هفتمین کنفرانس بین‌المللی
مهندسی قابلیت اطمینان و ایمنی

معرفی اولین نرم‌افزار ایرانی تحلیل ایمنی احتمالاتی، مطالعه‌ی موردی: تحلیل ایمنی احتمالاتی درخت خطای زیرمجموعه سیستم خنک‌کننده اضطراری قلب

پوریا قناعتیان جبذری[۱]، پوریا یوسفی[۱]، سروش صابریان[۱]، محمدمهدی خلیفه‌شوشتری[۱]

۱- مرکز محاسبات پیشرفته شرکت مسنا، تهران، ایران، pooria.gh94@gmail.com

چکیده

با گسترش علوم و کسب تجربیات مختلف در زمینه‌های طراحی، ساخت، بهره‌برداری و نگهداری، دیدگاه غیرقابل کنترل بودن خطاهای احتمالی نقض گردید و این باور شکل گرفت که می‌توان با استفاده از تجربیات مختلف و کمک گرفتن از روابط ریاضی، سیستم‌های مختلف را مدل‌سازی کرد و احتمال خرابی آنها را تخمین خرابی سیستم‌ها، استفاده از روش تحلیل ایمنی احتمالاتی (PSA[1]) بوده است. در این روش، از دو ابزار اصلی درخت خطا و درخت رویداد استفاده می‌شود. شرکت‌ها و موسسات تحقیقاتی مختلف نیز نرم‌افزارهای متعددی برای پیاده‌سازی PSA با استفاده از ابزارهای درخت خطا و درخت رویداد، ارائه کرده‌اند که از مهم‌ترین آن‌ها می‌توان به RiskSpectrum، SAPHIRE، RISKMAN و... اشاره کرد. با توجه به لزوم استفاده از PSA به عنوان یک ابزار کلیدی در راستای ارتقای سطح ایمنی و قابلیت اطمینان صنایع مختلف، و هم‌چنین دسترسی دشوار به نرم‌افزارهای خارجی موجود که مستلزم پرداخت هزینه‌ی زیاد است، مرکز محاسبات پیشرفته از حدود یک دهه قبل اقدام به نیازسنجی و توسعه‌ی نرم‌افزار IRES[2] برای پیاده‌سازی PSA کرده است. در حال حاضر آخرین نسخه‌ی این نرم‌افزار تحت عنوان IRES2.1 دردسترس است. در این پژوهش به بررسی توانمندی‌های مختلف نرم‌افزار IRES2.1 و مقایسه با نمونه‌ی خارجی آن پرداخته شده است.

واژه‌های کلیدی: تحلیل ایمنی احتمالاتی، درخت خطا، درخت رویداد، خطای انسانی، PSA، IRES، SAPHIRE، RiskSpectrum.

مقدمه

ایمنی به مجموعه‌ای از اقدامات نرم‌افزاری و سخت‌افزاری گفته می‌شود که به واسطه‌ی آن تلاش می‌شود ضمنِ استفاده حداکثری از ظرفیت یک سیستم یا مجموعه، سلامت انسان و محیط زیست نیز با چالش‌های بسیار کمی مواجه شود به طوری که با شناسایی تمامی عوامل بالقوه‌ی ایجاد خطا و خرابی، آن‌ها را رفع یا کنترل کرد. به طور کلی، ایمنی با دو رویکرد کلی یقینی و احتمالاتی مورد تحلیل قرار می‌گیرد که این دو رویکرد مکمل یکدیگر بوده و هر یک هدف مشخص و متمایزی دارند. تحلیل ایمنی با دیدگاه احتمالاتی، یک روش جامع، اصولی و با قاعده است که نسبت به سایر روش‌ها، استفاده از این روش به طور چشم‌گیری گسترش یافته است. PSA می‌تواند با فراهم آوردن نتایج کمی و برآوردهای کیفی، در اتخاذ صحیح‌ترین تصمیمات از نظر ایمنی، با توجه به شرایط موجود در طراحی سیستم و بهره‌برداری، کمک کند [۱]. در صنایع با تکنولوژی بالا[3]نظیر صنعت هسته‌ای، هوافضا، نفت، گاز، پتروشیمی و ... از تحلیل ایمنی احتمالاتی به طور عمده به عنوان یک ابزار در مطالعات بهینه‌سازی، طراحی، ارزیابی و افزایش ایمنی استفاده می‌شود. اصلی‌ترین ابزارهای PSA، درخت خطا[4] و درخت رویداد[5]هستند. تحلیل درخت خطا که هدف اصلی آن محاسبه‌ی احتمال

[1] Probabilistic Safety Assessment
[2] Integrated Reliability and Safety Assessment
[3] High Technology
[4] Fault Tree
[5] Event Tree

خرابی عملکرد سیستم‌های مختلف است از قابلیت‌های زیادی نظیر تحلیل عدم قطعیت، تحلیل خطای انسانی و تحلیل حساسیت برخوردار است. تحلیل درخت رویداد شامل تحلیل کمی و کیفی سناریوهای حوادث در شرایط کاری مختلف است. نرم‌افزارهای مطرحی همچون RiskSpectrum و SAPHIRE به منظور توسعه‌ی درخت خطا و درخت رویداد در تحلیل ایمنی احتمالاتی به‌کار گرفته می‌شوند. معادل ایرانی این نرم‌افزارها با نام IRES توسعه داده شده است که از قابلیت-های خوبی برخوردار می‌باشد. در این مقاله ضمن معرفی نرم‌افزارهای ذکر شده، با توسعه‌ی یک نمونه‌ی مطالعاتی در هر سه نرم‌افزار، قابلیت-های مختلفی همچون محاسبه‌ی احتمال خرابی سیستم‌ها، محاسبه‌ی فرکانس وقوع سناریوهای حوادث، تحلیل اهمیت[1] تحلیل حساسیت[2] و تحلیل عدم قطعیت[3] مورد بررسی قرار خواهد گرفت.

روش PSA و مهم‌ترین ابزارهای آن

PSA یک ارزیابی سیستماتیک است از ترکیب پدیده‌های مختلف که ممکن است به ایجاد حالتی ناخواسته منجر شوند و پیامدهای زیست محیطی، تلفات انسانی و خسارت‌های کلان اقتصادی را نیز به دنبال داشته باشند، تشکیل شده است. به عنوان مثال، PSA در یک نیروگاه هسته‌ای به دنبال ارزیابی احتمالاتی مجموعه عواملی است که موجب آسیب به قلب راکتور و پخش مواد رادیواکتیو از نیروگاه اتمی می‌شود [۱].

شاکله‌ی اصلی PSA به این صورت است که ابتدا یک رویداد آغازگر[4] شروع کننده‌ی ارزیابی است و در ادامه با در نظر گرفتن خطای انسانی و احتمال در دسترس نبودن سیستم‌ها، ارزیابی مورد نظر تکمیل می‌گردد [۲].

PSA، چگونگی ارتباط بین انسان، نرم‌افزار و اجزای سخت افزاری را مدل‌سازی می‌نمایند. هم‌چنین مهم‌ترین عوامل ایجاد ریسک در سیستم را مشخص و مقدار ریسک را تعیین می‌کند. PSA شامل تخمین مقدار احتمال خسارت است. یک تعریف رسمی که توسط کاپلان و گریک[5] ارائه شده است، توصیفی ساده و مفید از اجزا ارزیابی ریسک فراهم می‌سازد که شامل سه پرسش اساسی زیر است:

۱-چه چیزی می‌تواند بد کار کند تا در معرض مخاطره قرار گیرد ؟

۲-مقدار احتمال وقوع آن چقدر است؟

۳- پیامدهای مورد انتظار این رویداد چیست؟

فرآیند PSA شامل کاربرد کمّی سه سوال ذکر شده است که در آن احتمالات (یا فرکانس‌های) مربوط به سناریوهای رویدادهای منجر به قرارگیری در معرض مخاطره تخمین زده می‌شود و مقادیر متناظر پیامدهای مربوط به سلامت، ایمنی، محیط و اقتصاد، برای هر سناریو پیش‌بینی می‌گردد. مقدار ریسک (مثلا خسارت مورد انتظار) هر سناریو اغلب به صورت ضرب فرکانس سناریو در پیامد آن حاصل می‌شود. مهم‌ترین نتیجه‌ی PSA مقدار واقعی ریسک محاسبه شده نیست (اصطلاحاً عدد خط پایان)، بلکه شناسایی اجزایی از سیستم که در واقع عوامل بوجود آورنده‌ی ریسک می‌باشند، عدم قطعیت‌های وابسته به چنین تخمین‌ها و میزان اثربخشی استراتژی‌های مختلف کاهش ریسک است. بدین معنا که مقدار اولیه‌ی PSA برای مشخص کردن طراحی سیستم و عیب‌های کاربردی و برای بهینه‌سازی منابعی است که می‌توانند برای بهبود طراحی و عملکرد سیستم سرمایه گذاری شوند [۳].

