تأثیر طراحی و نوع معماری افزونگی بر ایجاد تعادل میان دستیابی به سطح یکپارچگی ایمنی هدف و دسترس‌پذیری عملیاتی در سیستم‌های ابزار دقیق ایمنی(SIS)

ویژه صنایع راهبردی نفت، گاز و پتروشیمی

رضا عباسی لرکی

بازرس فنی - شرکت پتروشیمی امیرکبیر

abbasilarkireza@yahoo.com

چکیده :

سیستم‌های ابزار دقیق ایمنی (Safety Instrumented Systems – SIS) به‌عنوان یک لایه حفاظتی مستقل (Independent Protection Layer – IPL)، از ارکان اصلی مدیریت ایمنی فرآیند بوده و با هدف حفاظت از انسان، محیط زیست و دارایی‌های فیزیکی طراحی و پیاده‌سازی می‌شوند. هر SIS شامل یک یا چند تابع ابزار دقیق ایمنی (Safety Instrumented Function – SIF) است که به‌منظور پیشگیری از وقوع رویداد آغازگر در سناریوهای خطرناک مشخص و کاهش ریسک تا سطح قابل‌تحمل سازمان طراحی و اجرا می‌گردد. این توابع با پایش و نظارت مداوم بر پارامترهای فرآیندی، در صورت بروز تقاضا (تشخیص رویداد آغازگر)، عمل نموده و به‌صورت خودکار فرآیند را به وضعیت ایمن از پیش تعیین‌شده می رسانند .

در فرآیند طراحی، برای هر SIF بر اساس میزان کاهش ریسک موردنیاز و نتایج روش‌های تحلیل و ارزیابی نظیرLOPA ، سطح یکپارچگی ایمنی (Safety Integrity Level – SIL)تخصیص داده می‌شود و از آنجا که در اغلب صنایع فرآیندی، توابع ابزاردقیق ایمنی در حالت تقاضای کم (Low Demand Mode)عمل می کنند , احتمال خرابی در صورت تقاضا (Probability of Failure on Demand – PFD) به‌عنوان شاخص اصلی ارزیابی عملکرد ایمن آنها به‌کار می‌رود. شاخصی که بیانگر احتمال عدم عملکرد صحیح و به‌موقع تابع ایمنی در زمان لازم(تقاضا) است.

در مقابل، فعال‌سازی ناخواسته توابع ابزار دقیق ایمنی در غیاب تقاضای واقعی فرآیندی که به‌عنوان توقف کاذب (Spurious Trip) شناخته می‌شود , یکی از چالش‌های اساسی در طراحی و بهره‌برداری از سیستم‌های ابزار دقیق ایمنی محسوب می‌گردد. این پدیده می‌تواند ناشی از تقاضای کاذب (False Demand)یا بروز خرابی در اجزای مرتبط با تابع ابزار دقیق ایمنی باشد و پیامدهایی نظیر خاموشی‌های برنامه‌ریزی‌نشده، کاهش دسترس‌پذیری سیستم و افزایش هزینه‌های عملیاتی را به همراه داشته باشد.

ازاینرو، مدیریت مؤثر چرخه عمر ایمن سیستم های ابزاردقیق ایمنی , مستلزم ایجاد تعادل مهندسی میان حفظ سطح یکپارچگی ایمنی (SIL) از طریق کاهش احتمال خرابی در صورت تقاضا (PFD) و کنترل نرخ توقفات کاذب (STR) است , چراکه تمرکز صرف بر افزایش سطح یکپارچگی ایمنی SIL ، بدون توجه به اثرات آن بر نرخ توقفات کاذب ، می‌تواند به کاهش قابلیت اطمینان و کارایی عملیاتی سیستم ابزاردقیق ایمنی منجر شود .

