هفتمین کنفرانس بین‌المللی
مهندسی قابلیت اطمینان و ایمنی

# آنالیز قابلیت اطمینان تجهیزات سیستم I&C نیروگاه اتمی نوع VVER-1000

**امیر باریک لو[۱]، محمدرضا عباسی[۲] و سعید کردعلیوند[۳]**

**۱- دانشجوی کارشناسی ارشد، دانشکده مهندسی هسته‌ای، دانشگاه شهید بهشتی، تهران، ایران، a.bariklou@mail.sbu.ac.ir**

**۲- استادیار، دانشکده مهندسی هسته‌ای، دانشگاه شهید بهشتی، تهران، ایران، m_abbasi@sbu.ac.ir**

**۳- معاونت مهندسی هسته‌ای، شرکت توسعه و ارتقاء ایمنی نیروگاه‌های اتمی (توانا)، تهران، ایران، skordalivand@gmail.com**

**چکیده**

قابلیت اطمینان به معنای توانایی سیستم در انجام دادن صحیح مأموریت مشخص خود است. قابلیت اطمینان یک نیروگاه اتمی در واقع تولید برق ایمن و پایدار است. به منظور ارزیابی قابلیت اطمینان یک نیروگاه اتمی، لازم است ابتدا تمامی سیستم‌های نیروگاه بررسی و قابلیت اطمینان آنها مشخص شود. در نیروگاه‌های اتمی VVER-1000، قابلیت اطمینان سیستم I&C آنها به عنوان مغز نیروگاه به صورت دقیق مشخص نشده است. قابلیت اطمینان سیستم I&C نیروگاه اتمی، در واقع توانایی این سیستم در انجام وظایف خود در راستای ایجاد برق ایمن و پایدار در شرایط معین و در دوره زمانی مشخص است. به منظور ارزیابی قابلیت اطمینان سیستم I&C نیروگاه اتمی VVER-1000، لازم است ابتدا کلیه زیرسیستم‌های آن مشخص و بصورت دقیق مدل‌سازی شده تا سپس براساس نتایج آنالیز آنها، ارزیابی قابلیت اطمینان کلی سیستم انجام شود. به همین منظور در مقاله حاضر، زیرسیستم‌های سیستم I&C نیروگاه اتمی VVER-1000 ابتدا شناسایی و سپس قابلیت اطمینان آنها بر اساس روش درخت خطا و با استفاده از داده‌های جنریک و از طریق نرم‌افزار SAPHIRE 7 بررسی شده و نتایج آن ارائه شده است.

**واژه‌های کلیدی:** آنالیز درخت خطا، قابلیت اطمینان، تجهیزات کنترل و ابزاردقیق، I&C، نیروگاه VVER

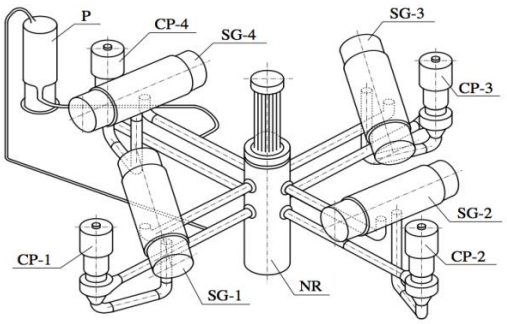
## مقدمه

در یک نیروگاه هسته‌ای سیستم های مختلفی وجود داشته که می‌بایست در یک هماهنگی بخصوصی با یکدیگر در تعامل و فعالیت بوده تا بتوانند هدف غایی نیروگاه هسته‌ای یعنی تولید برق ایمن را فراهم نمایند. در یک نیروگاه هسته‌ای این هماهنگی توسط سیستم‌های کنترل و ابزاردقیق انجام می‌گردد. همچنین این سیستم‌ها این قابلیت را به اپراتورهای نیروگاه می‌دهند که بر روی تمامی فعالیت‌های موجود در نیروگاه نظارت کافی را داشته باشند. این موارد نشان‌دهنده اهمیت سیستم کنترل و ابزاردقیق در نیروگاه بوده و لزوم بهبود عملکرد و افزایش راندمان و دقت و سرعت آن را نشان می‌دهد. به همین منظور ضروری است در ابتدا قابلیت اطمینان این سیستم‌ها به صورت دقیق ارزیابی شود.

در ارزیابی احتمالاتی ایمنی نیروگاه اتمی VVER-1000 مدل قابلیت اطمینان سیستم کنترل و ابزاردقیق به صورت یک رویداد پایه در نظر گرفته شده که در این پژوهش سعی شده است که به صورت دقیق بخشی از آن مدل‌سازی گردد.

## نیروگاه اتمی VVER-1000

نیروگاه اتمی VVER-1000 یک نیروگاه آب سبک تک‌واحدی با توان اسمی ۱۰۰۰ مگاوات الکتریکی، دارای راکتور آب تحت فشار به قدرت ۳۰۰۰ مگاوات حرارتی است و ساخت کشور روسیه می‌باشد. این نیروگاه از دو مدار اولیه و ثانویه (شکل ۱) تشکیل شده است. توان حرارتی تولیدی در قلب توسط آب برداشت شده و با انتقال از طریق پایه داغ، سیال مدار ثانویه را بخار می‌کند و سپس از طریق پایه سرد به راکتور باز می‌گردد. بخش اعظم بخار تولیدی در مدار ثانویه به توربین منتقل شده و اندکی از آن برای گرمایش آب تغذیه به کار می‌رود.




