمالات به صورت زیر بیان می‌شود.

$$P(A)=P(A\,|\,B)=P(A\,|\,b) \qquad (۱-۹)$$

لازم به ذکر است که وابستگی لزوماً بین دو اپراتور مختلف اتفاق نمی‌افتد، بلکه مجموعه کارهایی که توسط یک اپراتور انجام می‌شود نیز ممکن است به یکدیگر وابسته باشند. مثلاً وقتی اپراتور دو شیر در کنار هم را می‌بندد، یا دو سوئیچ در کنار هم را قطع می‌کند، احتمال موفقیت در انجام هر کدام از این وظایف به دیگری وابسته است.

۹-۲-۵-۱ مدل‌سازی وابستگی خطاهای انسانی

روشی که در این پروژه برای مدل‌سازی وابستگی خطاهای انسانی مورد استفاده قرار گرفته است، روش وابستگی مثبت[1] می‌باشد. کلمه مثبت در اینجا به معنی افزایش احتمال وقوع رویداد وابسته، در صورت وقوع رویداد پیشین می‌باشد. این روش براساس عوامل انسانی تخمینی از روابط احتمال شرطی را تعیین می‌کند. روابط احتمال شرطی در این روش، روابط ریاضی می‌باشند که تابع سطح وابستگی بین دو عملکرد هستند. مدل مورد استفاده در این روش یک طیف مثبت کامل از عدم وابستگی تا وابستگی کامل را در برمی‌گیرد، که در شکل ۱۸ نیز نشان داده شده است.



شکل ۱۸: طیف وابستگی مثبت بین اعمال اپراتور

همانطور که اشاره شد، وابستگی مثبت به معنی وجود یک رابطه مثبت بین رویدادها است، بدین صورت که موفقیت در انجام یک وظیفه منجر به افزایش احتمال موفقیت در انجام وظیفه بعدی می‌شود و بالعکس، عدم موفقیت در انجام یک وظیفه منجر به افزایش احتمال عدم موفقیت در انجام وظیفه بعدی می‌شود. این وابستگی به زبان ریاضی به صورت زیر بیان می‌شود:

$$P(B|A) > P(B) \quad \text{or} \quad P(B|a) < P(B) \qquad (۹-۲)$$

وابستگی منفی به معنی وجود یک رابطه منفی بین رویدادها است، بدین صورت که عدم موفقیت در انجام یک وظیفه منجر به کاهش احتمال عدم موفقیت در انجام وظیفه بعدی می‌شود و بالعکس، موفقیت در انجام یک وظیفه باعث کاهش احتمال موفقیت در انجام وظیفه بعدی می‌شود. این مسئله ممکن در زندگی روزمره نیز روی دهد، مثلاً گاهی موفقیت در انجام کاری باعث کمتر شدن دقت در انجام کار بعدی و در نتیجه افزایش احتمال عدم موفقیت می‌شود. این وابستگی به زبان ریاضی به صورت زیر بیان می‌شود:

$$P(B|A) < P(B) \quad \text{or} \quad P(B|a) > P(B) \qquad (۹-۳)$$

1 Positive Dependence

بنابراین به طور کلی درجه وابستگی بین اعمال اپراتور، یا بین رویدادهای سیستم و عکس‌العمل اپراتور نسبت به آنها، یک طیف پیوسته از وابستگی منفی کامل[1] تا عدم وابستگی کامل[2] (وابستگی صفر) تا وابستگی مثبت کامل[3] را در بر می‌گیرد. با اینکه در روش THERP فقط قسمت مثبت این طیف در نظر گرفته می‌شود، گاهی در تحلیل‌های دقیق‌تر قابلیت اعتماد انسانی ضروری است که وابستگی منفی نیز در نظر گرفته شود.

۹-۲-۵-۲ سطوح وابستگی

وابستگی بین رویدادها در عمل یک طیف پیوسته‌ای را شکل می‌دهد، و لازم است میزان وابستگی بین تمامی رویدادها برآورد و تعیین شود. این مسئله ممکن است در هنگام مدل‌سازی دشواری‌هایی را ایجاد کند، در نتیجه لازم است ساده‌سازی‌هایی در فرآیند مدل‌سازی صورت گیرد. راهبرد مورد استفاده در مدل‌سازی وابستگی در روش THERP این است که این طیف پیوسته به تعدادی نقاط گسسته از هم تقسیم شده است. این نقاط به ترتیب عبارتند از: وابستگی صفر[4] (ZD)، وابستگی کم[5] (LD)، وابستگی متوسط[6] (MD)، وابستگی زیاد[7] (HD) و وابستگی کامل[8] (CD).