مهم‌ترین نقاط قوت PSA به عنوان یک رویکرد رسمی مهندسی برای ارزیابی ریسک به صورت زیر است. PSA می‌تواند:

۱- آزمایشی جامع و سیستماتیک روی دسته وسیعی از ویژگی‌های طراحی و کارکردی یک سیستم مهندسی را مهیا سازد.

۲- اثر برهم‌کنش‌های سیستمی و ارتباطات انسان با سیستم را وارد نماید.

۳- مدلی را برای وارد کردن آزمون عملکردی سیستم مهندسی و به‌روز کردن تخمین‌های ریسک فراهم سازد.

۴- فرآیندی را برای بررسی جداگانه‌ی عدم قطعیت‌ها فراهم سازد.

۵- اجازه دهد به تحلیل ریسک‌هایی که باهم در رقابتند بپردازیم.

۶- این امکان را فراهم کند که به تحلیل موضوعات (فرضیات یا داده‌ها) بوسیله‌ی مطالعه‌ی حساسیت بپردازیم.

۷- مقیاسی از اهمیت مطلق یا نسبی سیستم‌ها و اجزاء در مقدار ریسک محاسبه شده به‌دست دهد.

۸- میزان کمی از حد کلی سلامت و ایمنی سیستم مهندسی به دست دهد.

خطاهای عمده ممکن است از ضعف یا نبود مدل‌ها یا داده‌های وابسته به عوامل بالقوه مهم در ریسک سیستم شامل مواردی که در زیر آمده حاصل شوند:

۱-رخدادهای آغازین خیلی به ندرت اتفاق بیفتند.

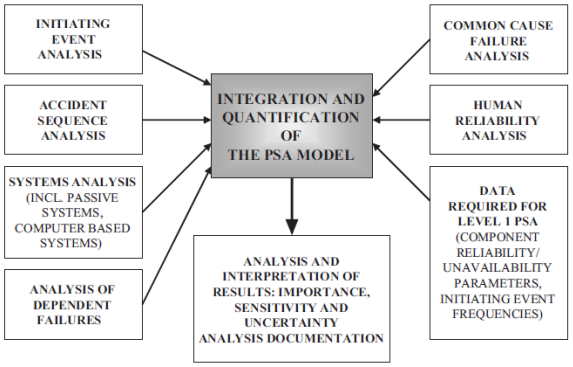
۲-مدل‌های عملکرد انسانی و ارتباط انسان با سیستم بسیار غیر قابل اطمینان باشند.

۳-شکست‌های ناشی از رویدادهای علت مشترک مانند یک محیط عملکردی حاد، به سختی قابل شناسایی و مدل‌سازی باشند [۴].

در شکل ۱، چارچوب کلی PSA سطح ۱ نشان داده شده است. در ادامه برخی از مفاهیم مهم و پرکاربرد که به نوعی ابزارهای مورد نیاز در توسعه‌ی PSA به حساب می‌آیند، معرفی شده است.

[1] Importance Analysis
[2] Sensitivity Analysis
[3] Uncertainty Analysis

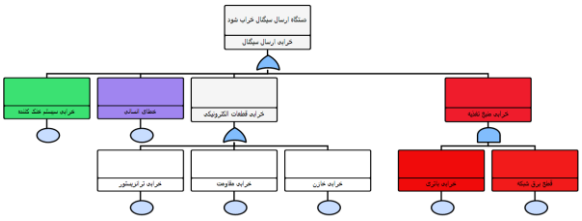
[4] Initial Event
[5] Kaplan and Garrick



شکل ۱: چارچوب کلی PSA [۵]

درخت خطا

روش درخت خطا یک فرآیند استنتاجی است که بوسیله‌ی آن یک رخداد نامطلوب که رویداد رأس نامیده می‌شود، در نظر گرفته می‌شود و راه‌های ممکن برای اتفاق افتادن این رویداد به صورت سیستمی استنتاج می‌شود [۶]. برای مثال، همانند آنچه در شکل ۲ نشان داده شده است، یک رویداد رأس متداول می‌تواند به این شکل باشد، "عیب مدار کنترل A در ارسال سیگنال زمانی که باید ارسال کند." فرآیند استنتاج به گونه‌ای انجام می‌شود که درخت عیب در برگیرنده تمامی خرابی‌های اجزاء (یعنی مودهای خرابی) که سهمی در وقوع رویداد رأس دارند، باشد. همچنین می‌توان تک تک مودهای خرابی هر قطعه و نیز خطاهای انسانی و نرم‌افزاری (و تداخل بین این دو) در طول مدت زمان عملکرد سیستم را وارد مسئله کرد. نمایش درخت خطا یک بیان گرافیکی از ترکیب‌های مختلفی از خرابی است که می‌تواند منجر به وقوع رخداد رأس گردند.



شکل ۲: نمونه‌ای از یک درخت خطا که با استفاده از نرم‌افزار IRES2.1 توسعه داده شده است.

مدل‌های قابلیت اطمینان

ورودی‌های کمّی در درخت‌های خطا، رویدادهای پایه نام دارند. رویدادهای پایه در واقع مدل‌سازی ریاضی یک قطعه به منظور یافتن احتمال خرابی (عدم دسترسی) آن است. در جدول ۱ تعدادی از مهم‌ترین مدل‌های قابلیت اطمینان که بیشتر مورد استفاده قرار می‌گیرد، لیست گردیده است.

جدول ۱: مدل‌های قابلیت اطمینان [۷]

نام مدل	رابطه‌ی ریاضی
عدم دسترسی ثابت[1]	$Q(t) = q$
جزء قابل تعمیر[2]	$Q(t) = (\frac{\lambda}{\lambda+\mu})*(1-e^{-(\lambda+\mu)t})$
جزء تست شونده[3]	$Q(t) = 1+ \frac{(\exp(\lambda T)-1)}{\lambda T}$
جزء با زمان ماموریت ثابت[4]	$Q(t) = 1- \exp(-\lambda t_m)$
جزء غیر قابل تعمیر[5]	$Q(t) = 1-e^{-\lambda t}$

لازم به ذکر است که پارامترهای بکار رفته در جدول فوق، شامل q، μ، λ، t، T، t_m هستند که به ترتیب احتمال خرابی، نرخ خرابی، نرخ تعمیر، زمان، زمان تست و زمان مأموریت می‌باشند.

گیت‌های منطقی

در بخش معرفی درخت خطا گفته شد که یک سیستم می‌تواند دارای عوامل خرابی بالقوه متعددی باشد، برای ایجاد ارتباط بین این عوامل در ساختار درخت خطا، از گیت‌های منطقی استفاده می‌شود، به طور کلی ۳ نوع گیت منطقی اصلی که شامل AND، OR و NOT می‌باشند، تعریف شده است و مابقیِ گیت‌ها از ترکیبات این ۳ گیت اصلی بوجود خواهند آمد.