**شکل ۱:** نمای کلی مدار اولیه نیروگاه اتمی VVER-1000 [۱].

## تجهیزات کنترل و ابزاردقیق (I&C)

از مهمترین سیستم‌های ایمنی یک نیروگاه اتمی، سیستم کنترل و ابزاردقیق است. معماری سیستم کنترل و ابزاردقیق، در کنار اقدامات اپراتوری نیروگاه، به عنوان مغز متفکر یک نیروگاه هسته‌ای عمل می‌کند. سیستم کنترل و ابزاردقیق از طریق عناصر تشکیل‌دهنده خود مانند تجهیزات، ماژول‌ها، حسگرها، فرستنده‌ها، موتورها، شیرها و سایر موارد، پارامترهای نیروگاه را حس نموده، عملکردهای سیستم‌ها را نظارت می‌کند، اطلاعات دریافتی را یکپارچه‌سازی نموده و در صورت لزوم تنظیمات خودکار را برای مودهای مختلف عملیاتی نیروگاه هسته‌ای انجام می‌دهد. همچنین به خرابی ها و رویدادهای غیرعادی به گونه‌ای پاسخ می‌دهد که تولید برق کارآمد و ایمن تضمین شود. این سیستم‌های پیشرفته عملکرد کل نیروگاه را مورد نظارت و بررسی قرار داده و در نتیجه اقتصاد و ایمنی نیروگاه‌های فعلی و آینده را بهبود می‌بخشد. سیستم‌های اندازه‌گیری و نظارت دیجیتالی مدرن نیز می‌توانند به امنیت فیزیکی و سایبری نیروگاه‌ها کمک کنند، اگر با امنیت به عنوان یک نیاز اصلی، طراحی شوند [۲].

تجهیزات کنترل و ابزاردقیق، هسته اصلی تمامی فعالیت‌های صنعتی و تولیدی است. در یک مرکز تولید، هر فرآیند باید به دقت نظارت و کنترل گردد تا به روشی از پیش تعیین شده که هم بهینه و هم ایمن باشد، پیش برود. به عنوان مثال، سیستم‌های نظارت و کنترل دما در پالایشگاه‌های پتروشیمی از افزایش دما به سطوح بحرانی و رسیدن به مرز انفجار جلوگیری می‌نمایند. بدون پانل‌های کنترل بخاری فرآیند الکتریکی، ممکن است جان انسان‌ها و دارایی آنان نابود گردد.

قابلیت اطمینان، عموماً به عنوان احتمال اینکه یک قطعه یا مجموعه بدون خرابی برای مدت معینی تحت شرایط مشخص کار کند تعریف می‌گردد. به منظور حصول اطمینان از یک نتیجه معنادار، شرایط عملکرد و همچنین استاندارد عملکرد مورد نیاز، اعم از فیزیکی و الکتریکی، به صورت زیر می‌بایست با جزئیات مشخص گردند:

۱. تغییرات در ولتاژ منابع تغذیه و مقادیر ولتاژ گذرا؛
۲. تغییرات فرکانس و محتوای هارمونیک؛
۳. سطح انرژی RF ساطع شده ناخواسته توسط تجهیزات نباید باعث تداخل در ارتباطات رادیویی گردد؛
۴. اگر قرار است قطعات یا تجهیزات در نزدیکی فرستنده‌های رادیویی یا رادارهای پُرقدرت مورد استفاده قرار گیرند، می‌بایست تجهیزات مقداری تابش RF را تحمل نمایند؛
۵. تجهیزات ماهواره‌ها و نیروگاه‌های هسته‌ای می‌بایست در برابر تشعشعات یونیزان دارای حفاظ باشند؛
۶. حداکثر و حداقل دمای محیط می‌بایست برای تجهیزات رعایت گردد؛
۷. حداکثر و حداقل رطوبت برای هر تجهیز در محیط کاری مدنظر باشد؛
۸. سطوح ارتعاش و شوک با توجه به محیط و شرایط کاری مدنظر قرار گیرد؛
۹. شرایط خارجی زیست محیطی اعم از قرار گرفتن در معرض طوفان‌های شن و گرد و غبار، باران یا تشعشعات خورشیدی؛
۱۰. فشار هوا؛
۱۱. تغییرات در بارگذاری (در صورت لزوم).

در طراحی بسیاری از سیستم‌های کنترل، اهمیت قابلیت اطمینان به پیامدهای خرابی وابسته می‌باشد. به عنوان مثال هزینه خرابی در مدارهای کنترل لوازم خانگی مانند ماشین لباسشویی تا حد زیادی به هزینه تعمیر محدود می‌شود. اگر در مدت ضمانت خرابی اتفاق بیفتد، این هزینه بر عهده سازنده آن خواهد بود. سازنده علاقه‌مند به ساخت محصولی با قابلیت اطمینان کافی، برای اطمینان از سطح بسیار بالا بازده محصول تحت ضمانت و همگامی با رقبا می‌باشد.

به عنوان مثال دیگر، هزینه خرابی سیستم‌های کنترل یا ایمنی یک راکتور هسته‌ای بسیار هنگفت می‌باشد، اما تعیین کمیت آن آسان نیست. در نتیجه این هزینه بسیار بالا، قابلیت اطمینان مشخص شده برای سیستم های ایمنی راکتور نیز بسیار بالا است.