کلمات کلیدی:

-سیستم ابزار دقیق ایمنی (SIS) - تابع ابزار دقیق ایمنی (SIF) -سطح یکپارچگی ایمنی(SIL) - احتمال خرابی در صورت تقاضا (PFD)-نرخ توقف کاذب (STR) -دسترس‌پذیری عملیاتی -معماری افزونگی -ترتیب رای گیری (voting) -خرابی‌های تصادفی سخت‌افزاری -خرابی‌های سیستماتیک -خرابی‌های با علت مشترک(CCF)

مقدمه :

در طراحی سیستم‌های ابزار دقیق ایمنی(Safety Instrumented Systems – SIS) ، انتخاب نوع معماری افزونگی و ترتیب رأی‌گیری مناسب با کاهش احتمال خرابی در صورت تقاضا (PFDavg) , نقش تعیین‌کننده‌ای در دستیابی به سطح یکپارچگی ایمنی (SIL) هدف دارد و از طرق دیگر نوع افزونگی با تاثیر بر نرخ خرابی های ایمن و خرابی ها با علل مشترک تاثیر مستقیمی بر نرخ توقفات کاذب (Spurious Trip Rate – STR) دارد.

از آنجا که عملکرد ایمن و دسترس‌پذیری توابع ابزار دقیق ایمنی (Safety Instrumented Function – SIF) تحت تأثیر دو نوع خرابی شامل , خرابی‌های تصادفی سخت‌افزاری و خرابی‌های سیستماتیک قرار می گیرد.در نتیجه انتخاب تجهیزات با نرخ خرابی تصادفی پایین، حذف یا کاهش عوامل سیستماتیک و نیز استفاده از معماری افزونگی مناسب ، هم عملکرد ایمن SIF ها را تضمین می‌کند و هم از افزایش توقفات ناخواسته جلوگیری می‌نماید. دستیابی همزمان به سطح یکپارچگی ایمنی هدف و دسترس‌پذیری بهینه , مستلزم هماهنگی میان طراحی، مدیریت خرابی‌ها و علل سیستماتیک تاثیر گذار بر آنها است.

بنابراین، ایجاد تعادل میان حفظ سطح یکپارچگی ایمنی هدف (SIL) و کنترل نرخ توقفات کاذب(STR) ، نقشی اساسی در تضمین دسترس‌پذیری سیستم و حفظ قابلیت اطمینان عملیاتی دارد. این موضوع یکی از چالش‌های اصلی در مدیریت چرخه عمر سیستم‌های ابزار دقیق ایمنی (SIS) محسوب می‌شود و نیازمند تصمیم‌گیری‌های فنی آگاهانه در مراحل طراحی، بهره‌برداری، تست و رویه های نگهداشت توابع ابزار دقیق ایمنی است.

ازاینرو، با توجه به اینکه بخش قابل‌توجهی از علل سیستماتیک در مرحله طراحی از چرخه عمر ایمنی سیستم‌های ابزار دقیق ایمنی به آن تحمیل می‌شود، انتخاب نامناسب معماری افزونگی بدون درنظرگرفتن هم‌زمان الزامات ایمنی عملکردی و دسترس‌پذیری عملیاتی می‌تواند پیامدهای نامطلوبی به همراه داشته باشد. چنین رویکردی از یک‌سو منجر به افزایش احتمال خرابی در صورت تقاضا و تضعیف سطح یکپارچگی ایمنی می‌شود و از سوی دیگر با افزایش نرخ توقفات کاذب، قابلیت اطمینان عملیاتی و تداوم تولید را تحت تأثیر قرار می‌دهد.

بر این اساس، در این پژوهش به‌طور خاص تأثیر نوع معماری افزونگی بر میزان احتمال خرابی در صورت تقاضا (دستیابی به SIL هدف) و نرخ توقفات کاذب در توابع ابزار دقیق ایمنی مورد بررسی و تحلیل قرار می‌گیرد.

1-مفاهیم پایه :

۱-۱ مفهوم افزونگی و ترتیب رای گیری :