خرابی‌های منشأ مشترک

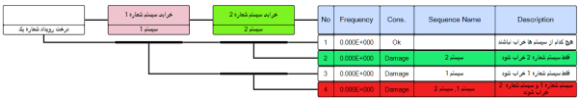
خرابی با منشأ مشترک یا همان CCF[6]، به دسته‌ای از خرابی‌ها گفته می‌شود که در آن چندین جزء (بیش از ۲) در زمانی یکسان و با علتی یکسان خراب می‌گردند، به این نوع از خطاها، خطاهای وابسته نیز گفته می‌شود. CCF، سهم زیادی در ایجاد خرابی و عدم دسترسی سیستم دارند، بنابراین مدل‌سازی، کمّی‌سازی و انجام محاسبات CCF نقش بسیار مهمی را در مطالعات قابلیت اطمینان و PSA ایفا می‌کنند. با توجه به نکات ذکر شده، می‌توان انتظار داشت که میزان توانمندی نرم‌افزارهای مربوطه در مدل‌سازی صحیح و دقیق CCF، می‌تواند یکی از شاخصه‌های برتری آن نرم‌افزار باشد.

درخت رویداد

درخت رویداد دارای یک ساختار گرافیکی افقی است که از سمت چپ شروع می‌شود. اولین متغیر آن رویداد آغازگر است و پس از آن سایر سیستم‌ها با همان ترتیب زمانی که در سناریوی حادثه ایفای نقش می‌کنند، به ساختار درخت رویداد اضافه خواهند شد. شکل ۳ یک درخت

[1] Constant Probability
[2] Repairable
[3] Periodically Tested
[4] Mission Time
[5] Non Repairable
[6] Common Cause Failures

رویداد نوعی است که با یک رویداد آغازگر (IE) شروع شده و در ادامه سیستم‌های ۱ و ۲ به تحلیل احتمالاتی وارد شده‌اند. به دنبال هر رویداد آغازگر، سناریوهای حوادث مختلفی شروع می‌گردند، که در نهایت با جمع شدن تمامی حالت‌ها و فرکانس‌ها، فرکانس نهایی محاسبه می‌گردد.



شکل ۳: نمونه‌ای از یک درخت رویداد در نرم افزار IRES2.1

خطای انسانی

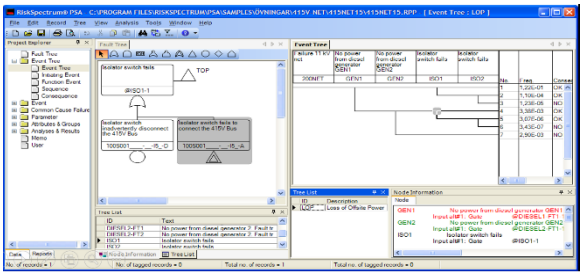
تجزیه و تحلیل قابلیت اطمینان انسانی (HRA)، یک ساختار نظام‌مند است که می‌توان از آن برای شناسایی رخدادهای بالقوه خطای انسانی و سیستماتیک کردن فرآیند تخمین خطای انسانی استفاده کرد. به عبارت دیگر، در تجزیه و تحلیل قابلیت اطمینان انسانی، با شناسایی و کمّی‌سازی فاکتورهای مختلف که می‌توانند در به وجود آمدن خطای انسانی نقش داشته باشند، میزان احتمال خطای انسانی تخمین زده می‌شود. برای تجزیه و تحلیل قابلیت اطمینان انسان، روش‌های مختلفی از جمله THERP، ASEP، CBDT، SLIM، FILM، SPAR-H و ... ارائه شده است [۸].

نرم‌افزارهای موجود برای پیاده‌سازی PSA

در طول سال‌های اخیر برنامه‌های پیچیده و کدهای کامپوتری محاسبات درخت خطای مستقل یا تحلیل‌های ترکیبی ایمنی احتمالاتی برای سیستم‌های پیچیده‌ی مهندسی هم‌چون نیروگاه‌های هسته‌ای و صنایع هوافضا توسعه یافته است. معتبرترین کدهای تحلیل ایمنی احتمالاتی عبارتند از: CAFTA[۲] Code، RISKMAN Code، Relex Software، PARAGON Software، Reliability Workbench Software، SAPHIRE، RISKSPECTRUM و IRES. در بین این کدها، SAPHIRE و RiskSpectrum دارای گسترده‌ترین استفاده برای پیاده‌سازی PSA هستند، لذا در این مقاله به بررسی این دو نرم‌افزار و معرفی نسخه‌ی ایرانی نرم‌افزار PSA پرداخته خواهد شد.

نرم‌افزار RiskSpectrum

این نرم‌افزار بدلیل سابقه‌ی طولانی که در انجام محاسبات ریسک و قابلیت اطمینان سیستم‌های پیچیده‌ی مهندسی دارد، به معتبرترین نرم‌افزار تجاری تحلیل ریسک تبدیل شده است که برای دسترسی به آن نیاز به هزینه‌ی زیادی است، لذا امکان استفاده از آن برای بسیاری از افراد فراهم نمی‌باشد. مجموعه‌ی توسعه دهنده‌ی این کد سال‌های زیادیست که آغاز به فعالیت کرده‌اند و امروزه یکی از ارائه‌دهندگان پیشرو در زمینه‌ی خدمات حرفه‌ای مهندسی، فناوری بهبود ایمنی و افزایش عملکرد زیرساخت‌های حساس برای مشتریان در بیش از ۷۵ کشور جهان هستند. در شکل ۴ محیط کاری کد RiskSpectrum نشان داده شده است.



شکل ۴: محیط کاری نرم‌افزار RiskSpectrum نسخه ۱

نرم‌افزار SAPHIRE

نرم‌افزار SAPHIRE نخستین بار در سال ۱۹۸۷ برای مرکز تحقیقات تنظیم مقررات هسته‌ای در کمیسیون تنظیم مقررات هسته‌ای ایالات متحدهٔ توسط آزمایشگاه ملی آیداهؤ ارائه شد و تا به امروز نسخه‌ی هشتم آن نیز توسعه یافته است. کمیسیون تنظیم مقررات هسته‌ای ایالات متحده یک سازمان مستقل است که توسط کنگره ایالات متحده تأسیس شده است تا از حفاظت کافی سلامت عمومی و ایمنی، پدافند عام و محیط پیرامون در برابر استفاده از مواد هسته‌ای اطمینان حاصل کند. نرم‌افزار SAPHIRE برای ایجاد و تجزیه و تحلیل ارزیابی احتمالاتی ریسک[۵] و البته در درجه‌ی اول برای نیروگاه‌های هسته‌ای توسعه یافته است[۹]. در شکل ۵ محیط کاری کد SAPHIRE نشان داده شده است.

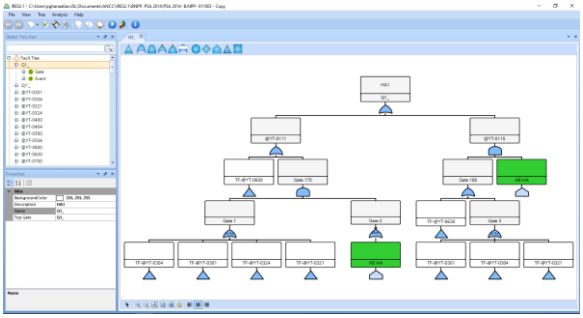
شکل ۵: محیط کاری نرم‌افزار SAPHIRE نسخه ۷

[1] Human Reliability Analysis
[2] Computer Assisted Fault Tree Analysis
[3] Nuclear Regulatory Commission (NRC)
[4] Idaho National Lab (INL)
[5] Probabilistic Risk Assessments (PRA)