از آنجایی که نیاز به قابلیت اطمینان بالاتر است، هزینه‌های طراحی، ساخت و آزمایش تجهیزات و نیروگاه نیز همگی به سرعت افزایش می‌یابند. هزینه‌های تعمیرات و نگهداری و تجهیزات آماده به کار، با افزایش قابلیت اطمینان همه آنها کاهش می‌یابد. برای سیستم‌های با قابلیت اطمینان بالا که ممکن است خرابی جان انسان‌ها را به خطر بیندازد، معمولاً یک الزام قانونی برای حداقل قابلیت اطمینان مشخص وجود دارد و این به عامل اصلی تبدیل می‌شود. سپس هدف طراح به سمت دستیابی به این قابلیت اطمینان با حداقل هزینه هدایت می‌شود. چنین الزاماتی برای سیستم‌های کنترل فرود کور برای هواپیماهای مسافربری و مدارهای ایمنی راکتورهای انرژی هسته‌ای پیش بینی شده است [۳].

روش ارزیابی احتمالاتی ایمنی جهت محاسبه ریسک در صنایع و سیستم‌های مهندسی پیچیده از جمله صنعت هسته‌ای به کار می‌رود. روش ارزیابی احتمالاتی ایمنی یک ترکیب کاملاً کلاسیک از آنالیز درخت خطا و آنالیز درخت رویداد جهت شبیه‌سازی ریسک می‌باشد. روش‌های درخت خطا و درخت رویداد بر پایه یک سری روابط آماری و منطق بولی استوار می‌باشند [۴].

## تجهیزات کنترل و ابزاردقیق نیروگاه اتمی VVER-1000

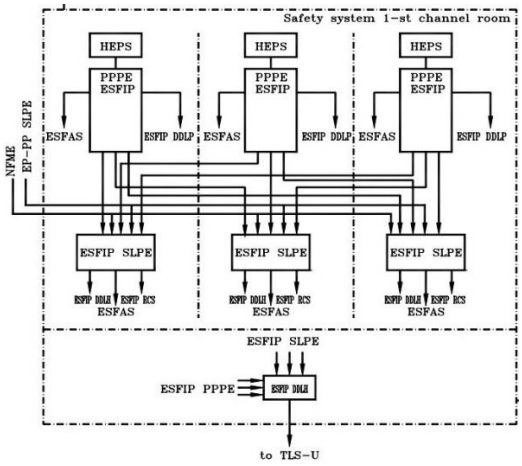
بخش تجهیزات کنترل و ابزاردقیق (I&C) نیروگاه شامل دو زیرسیستم است که با استفاده از نرم‌افزار و سخت‌افزارهای مختلف پیاده‌سازی می‌شوند:

- بخش آغازگر ویژگی مهندسی‌شده ایمنی (ESFIP)؛
- سیستم فعال‌سازی ویژگی مهندسی‌شده ایمنی (ESFAS).

بخش آغازگر ویژگی مهندسی‌شده ایمنی (ESFIP) موارد زیر را فراهم می‌نماید:

- دریافت و تبدیل سیگنال‌ها توسط پارامترهای مورد نیاز برای فعال‌سازی سیستم ایمنی و عملکردهای حفاظت محلی؛
- مقایسه پارامترهای کنترل‌شده سیگنال‌های در حال اجرا با نقاط‌تنظیم تعیین شده، تولید سیگنال‌های گسسته در انحراف پارامتر کنترل‌شده در خارج از رنج نقطه تنظیم و انتقال این سیگنال‌ها به زیرسیستم منطقی مناسب؛
- تولید سیگنال آنالوگ با پارامتر کنترل‌شده برای تولید در ESFAS و نمایش بعدی در نمایشگرهای جداگانه اتاق کنترل اصلی و اضطراری و سیگنال‌های دیجیتال در پانل‌های اتاق کنترل اصلی و اضطراری؛
- تولید سیگنال گسسته در ESFAS برای پردازش بعدی و فعال‌سازی مکانیسم‌های کنترل؛
- تولید داده با هدف پارامتر کنترل شده و نقص عملکرد ESFIP و انتقال به TLS-U برای نمایش آن بر روی کنسول کنترل اپراتور اتاق کنترل اصلی و اضطراری؛
- نظارت مستمر بر قابلیت سرویس‌دهی ویژگی‌های مهندسی‌شده سیستم و بازرسی منظم از عملکرد سیستم با پرسنل درگیر.

بلوک دیاگرام برای یک کانال ESFIP در شکل ۲ آورده شده است.




**شکل ۲:** بلوک دیاگرام برای یک کانال ESFIP

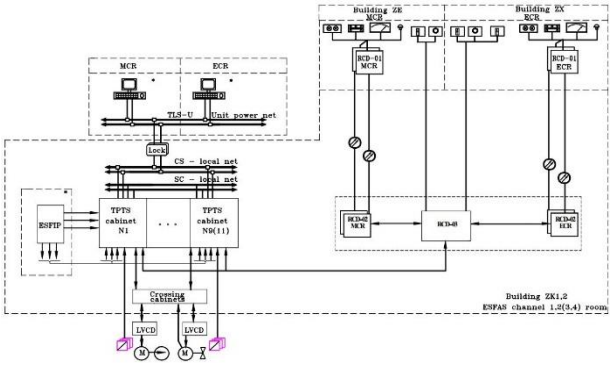
در بهره‌برداری نرمال سیستم فعال‌سازی ویژگی مهندسی‌شده ایمنی (ESFAS) موارد زیر فراهم می‌شود:

- نظارت مستمر بر قابلیت سرویس‌دهی ویژگی‌های مهندسی‌شده سیستم و بازرسی منظم از عملکرد سیستم با پرسنل درگیر؛
- کنترل ویژگی‌های مهندسی‌شده ایمنی و نمایش داده‌ها برای پرسنل بهره‌برداری؛
- اجرای حفاظت‌های پردازش محلی و اینترلاک‌های بهره‌برداری نرمال برای سیستم‌هایی که عملکردهای بهره‌برداری نرمال و ایمنی را با هم ترکیب می‌کنند و در برخی رویدادها یک اقدام کنترلی برای تجهیزات پردازش ایجاد می‌کنند؛
- کنترل خودکار؛
- کنترل از راه دور در صورت نیاز؛
- دریافت ماموریت‌ها از اپراتور که مود بهره‌برداری را برای تجهیزات آماده به کار و برای کنترلرها انتخاب می‌کند.

در موارد اضطراری که توسط سیگنال‌های پارامترهای رویداد اولیه معرفی می‌شوند، ESFAS عملکرد مستقیم خود را انجام می‌دهد و موارد زیر اجرا می‌شود:

- عمل کنترل برای محرک‌ها در ورود سیگنال‌های آغازگر ESFIP ایجاد می‌شود.
- اولویت‌های مورد نیاز خودکار و اقدامات اپراتور را متوجه می‌شود.
- در هنگام رسیدن سیگنال‌های گسسته ESFIP در تمام پارامترها که به شرایط فعال‌سازی حفاظت می‌رسند، رویدادهای اولیه، سیگنال‌های لازم روی پانل را تولید و به سیستم داده و دستگاه‌های ضبط می‌رسانند.
- کنترل عملکرد اختصاص داده شده، ارائه شده است.
- در صورت نیاز کنترل از راه دور ارائه می‌شود.

بلوک دیاگرام برای یک کانال ESFAS در شکل ۳ آورده شده است.

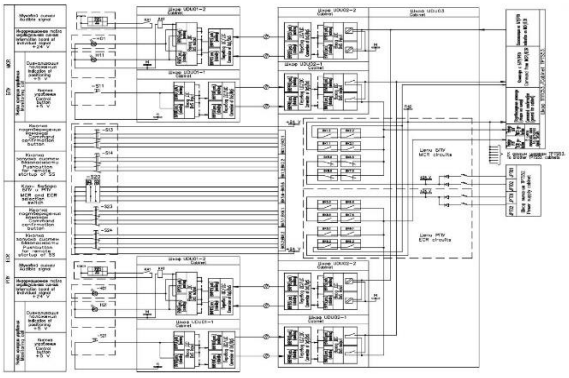



**شکل ۳:** بلوک دیاگرام برای یک کانال ESFAS

در صورت خرابی بخش های ESFAS و ESFIP، سیستم کنترل و ابزاردقیق از طریق سیستم کنترل از راه دور (RCD) از طریق اتاق کنترل اصلی/اضطراری هدایت خواهد کرد. در واقع مدارهای الکتریکی از پانل‌های ایمنی اتاق کنترل اصلی و اتاق کنترل اضطراری به دستگاه کنترل از راه دور (RCD) که در اتاق مجاور چیده شده‌اند، با استفاده از یک کابل غیرقابل انتشار ایمن وصل می‌شوند. جریان در این مدارها چند ده میلی‌آمپر در ولتاژ ۲۴ ولت است که احتمال احتراق کابل را به حداقل می‌رساند. کابل‌ها به طور جداگانه در کانال‌های مجزا هدایت

می‌شوند. پیوند RCD به اتاق‌های ایمنی در ساختمان‌های راکتور و توربین با استفاده از کابل فیبر نوری که در کانال‌های کابل مجزا هدایت می‌شود، طراحی شده‌اند.

سیستم کنترل از راه دور برای هر انتقال سیگنال‌های گسسته برای انجام کنترل دارای یک ساختار خاص برای هر سیستم و کنترل برای مثال دیاگرام کنترل موتور الکتریکی، کنترل شیرها و ... از اتاق کنترل اصلی و اضطراری می‌باشد. نمودار دستگاه کنترل از راه دور برای انتقال سیگنال‌های گسسته در شکل ۴ آورده شده است.



**شکل ۴:** نمودار دستگاه کنترل از راه دور برای انتقال سیگنال‌های گسسته

## تجهیزات کنترل و ابزاردقیق (I&C) ایمنی

I&C ایمنی، سیستم‌های مورد نیاز برای انجام عملکردهای ایمنی زیر را شامل می‌شود:

- تریپ راکتور و حفظ آن در شرایط زیربحرانی؛
- برداشت حرارت اضطراری؛
- نگهداری محصولات رادیواکتیو در محدوده تعیین شده.

مطابق با مفهوم «دفاع در عمق»، کارایی حصارهای حفاظتی در هنگام وقوع حوادث مبنای طراحی باید توسط عملکردهای ایمنی زیر ارائه شود:

۱. تریپ راکتور.

سیستم تریپ راکتور بخشی از I&C ایمنی به نام CPS-ESFIP است که در صورت لزوم، عملیات کنترلی را هنگام تریپ راکتور ایجاد می‌کند. سیستم تریپ راکتور شامل کنتاکتورهای شکسته‌ای است که با خاموش کردن مکانیسم‌های محرک میله کنترل و سپس سقوط تمام میله‌های کنترل توسط نیروی گرانشی در پاسخ به سیگنال‌های تولید شده در سیستم حفاظتی راکتور، به صورت خودکار یا دستی، امکان انجام تریپ راکتور را فراهم می‌کند. تریپ راکتور توسط اپراتور در پاسخ به سیگنال‌های آشکارسازهای پارامترهای نوترونی-فیزیکی و فرآیندی در مورد وضعیت نیروگاه راکتور و فشار محفظه ایمنی و همچنین توسط سیگنال‌های آشکارسازهای لرزه‌ای انجام می‌شود.