جدول شماره ۳: روابط تعیین احتمال خطای اپراتور در سطوح مختلف وابستگی

Item	Level of Dependence	Dependency Equation
1	Zero Dependence (ZD)	$\Pr\left[F(N)\middle\vert F(N-1)\middle\vert ZD\right]=N$
2	Low Dependence (LD)	$\Pr\left[F(N)\middle\vert F(N-1)\middle\vert LD\right]=\frac{1+19N}{20}$
3	Medium Dependence (MD)	$\Pr\left[F(N)\middle\vert F(N-1)\middle\vert MD\right]=\frac{1+6N}{7}$
4	High Dependence (HD)	$\Pr\left[F(N)\middle\vert F(N-1)\middle\vert HD\right]=\frac{1+N}{2}$
5	Complete Dependence (CD)	$\Pr\left[F(N)\middle\vert F(N-1)\middle\vert CD\right]=1$

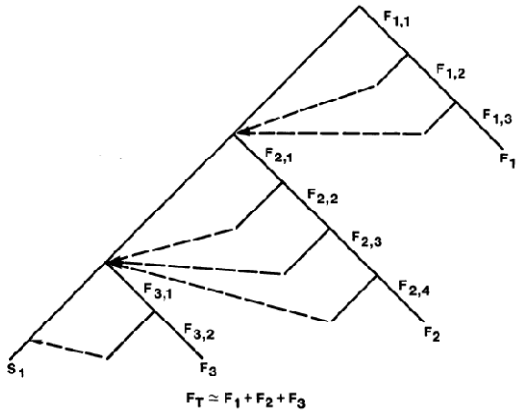
در روابط ستون دوم جدول ۳، حرف N نشان‌دهنده عملکردی از اپراتور می‌باشد که تعیین و محاسبه احتمال آن با در نظر گرفتن شرط وابستگی مدنظر است، و (N-1) نیز نشان دهنده عملکرد قبلی می‌باشد که عملکرد Nام به آن

1 Complete Negative Dependence
2 Complete Independence
3 Complete Positive Dependence
4 Zero Dependence
5 Low Dependence
6 Moderate Dependence
7 High Dependence
8 Complete Dependence

وابسته است. در رابطه داده شده برای محاسبه احتمال شرطی وابستگی نیز، به جای N باید احتمال خام خطای وابسته قرار داده شود. در دو حالت وابستگی صفر و وابستگی کامل جواب‌ها بدیهی می‌باشد. یعنی در صورتی که عملی به عمل قبلی وابسته نباشد احتمال آن تغییر نخواهد کرد. همچنین در صورت وجود وابستگی کامل اگر عمل قبلی موفق نباشد، دومی نیز حتماً موفق نخواهد بود.