نرم‌افزار IRES2.1

IRES2.1 که به عنوان اولین نرم‌افزار ایرانی در زمینه محاسبات ایمنی احتمالاتی توسعه داده شده است، یک نرم‌افزار یکپارچهٔ محاسبات PSA است که در سیر تکامل خود پس از انتشار نسخه‌های RELAB-FTA، RELAB-ETA، RELAB1.3، IRES1.0، IRES2.0 و رفع نواقص آنها، جهت دست‌یابی به یک نسخهٔ پایهٔ تجاری ارائه شده است. در این نرم‌افزار نیز با کمک ابزارهایی مانند درخت خطا و درخت رویداد و مفاهیمی همچون خطای انسانی، خرابی عامل مشترک، تحلیل اهمیت، حساسیت و عدم قطعیت به ارزیابی ریسک در یک مجموعهٔ صنعتی، یا فرایند تولید، یا هر مقوله‌ای که با مخاطرات و پیامدهای آنها مواجه است، به صورت احتمالاتی به ارزیابی مخاطرات و تحلیل پیامدهای آنها می‌پردازد. یکی از کاربردهای بسیار مهم و حساس که همواره نیازمند PSA است، تأسیسات هسته‌ای و به ویژه نیروگاه‌های هسته‌ای می‌باشند. این تأسیسات بدلیل سروکار داشتن با مواد پرتوزای مخاطره‌آمیز برای انسان، جامعه و محیط زیست و امکان انتشار آن در اثر حوادث طبیعی و غیرطبیعی، یکی از مهم‌ترین کاربردهای تحلیل ایمنی احتمالاتی هستند. علاوه براین، وقوع حوادث واقعی و ایجاد آسیب‌های خسارت‌باری نظیر حوادث نیروگاه‌های چرنوبیل و فوکوشیما، لزوم توجه به مبحث ایمنی هسته‌ای و به تبع آن ایمنی احتمالاتی، بیش از پیش شده است. بدین منظور نرم‌افزار IRES2.1 به عنوان اولین نسخهٔ دارای قابلیت‌های مختلف جهت ارزیابی حوادث در نیروگاه‌های هسته‌ای و یا هر سیستم صنعتی دیگر، توسعه داده شده است. در این نسخه از نرم‌افزار، با تغییر ساختار برنامه‌نویسی پیشین، اصلاح گیت‌های NAND، NOR، XOR و N/M، اصلاح قابلیت گیت انتقال، اصلاح نحوهٔ مدل‌سازی و نمایش خرابی عامل مشترک (CCF)، نسخهٔ پایهٔ تجاری بدست آمده است، در شکل ۶ محیط کاری نرم‌افزار IRES2.1 نشان داده شده است. در جدول ۲ لیست کاملی از توانمندی‌های محاسباتی نرم‌افزار IRES2.1 نشان داده شده است. هم‌چنین در طراحی پوسته گرافیکی[1]نیز تلاش‌های گسترده‌ای صورت گرفته است تا بتوان میزان کاربر پسند بودن[2]نرم‌افزار را افزایش داد، در همین راستا از امکاناتی مانند توسعه‌ی تعداد زیادی کلیدهای میانبر که می‌توانند روند مدل‌سازی را تسهیل کنند، استفاده شده است [۱۰].

نظر به اینکه موضوع این پژوهش، بررسی نرم‌افزار IRES2.1 است، لذا در ادامه توضیحات بیشتری در مورد این نرم‌افزار و قابلیت‌های آن ارائه شده است. لازم به ذکر است که بررسی و ذکر تمامی جنبه‌های نرم‌افزار IRES2.1 در این مقاله امکان پذیر نیست، لذا پیشنهاد می‌گردد که برای بررسی بیشتر و کامل‌تر به مدارک فنی نرم‌افزار که از طریق سایت مرکز محاسبات پیشرفته[3]قابل دسترسی است، مراجعه شود.



شکل ۶: محیط کاری نرم‌افزار IRES نسخه 2.1

جدول ۲: قابلیت‌های محاسباتی نرم‌افزار IRES2.1

نوع ماژول	ویژگی محاسباتی	
درخت خطا	مدل‌های متنوع قابلیت اطمینان	مدل قابل تعمیر مدل تست دوره‌ای مدل احتمال ثابت مدل ماموریت ثابت مدل فرکانس ثابت مدل غیر قابل تعمیر
	گیت‌های منطقی	گیت AND گیت OR گیت *NAND گیت *NOR گیت N/M گیت XOR
	مدل‌سازی CCF	روش بتا روش MGL روش آلفا (بدون محدودیت تعداد زیر مجموعه)
	آنالیز اهمیت	معیار RID معیار RRD معیار BI معیار RIR معیار RRR معیار F-V
	آنالیز حساسیت	
	آنالیز عدم قطعیت	تابع توزیع Normal، Beta، Gamma، Lognormal، Uniform، Loguniform
درخت رویداد	قابلیت انجام محاسبه بر اساس توالی یا پیامد	
قابلیت اطمینان انسانی	دارای روش THERP و امکان تشکیل درخت تصمیم‌گیری دودویی	
* گیت‌های NAND و NOR دارای دو منطق محاسباتی Logical و DeMorgan می‌باشند.		

پیاده‌سازی نمونه‌ی مطالعاتی

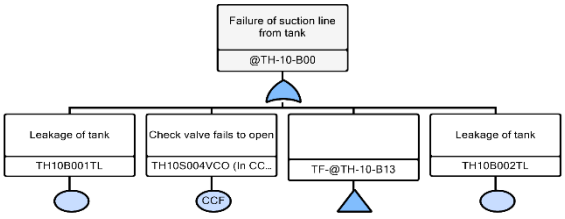
ملاک انتخاب نمونه مسئله‌ی عملیاتی، دو نکته‌ی مهم بوده است؛ اول اینکه نمونه مطالعاتی از مدارک معتبری باشد و دوم اینکه مسئله به

[1] Graphic User Interface
[2] User Friendly
[3] Www. ancc.ir

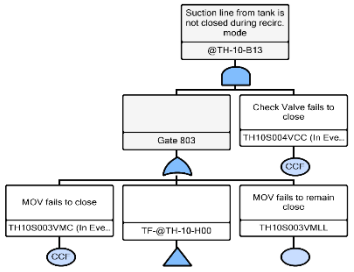
گونه‌ای باشد که طیف گسترده‌ای از امکانات مهم نرم‌افزار از جمله گیت‌های منطقی مختلف، گیت انتقال، مدل‌سازی CCF و ... به چالش کشیده شود. بنابراین از مدارک PSA نیروگاه اتمی نوع VVER-1000، درخت‌های خطای "خط مکش از سمت مخزن" که زیر مجموعه‌ی سیستم خنک‌کننده اضطراری قلب[2]است، انتخاب شده است. هم‌چنین در ادامه برای تکمیل نمونه‌ی مطالعاتی و تست عملکرد درخت رویداد (نحوه‌ی لینک شدن با درخت خطا و انجام محاسبات)، با استفاده از رویداد آغازگر فرضی IE1 که فرکانس وقوع آن (1/year) 1E-3 می‌باشد، یک درخت رویداد (Event Tree1) توسعه داده شده است.

مدل‌سازی درخت خطا و درخت رویداد با استفاده از نرم‌افزار IRES2.1

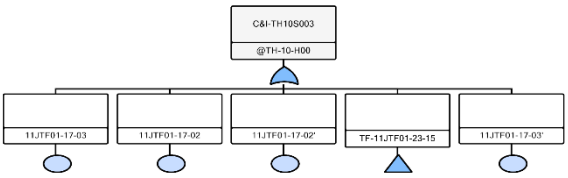
در خت های خ طای نمو نه با اســتفاده از نرم‌افزار IRES2.1 پیاده‌سازی شده که تصاویر آن در شکل‌های زیر نشان داده شده است. همانطور که از تصــاویر قابل مشــاهده اســت، هر یک از درخت‌های خطای ذکر شــده دارای تعدادی زیرمجموعه هســتند که با اســتفاده از گیت انتقال به درخت خطای اصلی متصل شده‌اند. هم‌چنین در ساختار آن‌ها از خرابی‌های منشأ مشترک (CCF) که از مهم‌ترین رویدادهای پایه هستند نیز استفاده شده است. در این نمونه، درخت‌های خطای اصــلی، خطوط مکش ۱۰، ۲۰، ۳۰ و۴۰ هســتند و زیر مجموعه‌های آن‌ها با عبارت‌های A10، B10 و ... نام‌گذاری شــده‌اند. هم‌چنین در توســعه درخت رویدادِ نمونه از درخت‌های خطای A10، C20، B30 و C40 استفاده شده است.