این سیستم شامل سیستم تحریک ESFIP است که برای تولید دستورات کنترلی توسط آشکارسازهای پارامترهای نوترونی-فیزیکی و فرآیند وضعیت نیروگاه راکتور و فشار محفظه ایمنی استفاده می‌شود.

۲. I&C سیستم ایمنی

I&C سیستم ایمنی یا به اصطلاح ESFAS بخشی از I&C است که با صدور دستورات ESFIP سیستم‌های حفاظتی، محلی‌سازی و پشتیبانی را فعال می‌کند [۵].

## روش آنالیز درخت خطا (FTA)

تجزیه و تحلیل درخت خطا یک ابزار گرافیکی می‌باشد که برای بررسی دلایل خرابی‌های سیستم مورد استفاده قرار می‌گیرد. این روش از منطق بولی (صفر و یک) برای ترکیب مجموعه‌ای از رویدادهای سطح پایین استفاده می‌نماید و اساساً یک رویکرد از بالا به پایین برای شناسایی خرابی‌های رویداد پایه‌ای است که باعث بروز خرابی در سیستم اصلی یا همان رویداد رأسی می‌گردد. آنالیز درخت خطا FTA متشکل از دو عنصر رویداد و گیت‌های منطقی بوده که رویدادهای مختلف را برای شناسایی علت وقوع رویداد احتمالی بهم متصل می‌نماید و نباید آن را با درخت رویداد یا درخت تصمیم اشتباه گرفت. روش تجزیه و تحلیل درخت خطا یک روش به مراتب ساده‌تر از تجزیه و تحلیل مودهای خرابی و اثرات آنها (FMEA) است، زیرا روی تمام شکست‌های احتمالی سیستم در یک رویداد اصلی احتمالی متمرکز می‌شود. در حالی که تجزیه و تحلیل مودهای خرابی و اثرات آنها، تجزیه و تحلیل را برای یافتن تمامی حالت‌های شکست سیستم بدون توجه به شدت آن‌ها انجام می‌دهد. تجزیه و تحلیل درخت خطا می‌تواند برای انجام فرآیند ارزیابی ریسک سیستم مورد استفاده قرار گیرد. هدف از تجزیه و تحلیل درخت خطا شناسایی علل موثر در خرابی سیستم و کاهش ریسک آنها قبل از رخدادن آنها است. ابزاری بسیار ارزشمند برای سیستم‌های پیچیده، که بطور گرافیکی، روش منطقی شناسایی خطا یا مشکل را نشان می‌دهد. علاوه بر این، می‌توان میزان بهره‌وری سیستم را با این تحلیل به دست آورد. این روش را می‌توان به تنهایی اجرا نموده و یا به عنوان روشی مکمل برای روش تجزیه و تحلیل مودهای خرابی و اثرات آنها قرار داد [۶].

تجزیه و تحلیل درخت خطا احتمال شکست سیستم را از طریق احتمالات خرابی زیر سیستم‌ها و اجزای آن و روابط منطقی بین آنها تخمین می‌زند. علاوه بر این، تجزیه و تحلیل FT نه تنها برای شناسایی تمام مسیرهای بالقوه ای که می‌تواند منجر به شکست شود، بلکه برای تعیین رویدادهای حیاتی که به طور قابل توجهی در احتمال خرابی یک سیستم نقش دارند و پیوندهای ضعیف در سیستم را آشکار می کنند، بکار می‌رود. نماد گیت "OR" نشان می دهد که اگر یکی از زیررویدادهای زیر رخ دهد، رویدادی ممکن است رخ دهد، که به

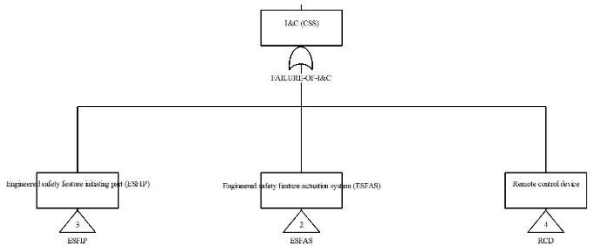
معنای اجتماع زیررویدادها است. نماد گیت "AND" نشان می دهد که در صورت وقوع همه زیررویدادها، رویدادی ممکن است رخ دهد، که به معنای فصل مشترک زیررویدادها است. مستطیل یک رویداد خطا را توصیف می‌کند که بیشتر از طریق گیت‌های منطقی به زیررویدادهای دیگر تبدیل می شود. دایره نشان دهنده خرابی اساسی ذاتی یک بخش سیستم، به اصطلاح یک رویداد خرابی اساسی است. رویدادهای اساسی از نظر آماری مستقل در نظر گرفته می‌شوند.