۹-۲-۶ عوامل بازیابی

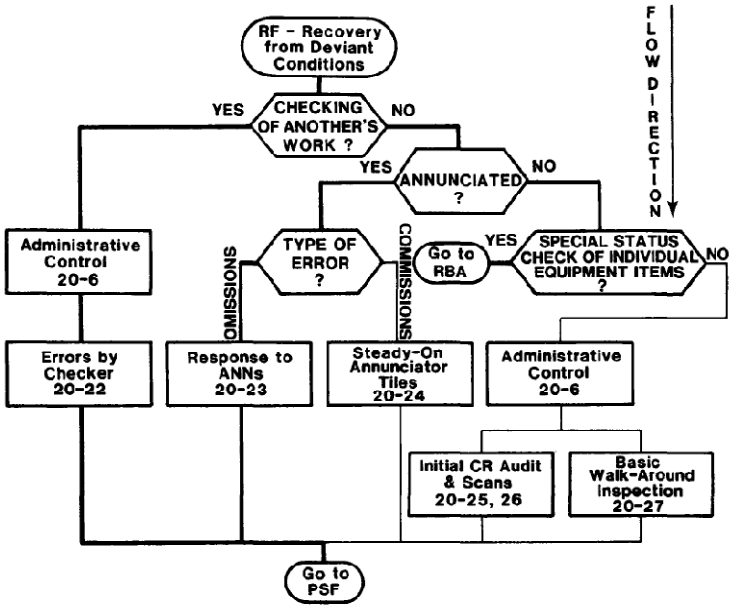
در بهره‌برداری از نیروگاه‌های هسته‌ای، معمولاً تعداد کمی از خطاهای اپراتور در نهایت منجر به آسیب دیدن نیروگاه یا پایین آمدن میزان دسترسی‌پذیری[1] به سیستم‌ها می‌شوند. زیرا تجهیزات، سیستم‌ها یا اپراتورهای دیگری می‌توانند از پیامدهای ناخواسته احتمالی جلوگیری کرده و خطای اپراتور را به نوعی جبران کنند. این عوامل بازدارنده و جبرانی، در اصطلاح عوامل بازیابی[2] (RF) نامیده می‌شوند. اغلب عوامل بازیابی مربوط به بازبینی عملکرد یک اپراتور[3] توسط اپراتور دیگر می‌باشد، که به این دسته از عوامل بازیابی، افزونگی انسانی[4] نیز گفته می‌شود. با توجه به آنچه در شکل ۱۸ مشاهده می‌کنید، اعمال $F_{1,2}$، $F_{1,3}$، $F_{2,2}$، $F_{2,3}$، $F_{2,4}$ و $F_{3,2}$ همگی از نوع عوامل بازیابی هستند، و موفقیت در انجام هر کدام از آنها معادل این است که خطای قبلی روی نداده است. این موضوع در شکل با استفاده از خط‌چین نشان داده شده است. مثلا دو خط‌چین مربوط به $F_{1,2}$ و $F_{1,3}$ به این معنی هستند که موفقیت در انجام هر کدام از آنها معادل موفقیت در $F_{1,1}$ می‌باشد و ادامه این مسیر از همان جا دنبال می‌شود.



شکل ۱۹: اعمال بازیابی در درخت رویداد خطای انسانی

1 Availability
2 Recovery Factor
3 Checking of Another's Work
4 Human Redundancy

اعمال بازیابی به چهار دسته کلی تقسیم می‌شوند: افزونگی انسانی، علائم هشدار دهنده، بازرسی‌های فعال[1] و بازرسی‌های غیر فعال[2]. عامل بازیابی مربوط به افزونگی انسانی، به دلیل جنبه‌های روان‌شناسی قضیه، یکی از حالت‌هایی است که نیاز به بررسی دقیق‌تری دارد. علائم هشدار دهنده معمولاً آنقدر الزام‌آور[3] و مجاب کننده هستند که توجه نکردن به آنها تقریباً غیرمحتمل است، و در نتیجه یکی از بهترین عوامل بازیابی هستند. بازرسی‌های فعال به آن دسته از بازرسی‌ها گفته می‌شود که در آنها هدف اپراتور بازرسی موارد مشخصی از تجهیزات بر اساس دستورالعمل‌های مکتوب می‌باشد. در مقابل، در بازرسی‌های غیر فعال، جستجو برای یافتن تجهیزات و سیستم‌های معیوب به صورت غیر جدی[4] انجام می‌شود. در صورت وجود شرایط انحرافی[5] در حالت بهره‌برداری عادی، یعنی هنگامی که یک سیستم یا تجهیز در وضعیت عادی خود قرار ندارد، به طور کلی دو نوع عامل بازیابی وجود دارد: چک کردن و بازبینی دوباره عمل یک اپراتور، یا بازرسی شرایط کلی نیروگاه از لحاظ وجود شرایط انحرافی. هر کدام از این مسیرها در ادامه بررسی خواهند شد. برای تعیین نوع و احتمال عوامل بازیابی نیز، همان فلوچات روش جستجو[6] دنبال می‌شود. ادامه این فلوچارت در شکل ۱۹ آمده است. همانطور که مشاهده می‌کنید اولین سوال مربوط به این است که آیا عامل بازیابی از نوع بازبینی عمل اپراتور می‌باشد یا خیر؟