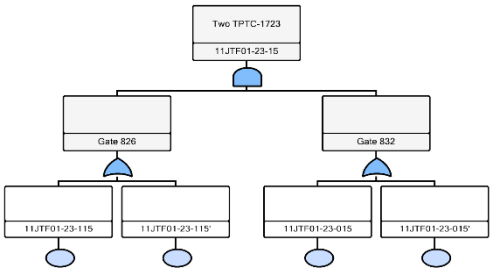
شکل ۷: پیاده‌سازی درخت خطای خط مکش شماره ۱۰ با استفاده از نرم‌افزار IRES2.1



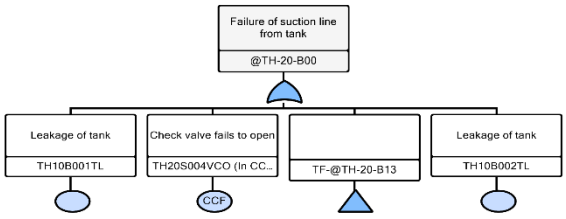
شکل ۸: پیاده‌سازی درخت خطای A10 با استفاده از نرم‌افزار IRES2.1



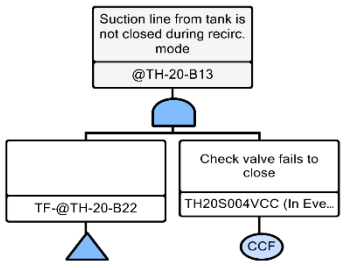
شکل ۹: پیاده‌سازی درخت خطای B10 با استفاده از نرم‌افزار IRES2.1



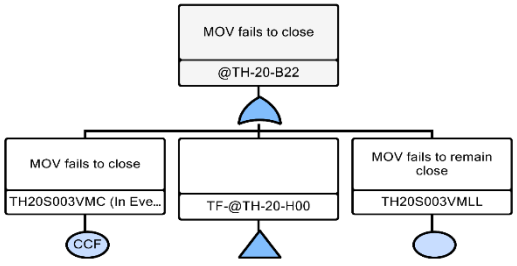
شکل ۱۰: پیاده‌سازی درخت خطای C10 با استفاده از نرم‌افزار IRES2.1



شکل ۱۱: پیاده‌سازی درخت خطای خط مکش شماره ۲۰ با استفاده از نرم‌افزار IRES2.1



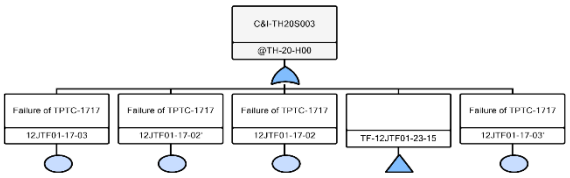
شکل ۱۲: پیاده‌سازی درخت خطای A20 با استفاده از نرم‌افزار IRES2.1



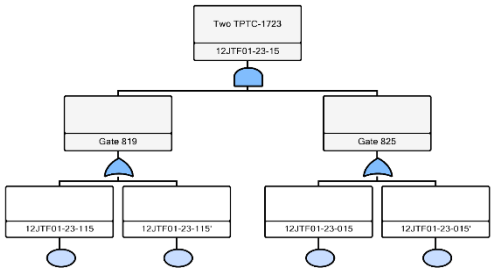
شکل ۱۳: پیاده‌سازی درخت خطای B20 با استفاده از نرم‌افزار IRES2.1

[1] Failure of suction line from tank

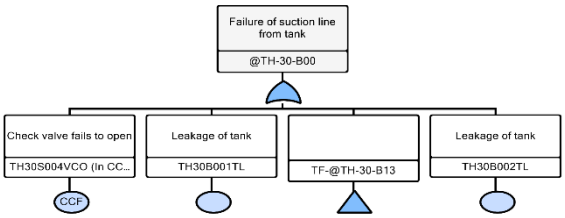
[2] Emergency Core Cooling System (ECCS)



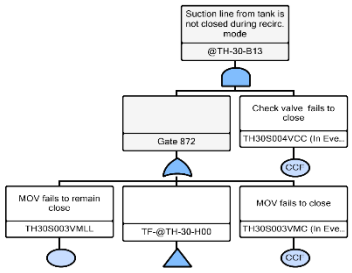
شکل ۱۴: پیاده‌سازی درخت خطای C20 با استفاده از نرم‌افزار IRES2.1



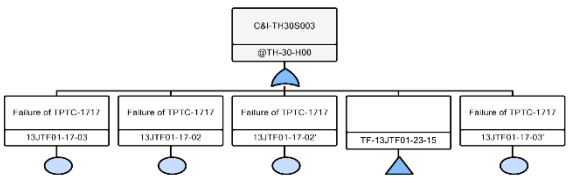
شکل ۱۵: پیاده‌سازی درخت خطای D20 با استفاده از نرم‌افزار IRES2.1



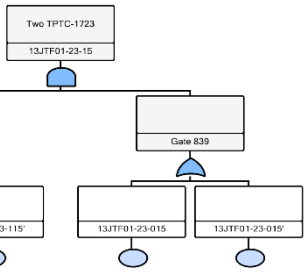
شکل ۱۶: پیاده‌سازی درخت خطای خط مکش شماره ۳۰ با استفاده از نرم‌افزار IRES2.1



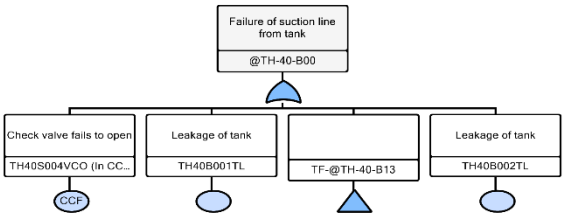
شکل ۱۷: پیاده‌سازی درخت خطای A30 با استفاده از نرم‌افزار IRES2.1



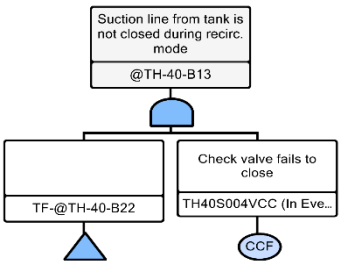
شکل ۱۸: پیاده‌سازی درخت خطای B30 با استفاده از نرم‌افزار IRES2.1



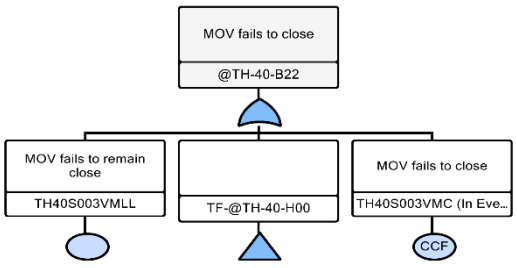
شکل ۱۹: پیاده‌سازی درخت خطای C30 با استفاده از نرم‌افزار IRES2.1



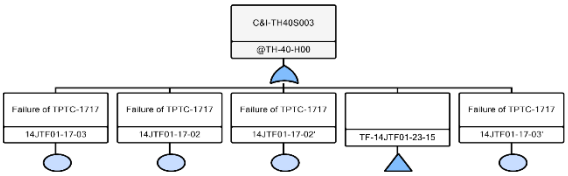
شکل ۲۰: پیاده‌سازی درخت خطای خط مکش شماره ۴۰ با استفاده از نرم‌افزار IRES2.1



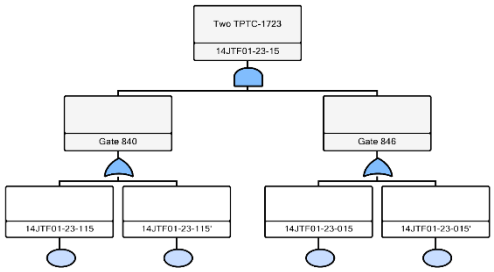
شکل ۲۱: پیاده‌سازی درخت خطای A40 با استفاده از نرم‌افزار IRES2.1