## معرفی نرم‌افزار SAPHIRE

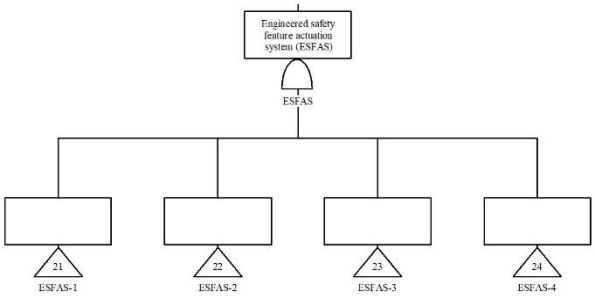
نرم‌افزار SAPHIRE بیانگر مجموعه‌ای از برنامه‌های کامپیوتری است که برای تولید و تحلیل ارزیابی ریسک احتمالاتی توسعه یافته‌اند . نسخه‌های گوناگونی از این کد توسعه یافته‌اند که اولین آنها در سال ۱۹۸۷ با نام IRRAS عرضه شد و آخرین گزارش مربوط به این کد در سال ۲۰۱۰ عرضه گردید. اساس کار این کد ترسیم درخت‌های عیب، درخت‌های رویداد ، ارتباط این دو درخت به یکدیگر و نهایتاً محاسبه موفقیت، خرابی نسبی و خرابی کامل سیستم است. با این تفاسیر، محاسبه احتمالات مذکور نیازمند شناخت دقیق اجزای سیستم و عملکرد آنها است. می‌توان گفت که عیب عمده این کد در User Interface نبودن آن است ولی راحتی کار با آن، روند مشخص اجرای کد و درک آسان قسمت‌های مختلف Manual کد از جمله مزایای آن به شمار می‌رود [۷].

## نتایج

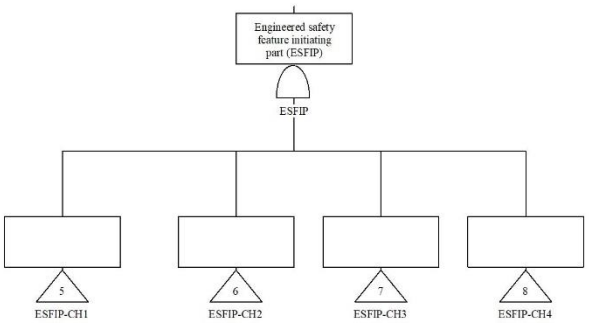
در این پژوهش تجزیه و تحلیل خطا بر روی سیستم کنترل و ابزاردقیق نیروگاه اتمی VVER-1000 انجام گرفته و برای این کار از داده‌های جنریک استفاده شده است [۸]. این تجزیه و تحلیل شامل قسمت تجهیزات نظارت بر شار نوترون نمی‌باشد. در این تجزیه و تحلیل از نرم افزار SAPHIRE7 برای ارزیابی درخت خطا استفاده شده است. همچنین در این ارزیابی تعداد ۶۹ درخت خطا ایجاد شده است که در ادامه مهمترین FTهای مدلسازی شده که توضیح هر کدام از این زیرسیستم‌ها در بخش‌های قبلی ارائه گردید، آورده شده است.



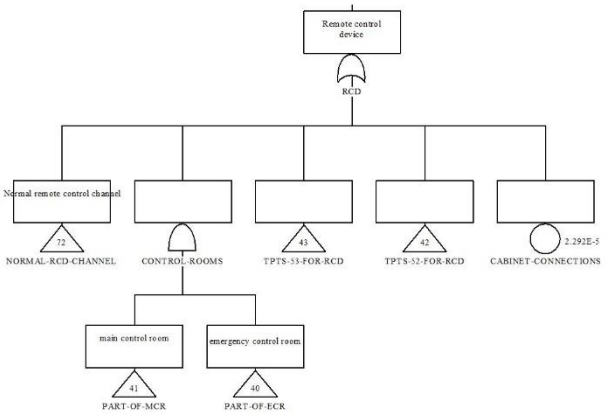

**شکل ۵:** درخت خطای اصلی سیستم کنترل و ابزاردقیق (I&C) نیروگاه VVER




**شکل ۶:** درخت خطای اصلی سیستم فعال‌سازی ویژگی‌های مهندسی‌شده ایمنی (ESFAS)




**شکل ۷:** درخت خطای اصلی بخش آغازگر ویژگی‌های مهندسی‌شده ایمنی (ESFIP)




**شکل ۸:** درخت خطای اصلی بخش کنترل از راه دور (RCD)

با جایگذاری اعداد جنریک برای رویدادهای خرابی اساسی، نتایج این تجزیه و تحلیل و اعدام مربوط به خرابی هر کدام از زیرسیستم‌های I&C نیروگاه اتمی VVER-1000 در جدول ۲ آورده شده است.

**جدول ۱:** نتایج تجزیه و تحلیل درخت خطا بر روی I&C نیروگاه VVER-1000

| درخت خطا | فرکانس وقوع خرابی بر سال | Cut Sets |
|---|---|---|
| ANALOG-TRANSDUCER | ۳/۴۳۳ × ۱۰$^{-۴}$ | ۴ |
| ANALOG-TRANSDUCER-DP&L | ۳/۴۳۳ × ۱۰$^{-۴}$ | ۴ |
| CABINET-TPTS53-2082-CV | ۲/۲۲۰× ۱۰$^{-۴}$ | ۸ |
| CABINET-UDU01-1 | ۴/۷۹۹× ۱۰$^{-۴}$ | ۴ |
| CABINET-UDU01-2 | ۴/۸۲۳× ۱۰$^{-۴}$ | ۵ |