شکل ۲۰: فلوچارت تعیین نوع و احتمال عوامل بازیابی در روش THERP

1 Active Inspection
2 Passive Inspection
3 Compelling
4 Casual
5 Deviant Condition
6 Search Scheme

۱. پاسخ مثبت به سوال قبلی یعنی اینکه عامل بازیابی از نوع بازبینی عمل اپراتور می‌باشد. در این مسیر دو جدول ۲۰-۶ و ۲۰-۲۲ قرار دارند، که جدول ۲۰-۶ حاوی فهرست خطاهای اپراتور در اجرای یک دستورالعمل، و جدول ۲۰-۲۲ نیز حاوی فهرست خطاهای اپراتور در بازبینی عمل یک اپراتور دیگر می‌باشد.

۲. اما در صورت پاسخ منفی ابتدا باید تعیین شود که، آیا علائمی که اپراتور با مشاهده آنها تصمیم به بازیابی خواهد گرفت، به واسطه هشدارهای صوتی نمایشگر هستند، یا اینکه نمایشگرها دارای هشدار صوتی نیستند؟

۳. در صورت پاسخ مثبت به سوال، با توجه به نوع خطای اپراتور یکی از دو حالت زیر پیش خواهد آمد:

- در صورتی که خطا از نوع غفلت و فروگذاری در انجام یک وظیفه (Omission) باشد، مقدار احتمال آن از جدول ۲۰-۲۳ مرجع [۹]، انتخاب خواهد شد. در این جدول احتمال غفلت از انجام دادن یک وظیفه توسط اپراتور، در پاسخ به تعداد مختلفی از نمایشگرهای هشدار دهنده، داده شده است. اینکه اپراتور در پاسخ به هشدارها عمل اشتباهی را انجام دهد، در جدول دیگری بررسی شده است، و نباید با این جدول اشتباه گرفته شود.

- در صورتی که خطا از نوع اشتباه در انجام یک وظیفه (Commission) باشد، مقدار احتمال آن از جدول ۲۰-۲۴ مرجع [۹] انتخاب خواهد شد. این جدول حاوی مقادیر احتمال دو دسته از خطاها می‌باشد: خطا در یادآوری یک هشدار دائماً روشن[1]، پس از یک اخلال در توجه که به واسطه یک عامل دیگر ایجاد شده است، و خطا در توجه به یک هشدار دائماً روشن در حین بازرسی اولیه و بازرسی‌های بعدی اتاق کنترل.

۴. پاسخ منفی به سوال ۲ به این معنی است که علائمی که اپراتور با استفاده از آنها متوجه شرایط انحرافی می‌شود، از نوع نمایشگرهای بدون هشدار هستند. اگر نمایشگرهای به خصوصی بر اساس یک برنامه مشخص توسط اپراتور خوانده می‌شوند، یا به اپراتور دستور داده می‌شود که چند نمایشگر خاص را مشاهده نماید، خطا در انجام این کارها در واقع از نوع RBA می‌باشد و احتمال این خطاها باید با استفاده از فلوچارت شکل ۱۵ تعیین می‌شود. در غیر این صورت، یعنی اگر برای انجام بازرسی هیچ ملزومات به خصوصی وجود نداشته باشد و بازرسی نمایشگرها بخشی از یک بازرسی عمومی باشد، مسیر مربوط به پاسخ منفی دنبال خواهد شد.