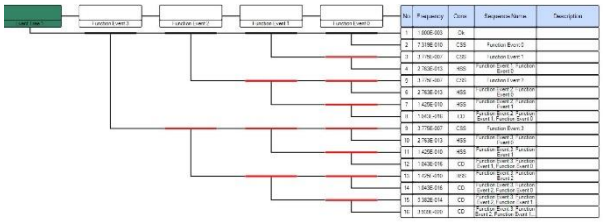
شکل ۲۲: پیاده‌سازی درخت خطای B40 با استفاده از نرم‌افزار IRES2.1



شکل ۲۳: پیاده‌سازی درخت خطای C40 با استفاده از نرم‌افزار IRES2.1



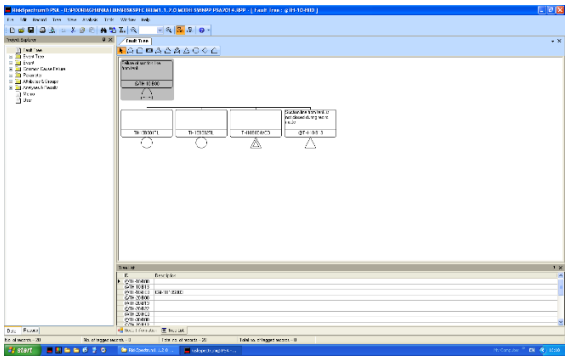
شکل ۲۴: پیاده‌سازی درخت خطای D40 با استفاده از نرم‌افزار IRES2.1



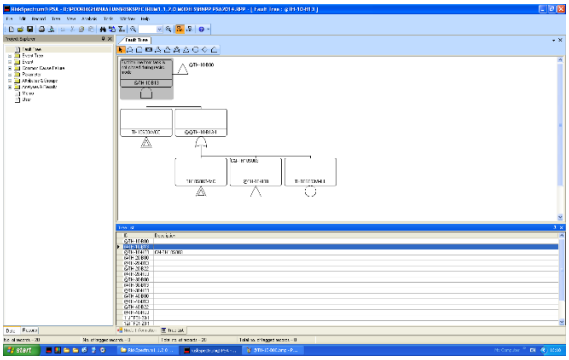
شکل ۲۵: پیاده‌سازی درخت رویداد Event Tree 1 با استفاده از نرم‌افزار IRES2.1

مدل‌سازی درخت خطا و درخت رویداد با استفاده از نرم‌افزار RiskSpectrum1.1.2.0

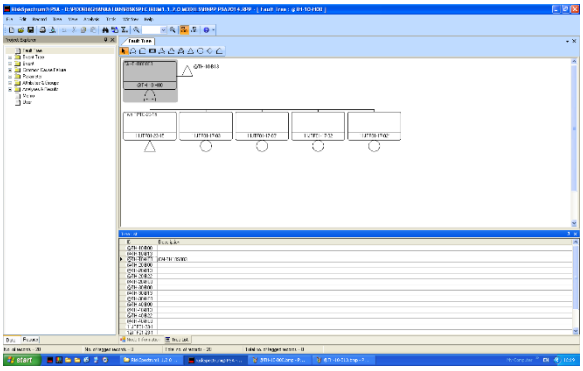
با هدف مقایسه‌ی بین نتایج، درخت‌های خطا و رویداد با استفاده از نرم‌افزار RiskSpectrum1.1.2.0 نیز پیاده‌سازی شده است که تصاویر آن در شکل‌های زیر نشان داده شده است.



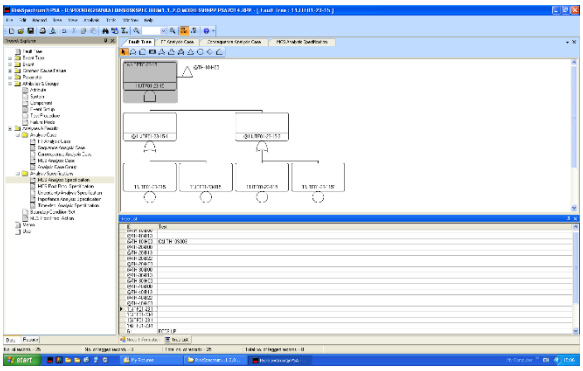
شکل ۲۶: پیاده‌سازی درخت خطای خط مکش شماره ۱۰ در نرم‌افزار RiskSpectrum1.1.2.0



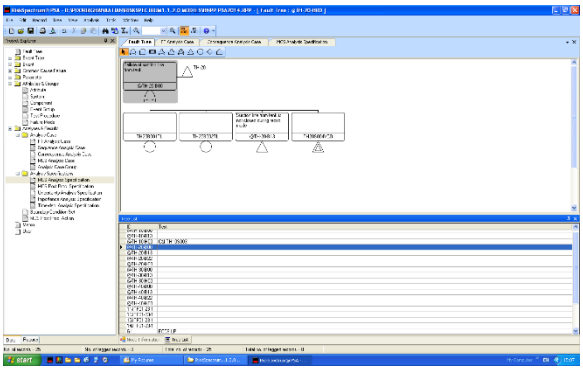
شکل ۲۷: پیاده‌سازی درخت خطای A10 در نرم‌افزار RiskSpectrum1.1.2.0



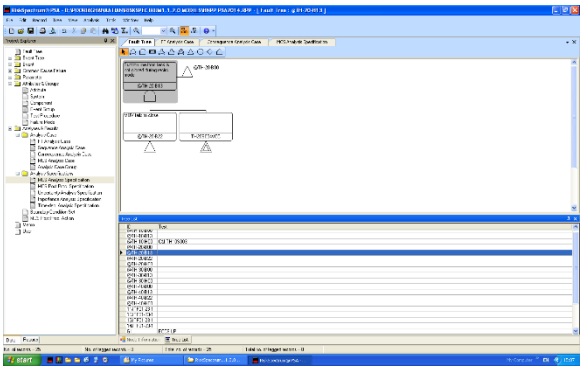
شکل ۲۸: پیاده‌سازی درخت خطای B10 در نرم‌افزار RiskSpectrum1.1.2.0



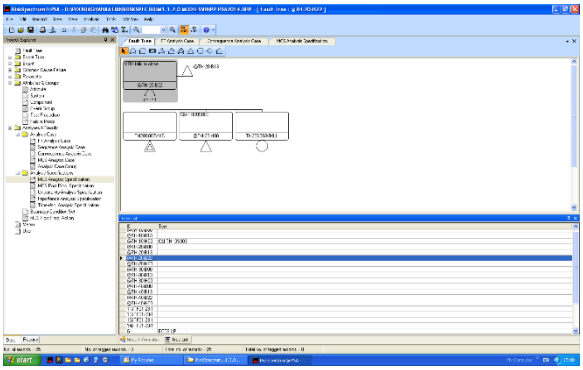
شکل ۲۹: پیاده‌سازی درخت خطای C10 در نرم‌افزار RiskSpectrum1.1.2.0



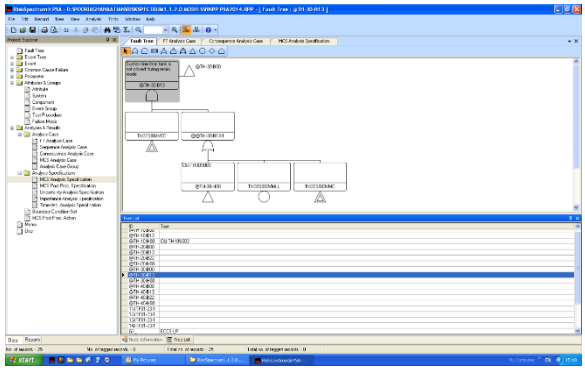
شکل ۳۰: پیاده‌سازی درخت خطای خط مکش شماره ۲۰ در نرم‌افزار RiskSpectrum1.1.2.0