| درخت خطا | فرکانس وقوع خرابی بر سال | Cut Sets |
|---|---|---|
| CABINET-UDU02-1 | ۴/۷۹۹× ۱۰$^{-۴}$ | ۴ |
| CABINET-UDU02-2 | ۴/۷۹۹× ۱۰$^{-۴}$ | ۴ |
| CV-FROM-MCR&ECR | ۴/۶۱۴× ۱۰$^{-۳}$ | ۵۹ |
| EMC-FROM-MCR&ECR | ۲/۲۷۸× ۱۰$^{-۳}$ | ۱۳۲ |
| ESFAS | ۱/۵۹۴× ۱۰$^{-۴}$ | ۶ |
| ESFAS-1 | ۱/۵۹۴× ۱۰$^{-۴}$ | ۶ |
| ESFAS-2 | ۱/۵۹۴× ۱۰$^{-۴}$ | ۶ |
| ESFAS-3 | ۱/۵۹۴× ۱۰$^{-۴}$ | ۶ |
| ESFAS-4 | ۱/۵۹۴× ۱۰$^{-۴}$ | ۶ |
| ESFIP | ۳/۲۴۷× ۱۰$^{-۳}$ | ۱۷ |
| ESFIP-CH1 | ۳/۲۴۷× ۱۰$^{-۳}$ | ۱۷ |
| ESFIP-CH2 | ۳/۲۴۷× ۱۰$^{-۳}$ | ۱۷ |
| ESFIP-CH3 | ۳/۲۴۷× ۱۰$^{-۳}$ | ۱۷ |
| ESFIP-CH4 | ۳/۲۴۷× ۱۰$^{-۳}$ | ۱۷ |
| FAILURE-OF-I&C | ۵/۵۹۵× ۱۰$^{-۳}$ | ۱۸۲ |
| HEPS1 | ۴/۰۰۷× ۱۰$^{-۴}$ | ۳ |
| HEPS2 | ۴/۰۰۷× ۱۰$^{-۴}$ | ۳ |
| HEPS3 | ۴/۰۰۷× ۱۰$^{-۴}$ | ۳ |
| LV-ASSEMBLE-UNIT-400V | ۸/۳۷۶× ۱۰$^{-۵}$ | ۶ |
| NORMAL-RCD-CHANNEL | ۷/۰۵۳× ۱۰$^{-۴}$ | ۱۱ |
| PART-OF-ECR | ۲/۵۱۰× ۱۰$^{-۳}$ | ۳۱ |
| PART-OF-ECR-CV | ۱۰$^{-۳}$ | ۲۷ |
| PART-OF-ECR-OF-EMC | ۲/۵۱۲× ۱۰$^{-۳}$ | ۲۸ |
| PART-OF-MCR | ۲/۴۹۰× ۱۰$^{-۳}$ | ۲۹ |
| PART-OF-MCR-CV | ۲/۴۹۷× ۱۰$^{-۳}$ | ۲۶ |
| PART-OF-MCR-OF-EMC | ۲/۱۷۵× ۱۰$^{-۳}$ | ۳۴ |
| PPPE-SLPE-1 | ۲/۷۲۵× ۱۰$^{-۳}$ | ۸ |
| PPPE-SLPE-2 | ۲/۷۲۵× ۱۰$^{-۳}$ | ۸ |
| PPPE-SLPE-3 | ۲/۷۲۵× ۱۰$^{-۳}$ | ۸ |
| PPPE-SPD1 | ۱/۴۰۲× ۱۰$^{-۳}$ | ۵ |
| PPPE-SPD2 | ۱/۴۰۲× ۱۰$^{-۳}$ | ۵ |
| PPPE-SPD3 | ۱/۴۰۲× ۱۰$^{-۳}$ | ۵ |
| PRESSURE-CONTROL | ۸/۴۱۸× ۱۰$^{-۴}$ | ۱۱ |
| RCD | ۲/۳۵۵× ۱۰$^{-۳}$ | ۱۶۵ |
| SLPE-SPD1 | ۶/۵۶۷× ۱۰$^{-۴}$ | ۵ |
| SLPE-SPD2 | ۶/۵۶۷× ۱۰$^{-۴}$ | ۵ |
| SLPE-SPD3 | ۶/۵۶۷× ۱۰$^{-۴}$ | ۵ |
| STANDARD-CONTROL-CHANNEL | ۲/۵۴۶× ۱۰$^{-۲}$ | ۱۳ |
| SWITCHGEAR-400V | ۶/۷۸۷× ۱۰$^{-۴}$ | ۸ |
| TEMPRATURE-CONTROL | ۱/۴۳۴× ۱۰$^{-۳}$ | ۱۳ |
| TERMOCOUPLES | ۴/۹۳۱× ۱۰$^{-۴}$ | ۴ |
| TPTS-1322 | ۱/۴۹۳× ۱۰$^{-۴}$ | ۴ |
| TPTS-1332 | ۱/۴۹۳× ۱۰$^{-۴}$ | ۴ |
| TPTS-1411 | ۱/۴۹۳× ۱۰$^{-۴}$ | ۴ |
| TPTS-1703 | ۱/۴۹۳× ۱۰$^{-۴}$ | ۴ |
| TPTS-1717 | ۱/۴۹۳× ۱۰$^{-۴}$ | ۴ |
| TPTS-1717-01 | ۱/۴۹۳× ۱۰$^{-۴}$ | ۴ |
| TPTS-1722 | ۱/۴۹۳× ۱۰$^{-۴}$ | ۴ |
| TPTS-1723 | ۱/۴۹۳× ۱۰$^{-۴}$ | ۴ |
| TPTS-1731 | ۱/۴۹۳× ۱۰$^{-۴}$ | ۴ |
| TPTS-52-FOR-RCD | ۱/۱۲۸× ۱۰$^{-۵}$ | ۲ |
| TPTS-53-FOR-RCD | ۲/۹۶۸× ۱۰$^{-۴}$ | ۴ |
| TPTS-NORMAL-RCD-CHANNEL | ۲/۶۲۲× ۱۰$^{-۴}$ | ۶ |
| TPTS-PRESSURE-CONTROL | ۲/۶۲۲× ۱۰$^{-۴}$ | ۶ |
| TPTS-STANDARD-CONTROL-CH | ۲/۶۲۲× ۱۰$^{-۴}$ | ۶ |
| TPTS-TEMPRATURE-CONTROL | ۲/۶۲۲× ۱۰$^{-۴}$ | ۶ |
| TPTS53-2082-EMC | ۲/۲۲۰× ۱۰$^{-۴}$ | ۸ |
| UDU03 | ۶/۷۹۲× ۱۰$^{-۵}$ | ۹ |
| UDU03-ECR | ۷/۶۰۸× ۱۰$^{-۵}$ | ۱۰ |
| UDU03-ECR-CV | ۶/۶۴۸× ۱۰$^{-۵}$ | ۶ |
| UDU03-ECR-EMC | ۶/۶۴۸× ۱۰$^{-۵}$ | ۶ |
| UDU03-MCR-CV | ۶/۳۱۲× ۱۰$^{-۵}$ | ۶ |
| UDU03-MCR-EMC | ۶/۳۱۲× ۱۰$^{-۵}$ | ۶ |
| VALVE-ACTUATOR | ۷/۹۶۸× ۱۰$^{-۵}$ | ۷ |