[1] Steady-on Annunciator

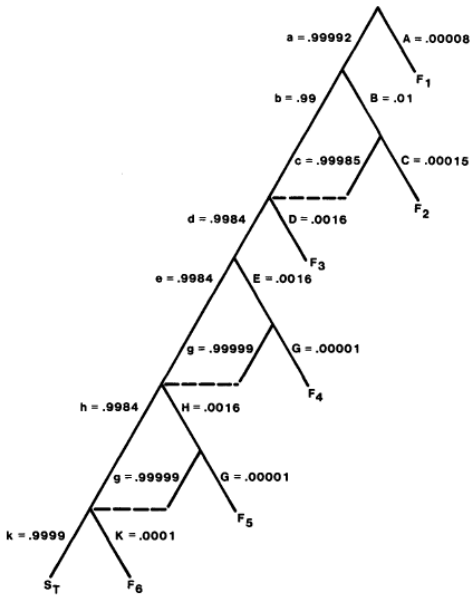
- در این مسیر اولین خطایی که ممکن است رخ دهد، اشتباه در اجرای دستورالعمل اجرایی توسط اپراتور مسئول بازرسی می‌باشد. مقادیر احتمال این نوع از خطای اپراتور در جدول ۲۰-۶ داده شده است.
- یکی از راه‌های جلب شدن توجه اپراتور به نمایشگرهای نشان دهنده شرایط انحرافی، که دارای هشدار صوتی نیز نیستند، در بازرسی اولیه اتاق کنترل یا بازرسی‌های بعدی است. مقادیر احتمال خطای مربوط به توجه اپراتور به این نمایشگرها در دو جدول ۲۰-۲۵ و ۲۰-۲۶ داده شده است. جدول ۲۰-۲۵ برای یک نمایشگر و جدول ۲۰-۲۶ برای تعداد بیشتر از همان نمایشگرها می‌باشد.
- راه دیگر پیدا کردن نمایشگرهای بدون هشدار از طریق بازدیدهای روزانه[1] معمولی می‌باشد. جدول ۲۰-۲۷ مقادیر احتمال خطای اپراتور در بازدیدهای روزانه را برحسب روزهای فاصله بین بازدیدها ارائه می‌دهد.

تا اینجا تمام انواع خطاهای بازیابی در روش THERP مورد بحث قرار گرفته است. همانطور که در شکل ۲۰ مشاهده می‌کنید، برای خطاهای بازیابی نیز باید عوامل PSF را بررسی کرد. به همین دلیل ادامه این فلوچارت نیز همانند خطاهای RBA به فلوچارت شکل ۱۸ برخواهد گشت و پس از تعیین عوامل PSF احتمال نهایی خطاهای بازیابی نیز تعیین می‌شود.

۹-۳ محاسبه احتمال خطای انسانی

پس از تعیین وابستگی‌های بین عملکردهای اپراتورها، در این مرحله کمی‌سازی و محاسبه احتمال خطای کل با استفاده از درخت رویداد خطای انسانی قابل انجام است. احتمال خطای انسانی در انجام یک وظیفه به سادگی از جمع احتمال کلیه مسیرهای منجر به خرابی محاسبه می‌شود. در بخش‌های پیشین نحوه ایجاد درخت رویداد خطای انسانی شرح داده شده است.

[1] Walk-around Inspection



شکل ۲۱: تحلیل درخت رویداد HRA

همانطور که در درخت رویداد شکل ۲۱ مشاهده می‌کنید هفده مسیر عدم موفقیت برای اپراتور وجود دارد. آنچه در اینجا ممکن است باعث ایجاد پیچیدگی شود، در نظر گرفتن مسیرهای مربوط به عملکردهای بازیابی می‌باشد. به عنوان مثال هر دو مسیر abD و aBcD در این درخت به F3 منتهی می‌شوند که یکی از حالت‌های خرابی سیستم است. بنابراین هر دوی آنها در محاسبه احتمال کل درخت رویداد در نظر گرفته می‌شوند. فهرست کامل این مسیرها در جدول شماره ۴ داده شده است.

جدول شماره ۴: مقادیر احتمال خطا در انجام دستورالعمل‌های اجرایی توسط اپراتور

Item	Path Name	Probability
1	A	8.0E-05
2	aBC	1.5E-06
3	aBcD	1.6E-05
4	abD	0.0015839
5	abdEG	1.0E-08
6	abdEgHG	1.0E-11
7	abdEghK	1.0E-07
8	abdEgHgK	1.0E-10
9	abdeHG	1.0E-08
10	abdeHgK	1.0E-07
11	abdehK	1.0E-04
12	aBcdEG	1.0E-10

13	aBcdEgHG	1.0E-13
14	aBcdEgHgK	1.0E-12
15	aBcdeHG	1.0E-10
16	aBcdeHgK	1.0E-09
17	aBcdehK	1.0E-06
18	Sum of Paths	0.00178

دقیق‌ترین برآورد از احتمال عدم موفقیت اپراتور در انجام وظیفه‌ای که در این درخت مدل‌سازی شده است، با استفاده از مجموع احتمال کلیه مسیرهای عدم موفقیت بدست می‌آید. عدد بدست آمده در این روش 0.00178 یا تقریباً 0.002 خواهد بود که مجموع اعداد ستون سوم جدول شماره ۳ می‌باشند. اما روش دقیق همیشه کارساز نبوده و در صورتی که وظیفه ایمنی مورد بحث شامل عناصر زیادی بوده و محاسبات نیز به صورت دستی انجام شود، پیدا کردن کلیه مسیرهای عدم موفقیت کار زمان‌بری خواهد بود.