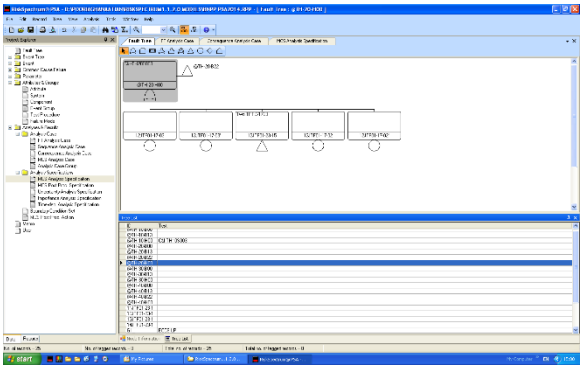
شکل ۳۱: پیاده‌سازی درخت خطای A20 در نرم‌افزار RiskSpectrum1.1.2.0



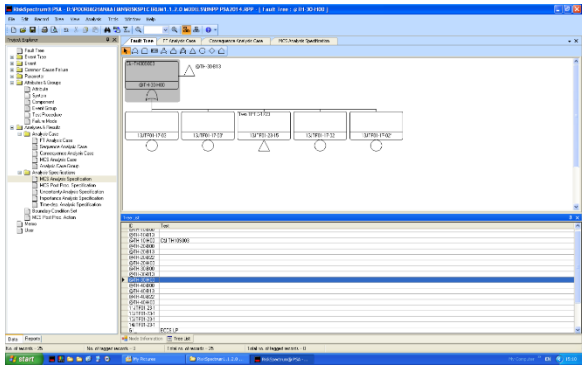
شکل ۳۲: پیاده‌سازی درخت خطای B20 در نرم‌افزار RiskSpectrum1.1.2.0



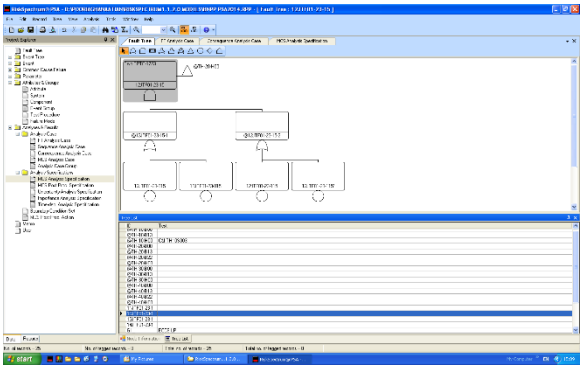
شکل ۳۶: پیاده‌سازی درخت خطای A30 در نرم‌افزار RiskSpectrum1.1.2.0



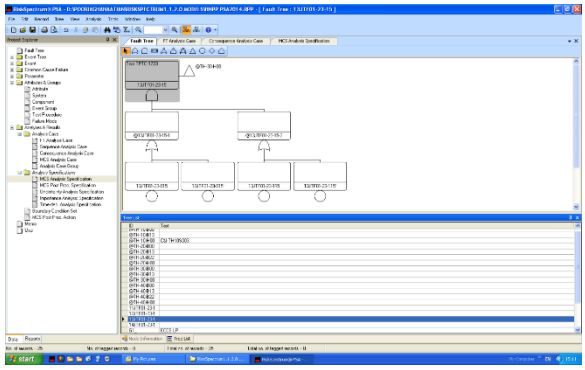
شکل ۳۳: پیاده‌سازی درخت خطای C20 در نرم‌افزار RiskSpectrum1.1.2.0



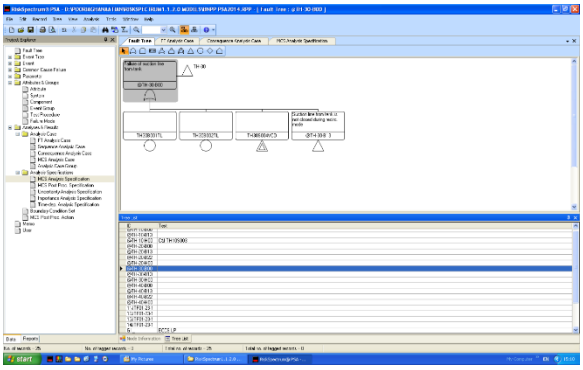
شکل ۳۷: پیاده‌سازی درخت خطای B30 در نرم‌افزار RiskSpectrum1.1.2.0



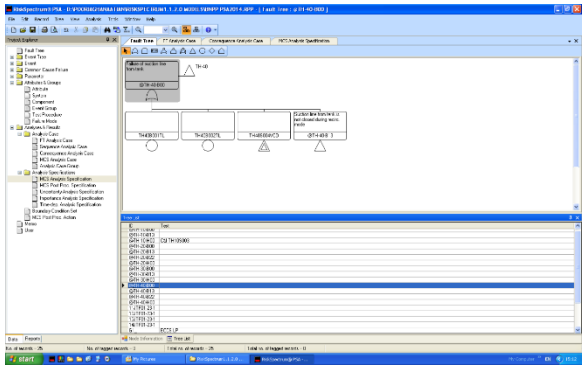
شکل ۳۴: پیاده‌سازی درخت خطای D20 در نرم‌افزار RiskSpectrum1.1.2.0



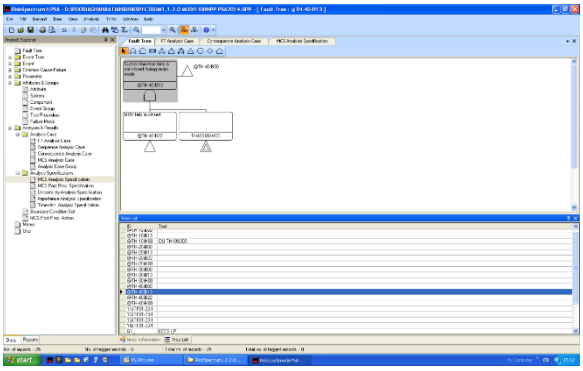
شکل ۳۸: پیاده‌سازی درخت خطای C30 در نرم‌افزار RiskSpectrum1.1.2.0



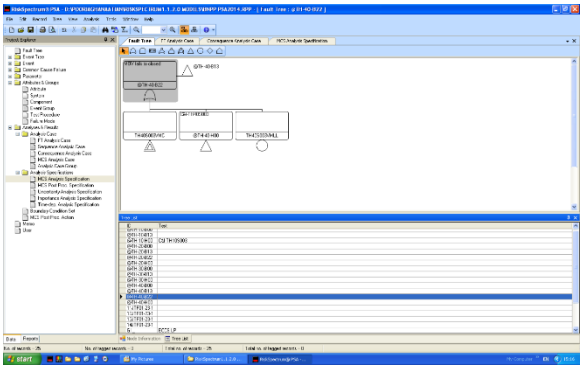
شکل ۳۵: پیاده‌سازی درخت خطای خط مکش شماره ۳۰ در نرم‌افزار RiskSpectrum1.1.2.0



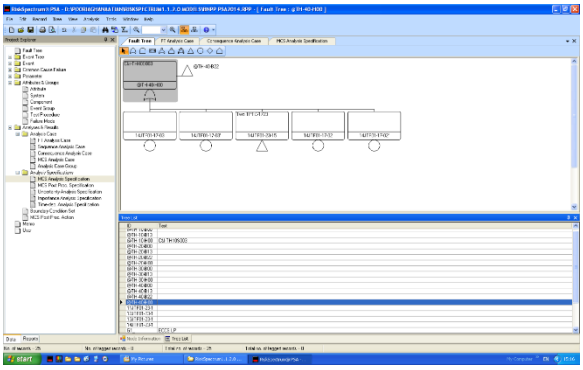
شکل ۳۹: پیاده‌سازی درخت خطای خط مکش شماره ۴۰ در نرم‌افزار RiskSpectrum1.1.2.0



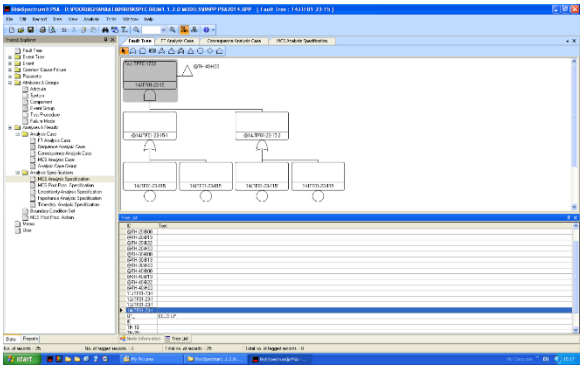
شکل ۴۰: پیاده‌سازی درخت خطای A40 در نرم‌افزار RiskSpectrum1.1.2.0