می توان با جایگذاری داده های مخصوص به هر نیروگاه اتمی VVER-1000 این تحلیل درخت خطا را مختص آن نیروگاه انجام داد.

## نتیجه‌گیری و جمع‌بندی

سیستم I&C نیروگاه اتمی VVER-1000 در واقع از بخش‌های ESFAS و ESFIP و RCD تشکیل شده است که در مقاله حاضر به بررسی قابلیت اطمینان این بخش‌ها پرداخته شده است. این بخش‌ها خود به بخش‌های زیر تقسیم می‌شود:

- دریافت اطلاعات؛
- پردازش اطلاعات؛
- صدور دستورات لازم.

در این مقاله مطابق بلوک دیاگرام‌های آمده در شکل‌های ۵، ۶، ۷ و ۸ و با استفاده از نرم‌افزار SAPHIRE 7 درخت خطای این زیرسیستم‌ها ترسیم شده است. لازم به ذکر است در کل مقاله تعداد ۶۹ درخت خطا ترسیم گردیده است. سپس با استفاده از داده‌های جنریک [۸] قابلیت اطمینان هر کدام محاسبه که نتایج آنها در جدول ۲ ارائه شده است.

## فهرست علائم

| | |
|---|---|
| TLS-U | سیستم سطح بالای واحد قدرت |
| I&C | کنترل و ابزاردقیق |
| RF | فرکانس رادیویی |
| ESFIP | بخش آغازگر ویژگی مهندسی‌شده ایمنی |
| ESFAS | سیستم فعال‌سازی ویژگی مهندسی‌شده ایمنی |
| RCD | دستگاه کنترل از راه دور |
| CPS-ESFIP | سیستم کنترل و حفاظت ویژگی‌های مهندسی‌شده ایمنی |
| FT | درخت خطا |
| FTA | آنالیز درخت خطا |
| FMEA | تجزیه و تحلیل مودهای خرابی و اثرات آن‌ها |
| IE | رویداد آغازگر |
| BE | رویداد پایه |
| TPTS | مجموعه سخت افزار و نرم افزار |
| ECR | اتاق کنترل اضطراری |
| MCR | اتاق کنترل اصلی |

## مراجع

[1] Atomenergoproekt, "Bushehr NPP Probabilistic Safety Assessment, level 1", revision 3, State research, 2003.
[2] IAEA, *Safety of Nuclear Power Plants*, Safety Standards Series No. NS-R-1, 2000.
[3] W. Boyes, *Instrumentation reference book*, Butterworth-Heinemann, 2009.
[4] A. S. Shirani, S. A. Hosseini, M. Zangian and S. Kord Alivand, "*Feasibility of using dynamic probability assessment method of safety in nuclear power plants and a review of the work done in this field*," 5th International Reliability and Safety Engineering Conference (IRSEC2018), 2018.
[5] Final Safety Assurance Report BNPP-1, CHAPTER 7 INSPECTION AND CONTROL SYSTEMS (I&A), Revision-1, 2007.
[6] S. Kwag, and J. Oh, "*Development of network-based probabilistic safety assessment: A tool for risk analyst for nuclear facilities*," Progress in Nuclear Energy, Vol. 110, pp. 178-190, 2019.
[7] K.J. Kvarfordt, S.T. Wood, and C.L. Smith, "Systems Analysis Programs for Hands-On Integrated Reliability Evaluations (SAPHIRE) Code Reference Manual," *U.S. Department of Energy*, Idaho National Laboratory, 2006.
[8] IAEA, "*COMPONENT RELIABILITY DATA FOR USE IN PROBABILISTIC SAFETY ASSESSMENT*," IAEA-TECDOC-478, 1988.