یکی از روش‌های تقریبی، در نظر گرفتن مسیرهای اصلی عدم موفقیت، بدون رویدادهای موفقیت در هر مسیر می‌باشد. احتمال بدست آمده از این روش برای درخت رویداد شکل ۱۱ مطابق رابطه ۷-۴ خواهد بود. مقدار گرد شده در این روش و روش حل دقیق، برابر خواهد شد. این روش تقریبی در صورتی جواب خوبی خواهد داشت که احتمال وقوع عناصر یک رویداد، به اندازه کافی کوچک (مثلا کمتر از 0.01) باشد [۹].

$$F_T\,|\,(\text{HEPs} \le 0.01) = A + BC + D + EG + HG + K = 8.0E-05 + (0.01 \times 1.5E-04) + 0.0016$$
$$+ (0.0016 \times 1.0E-05) + (0.0016 \times 1.0E-05) + 1.0E-04 = 0.0018 \cong 0.002$$

(۴-۹)

همانگونه که در رابطه (۴-۹) نیز دیده می‌شود، احتمال‌های موفقیت، که با حروف کوچک انگلیسی نشان داده می‌شوند، در نظر گرفته نشده‌اند. همچنین از مسیرهای خرابی که شامل بیش از دو عنصر عدم موفقیت نیز باشند صرف‌نظر شده است. زیرا احتمال مربوط به این مسیرها تأثیر چندانی در عدد نهایی احتمال خرابی ندارد.

اما روش دیگری که بسیار ساده‌تر از دو روش قبل می‌باشد، استفاده از احتمال متمم برای پیدا کردن احتمال خطای کل می‌باشد. در این روش احتمال کل موفقیت در انجام وظیفه توسط اپراتور بطور دقیق محاسبه می‌شود. سپس با استفاده از آن احتمال خطای کل بدست می‌آید.

$$S_T = a(b+Bc)d(e+Eg)(h+Hg)k = 0.99992\times\left[0.99+\left(0.01\times 0.99985\right)\right]\times 0.9984$$
$$\times\left[0.9984+\left(0.0016\times 0.99999\right)\right]\times\left[0.9984+\left(0.0016\times 0.99999\right)\right]\times 0.9999 = 0.9982188 \cong 0.998 \quad (۵-۹)$$

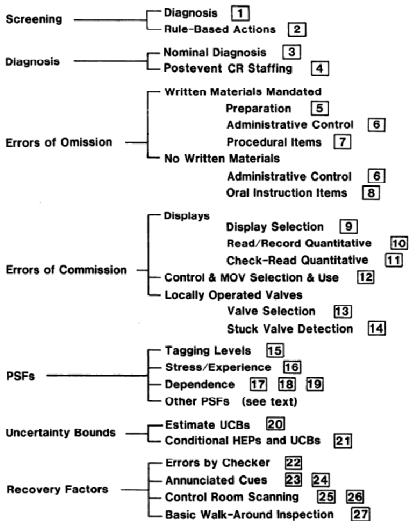
در نتیجه احتمال عدم موفقیت نیز از رابطه زیر بدست خواهد آمد.

$$S_T = 1.0 - 0.9982188 \cong 0.0018 \cong 0.002 \quad (۶-۹)$$

در کد توسعه داده شده در این پروژه از دو روش اول و سوم استفاده شده است. و پس از تحلیل درخت رویداد نتایج حاصل از هر دو روش نمایش داده می‌شود.

۹-۴ جداول مقادیر نامی احتمال خطای اپراتور

جداول حاوی مقادیر نامی مورد استفاده در تحلیل HRA با استفاده از روش THERP، مجموعاً ۲۷ عدد می‌باشند که در فصل بیستم مرجع [۹] آورده شده است. در کد توسعه داده شده نیز از همین مقادیر استفاده شده است، اما به دلیل حجم بالای آنها، در این گزارش فقط به این مدرک ارجاع داده شده است و از آوردن خود جداول خودداری شده است.