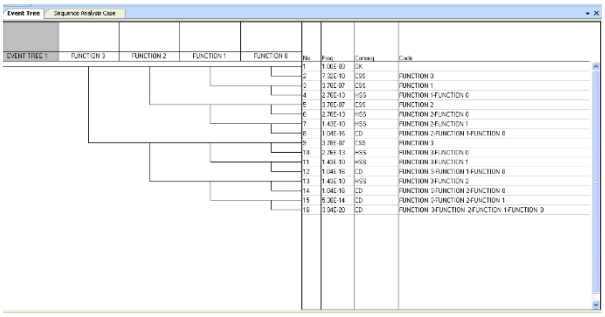
شکل ۴۱: پیاده‌سازی درخت خطای B40 در نرم‌افزار RiskSpectrum1.1.2.0



شکل ۴۲: پیاده‌سازی درخت خطای C40 در نرم‌افزار RiskSpectrum1.1.2.0



شکل ۴۳: پیاده‌سازی درخت خطای D40 در نرم‌افزار RiskSpectrum1.1.2.0



شکل ۴۴: پیاده‌سازی درخت رویداد Event Tree 1 در نرم‌افزار RiskSpectrum1.1.2.0

بررسی نتایج

نتایج مدل‌سازی درخت‌های خطای نمونه در جدول ۳ و نتایج مدل‌سازی درخت رویداد نمونه در جدول ۴ لیست شده است. با مقایسه‌ی بین نتایج مدل‌سازی در دو نرم‌افزار IRES2.1 و RiskSpectrum1.1.2.0، مشاهده می‌شود که در مسأله نمونهٔ انتخابی، نتایج تقریباً یکسانی حاصل شده است. لازم به ذکر است با پیچیده‌تر شدن مسأله، از جمله انتخاب درخت‌های خطا و رویداد بزرگتر، امکان حصول تمایزهایی بین نتایج دو نرم‌افزار وجود دارد.

جدول ۳: مقایسه بین نتایج درخت خطا در دو نرم افزار IRES2.1 و RiskSpectrum1.1.2.0

شماره	نام درخت خطا	IRES2.1		RiskSpectrum1.1.2.0	
		تعداد مجموعه برشی کمینه	احتمال عدم دسترسی	تعداد مجموعه برشی کمینه	احتمال عدم دسترسی
۱	خط مکش شماره ۱۰	146	7.231E-5	146	7.231E-5
۲	A10	136	7.319E-5	136	7.319E-5
۳	B10	8	3.775E-4	8	3.775E-4
۴	C10	4	5.156E-8	4	5.156E-8
۵	خط مکش شماره ۲۰	146	7.231E-5	146	7.231E-5
۶	A20	136	7.319E-5	136	7.319E-5
۷	B20	17	7.566E-4	17	7.566E-4
۸	C20	8	3.775E-4	8	3.775E-4
۹	D20	4	5.156E-8	4	5.156E-8
۱۰	خط مکش شماره ۳۰	146	7.231E-5	146	7.231E-5
۱۱	A30	136	7.319E-7	136	7.319E-7
۱۲	B30	8	3.775E-4	8	3.775E-4
۱۳	C30	4	5.156E-8	4	5.156E-8
۱۴	خط مکش شماره ۴۰	146	7.231E-5	146	7.231E-5
۱۵	A40	136	7.319E-7	136	7.319E-7
۱۶	B40	17	7.566E-4	17	7.566E-4
۱۷	C40	8	3.775E-4	8	3.775E-4
۱۸	D40	4	5.156E-8	4	5.156E-8

جدول ۴: مقایسه بین نتایج درخت رویداد در دو نرم افزار IRES2.1 و RiskSpectrum1.1.2.0

شماره توالی درخت رویداد	IRES2.1		RiskSpectrum1.1.2.0	
	تعداد مجموعه برشی کمینه	فرکانس رخداد (1/year)	تعداد مجموعه برشی کمینه	فرکانس رخداد (1/year)
۱	0	1E-3	1	1E-3
۲	136	7.319E-10	136	7.316E-10
۳	8	3.775E-7	8	3.775E-7
۴	1088	2.763E-13	1088	2.762E-13
۵	8	3.775E-7	8	3.775E-7
۶	1088	2.763E-13	1088	2.762E-13
۷	64	1.425E-10	64	1.425E-10
۸	8704	1.043E-16	8704	1.043E-16
۹	8	3.775E-7	8	3.775E-7
۱۰	1088	2.763E-13	1088	2.762E-13
۱۱	64	1.425E-10	64	1.425E-10
۱۲	8704	1.043E-16	8704	1.043E-16
۱۳	64	1.425E-10	64	1.425E-10
۱۴	8704	1.043E-16	8704	1.043E-16
۱۵	512	5.382E-14	512	5.382E-14
۱۶	69632	3.939E-20	69632	3.937E-20

نتیجه‌گیری

نرم‌افزار IRES2.1 پس از طی کردن مراحل مختلف طراحی و توسعه که همگی از استانداردهای لازم برخوردار بوده‌اند، به منظور کشف نقاط ضعف، نمونه مسائل عملیاتی متعددی با استفاده از آن توسعه یافته است و نتایج مدل‌سازی‌ها با بهترین نرم‌افزارهای حال حاضر (RiskSpectrum و SAPHIRE) مقایسه شده‌اند که حکایت از قابل اعتماد بودن این نرم‌افزار دارد. قطعاً نسخه‌ی ۲,۱ این نرم‌افزار، پایان کار نیست و احتمال یافتن نقاط ضعف وجود دارد، لذا روند توسعه این نرم افزار ادامه دارد و در این راستا از تمامی صاحب‌نظران و پژوهشگران برای کمک به پیشرفت نرم‌افزار دعوت بعمل می‌آید. برخی از اقدامات آتی از جمله بهینه‌سازی سرعت محاسبات و توسعه‌ی مدل‌های وابسته به زمان با هدف پوشش دادن مسائل Living-PSA، توسعه‌ی مدل‌های تعمیر و نگهداری، توسعه‌ی روش SPAR-H برای محاسبه‌ی خطای انسانی و ایجاد قابلیت انجام PSA سطح ۲، در راستای ارتقای نرم‌افزار IRES انجام خواهد شد.

مراجع

[1]. Hwang, S., & Pham, H. (2009). Quasi-renewal time-delay fault-removal consideration in software reliability modeling. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 39(1), 200-209.
[2]. Jordan-Cizelj, R., Vrbanić, I., & Mavko, B. (2002). Uncertainty analysis of fault tree parameters.
[3]. Kaplan, S. and J. Garrick, on the quantitative definition of risk, Risk Anal., 1(1), 11-28, 1981.
[4]. Stamatelatos, M., Dezfuli, H., Apostolakis, G., Everline, C., Guarro, S., Mathias, D., & Vesely, W. (2011). Probabilistic risk assessment procedures guide for NASA managers and practitioners.
[5]. Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide, No.SSG-3, IAE.
[6]. Modarres, M., Kaminskiy, M. P., & Krivtsov, V. (2016). Reliability engineering and risk analysis: a practical guide.
[7]. RiskSpectrum Analysis Tools, Theory Manual, 2008.
[8]. Evaluation of Human Reliability Analysis Methods Against Good Practice, NUREG-1842, August 2006.
[9]. Smith, C., Knudsen, J., Vedros, K., Calley, M., Kvarfordt, K., & Wood, T. (2016). SAPHIRE 8 Basics An Introduction to Probabilistic Risk Assessment via the Systems Analysis Program for Hands-On Integrated Reliability Evaluations (SAPHIRE) Software P-201 (No. INL/EXT-17-40988-Rev000). Idaho National Lab.(INL), Idaho Falls, ID (United States).
[10]. Integrated Reliability and Safety Assessment (IRES) Technical Manual, Release Version 2.1, 2022.