شکل ۲۲: فهرست جداول مقادیر نامی احتمال خطاهای انسانی در روش THERP

همانطور که در شکل ۲۲ نیز می‌بینید، می‌توان این جداول را به هفت گروه مجزا تقسیم نمود که عبارتند از:

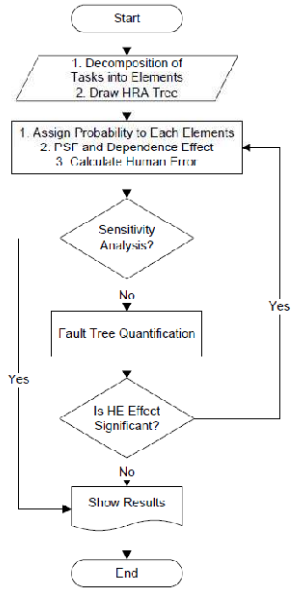
- گروه اول شامل جداول ۱ و ۲ حاوی مقادیر احتمال خطای اپراتور در حالت تحلیل غربالگری می‌باشد.
- گروه دوم شامل جداول ۳ و ۴ می‌باشد، که جدول ۳ حاوی مقادیر احتمال خطای اپراتور در تشخیص رویداد نامطلوب و جدول ۴ نیز تعداد و سطح وابستگی بین اپراتورها در اتاق کنترل در شرایط حادثه را نشان می‌دهد.
- گروه سوم شامل جداول ۵ تا ۸ حاوی مقادیر احتمال خطای اپراتور از نوع Omission می‌باشد.
- گروه چهارم شامل جداول ۹ تا ۱۴ حاوی مقادیر احتمال خطای اپراتور از نوع Commission می‌باشد.
- گروه پنجم شامل جداول ۱۵ تا ۱۹ حاوی مقادیر و روابط مربوط به PSFها می‌باشد.
- گروه ششم شامل جداول ۲۰ و ۲۱ حاوی مقادیر و روابط مربوط به عدم قطعیت در احتمال خطا می‌باشد.
- گروه هفتم شامل جداول ۲۲ تا ۲۷ حاوی مقادیر احتمال خطای اپراتور از نوع بازیابی می‌باشد..

۹-۵ پیاده‌سازی روابط و الگوریتم تحلیل خطای انسانی

این نرم‌افزار به عنوان یک ماژول به کد محاسباتی ReLab افزوده شده است، و به دو صورت می‌توان در چهارچوب تحلیل‌های کد ReLab از آن استفاده نمود. روش اول این است که برای تحلیل HRA، ابتدا باید یک رویداد پایه از نوع خطای انسانی در یک درخت خطا ایجاد شود. پس از اضافه‌شدن رویداد خطای انسانی به درخت خطا یک تحلیل HRA در پایگاه داده پروژه ایجاد می‌شود. از طریق این تحلیل HRA، کاربر می‌تواند وظیفه 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. اما روش دوم نیز به این شکل است که مستقل از تحلیل درخت خطا، یک تحلیل HRA 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.

همانطور که پیشتر نیز اشاره شد، تحلیل خطای انسانی معمولاً به عنوان بخشی از یک تحلیل کلی ایمنی مانند تحلیل PSA یک نیروگاه هسته‌ای انجام می‌شود. بنابراین اگرچه می‌توان در کد ReLab یک خطای انسانی را مستقلاً و نه به عنوان بخشی از یک درخت خطا تحلیل نمود، اما 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. همانگونه

که در شکل ۲۳ نیز مشاهده می‌کنید، تحلیل حساسیت برای خطای انسانی در صورتی قابل انجام است که به عنوان بخشی از تحلیل درخت خطا باشد.



شکل ۲۳: فلوچارت تحلیل HRA در کد محاسباتی ReLab

۹-۶ نتیجه‌گیری محاسبه‌ی خطای انسانی

به دلیل اهمیت زیاد خطاهای انسانی و نقش آن در وقوع یا پیشروی حوادث، در آخرین نسخه کدهای شناخته شده PSA مانند SAPHIRE و Risk Spectrum، قابلیت تحلیل خطای انسانی نیز به آنها افزوده شده است. ماژول تحلیل خطای انسانی در کد Risk Spectrum از روش‌های مختلفی مانند THERP، HEART و SPAR-H استفاده می‌کند. آخرین نسخه کد SAPHIRE نیز برای تحلیل خطای انسانی از روش SPAR-H استفاده می‌کند. در این پروژه به عنوان قدم اول در توسعه ماژول تحلیل خطای انسانی در کد ReLab، روش THERP به عنوان روش اصلی در نظر گرفته شده است. در مراحل بعد سایر روش‌های شناخته شده نیز به این ماژول افزوده خواهند شد. در نهایت به دلیل نداشتن دسترسی به آخرین نسخه کدهای SAPHIRE و Risk Spectrum، نتایج حاصل از کد ReLab به منظور اعتباربخشی با نتایج مثال‌های تحلیل HRA در مرجع [۹] مقایسه شده است، که این مقایسه حاکی از تطابق کامل نتایج می‌باشد.

۱۰- نتیجه‌گیری

کد ReLab 1.3 دارای چهار ماژول اصلی محاسباتی است. این چهار ماژول عبارتند از تحلیل درخت رویداد، تحلیل درخت خطا، دیاگرام تصمیم‌گیری دودویی و تحلیل خطای انسانی. از این چهار ماژول دیاگرام تصمیم‌گیری دودویی به عنوان یک ابزار جهت تسریع الگوریتم تعیین مجموعه‌های برشی استفاده می‌شود. این ابزار به عنوان یک هسته محاسباتی در ماژول‌های تحلیل درخت خطا، رویداد و خطای انسانی استفاده می‌شود. در پایان تحلیل خطای انسانی از مهمترین ابزارهای مورد استفاده در کدهای محاسباتی ایمنی احتمالاتی است که در آن به تفصیل به تحلیل این خطای مهم می‌پردازد و در این بسته نرم‌افزاری مورد استفاده قرار می‌گیرد. این ماژول‌ها با کدهای SAPHIRE و Risk Spectrum راستی آزمایی شده‌اند و پس از اینکه به نتایج صحیحی دست یافتند به این بسته نرم‌افزاری اضافه‌گردیدند.

۱۱- مراجع

1. Vesely, W. E., N. Roberts, “Fault tree handbook”, Nuclear Regulatory Commission, 1987.
2. Epstein, S., A. Rauzy, “Can we trust PRA?” Reliability Engineering & System Safety 88(3):195-205, 2005.
3. Rauzy A.,”New Algorithm for fault trees analysis”, Reliability engineering and safety system, vol. 40, pp. 203-213, 1993.
4. Modarres M., “Risk Analysis in Engineering, Techniques, Tools, and Trends”, Taylor and Francis Group, 2006.
5. Limnios N., “fault trees”, ISTE, 2007.
6. Modarres M.,”Risk Analysis in Engineering”, CRC Press,1, pp.60-63, 2006.
7. Lee j., McCormick N.,” Risk and Safety Analysis of nuclear system”, WILEY, pp.187-193, 2011.
8. Bedford T., Cooke R., “Probabilistic Risk Analysis: Foundations and Methods”, Cambridge University Press, 6th Edition, pp. 123-134, 2009.
9. Swain, A.D., Guttmann, H.E., “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications”, Nuclear Regulatory Commission, 1983.
10. Gertman, D., Blackman, H., Marble, J., Byers, and Smith, C. (2004a). “The SPAR-H human reliability analysis method”, NUREG/CR-6883. Idaho National Laboratory, prepared for U. S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research Washington, DC 205555-0001.
11. Kirwan, B., “The validation of three Human Reliability Quantification techniques - THERP, HEART and JHEDI: Part 1 - technique descriptions and validation issues”, Applied Ergonomics, Vol. 27, No. 6, pp. 359-373, 1996.
12. Ibanez-Llano, C., et al. “Hybrid approach for the assessment of PSA models by means of binary decision diagrams”, Reliability Engineering & System Safety 95(10): 1076-1092, 2010.
13. Smith, C., “System Analysis Program for Hands-on Integrated Reliability Evaluations-Technical Reference”, 2008, Idaho National Laboratory (INL).