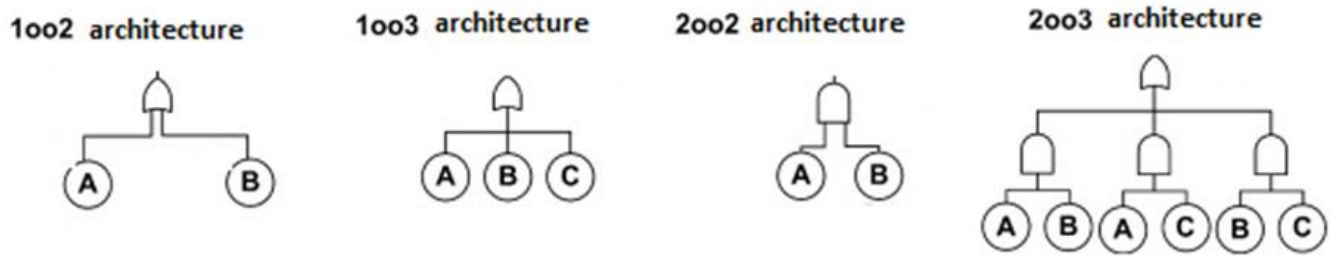
افزونگی سخت‌افزاری در سیستم‌های ابزار دقیق ایمنی (SIS) عبارت است از استفاده از چند مسیر مستقل برای اجرای یک تابع ابزار دقیق ایمنی (SIF) به منظور تضمین عملکرد ایمن در صورت خرابی یک مسیر است . این طراحی افزونه در صورتی که منجر به کاهش نرخ خرابی های خطرناک پنهان شود , باعث کاهش احتمال خرابی در صورت تقاضا (PFD) و ارتقاء سطح یکپارچگی ایمنی (SIL) می‌شود. همچنین نوع معماری افزونگی ، تأثیر مستقیم بر نرخ توقفات کاذب (Spurious Trip Rate – STR) دارد؛ زیرا فعال‌سازی ناخواسته توابع SIF به نرخ خرابی های ایمن , نوع و میزان استقلال مسیرهای افزونه بستگی دارد.

جهت اثربخشی واقعی، مسیرهای افزونه باید از نظر سخت‌افزاری مستقل و ترجیحاً متنوع باشند تا اثر خرابی‌های سیستماتیک و خرابی‌های با علت مشترک (CCF) به حداقل برسد. از اینرو نگهداشت مؤثر و تست‌های دوره‌ای (Proof Testing) نقش کلیدی در حفظ عملکرد ایمن و کنترل STR دارند .

ترتیب رای گیری با الگوی N-out-of-M (NOOM) تعریف می‌گردد به این معنی که از Mتجهیز مورد استفاده در معماری افزونگی ، حداقل N تجهیز باید سالم(بدون خرابی خطرناک) و در دسترس باشند تا عملکرد ایمن تضمین شود .

تفسیر عملکردیNOOM : از منظر عملکردی، الگوی NOOM نشان می‌دهد که جهت فعال شدن (عملکرد ایمن) یک تابع ابزاردقیق ایمنی ، چه تعداد از تجهیزات موجود باید شرایط ناایمن را تشخیص داده و آن را تأیید کنند. به عبارت دیگر در ترتیب رای گیری NOOM حرف N تعداد تجهیزات رای دهنده و حرف دوم M تعداد کل تجهیزات شرکت کننده در معماری افزونگی است , بنابراین جهت فعال شدن تابع ابزاردقیق مورد نظر نیاز به تایید N تجهیز از مجموع M تجهیز موجود می باشد.

متداولترین معماری های افزونگی به صورت زیر می باشد:

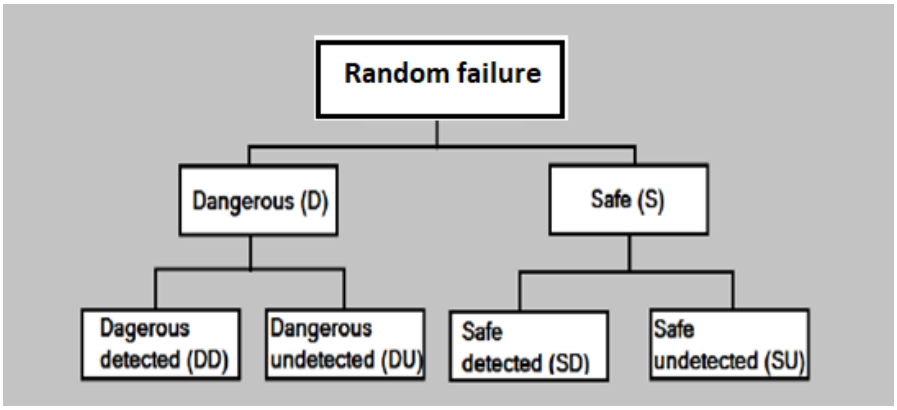


2-۱خرابی‌های تصادفی و سیستماتیک در سیستم‌های ابزار دقیق ایمنی(SIS) :

در سیستم‌های ابزار دقیق ایمنی(SIS) ، عملکرد ایمن توابع ابزار دقیق ایمنی (SIF) تحت تأثیر دو نوع خرابی قرار دارد:

الف- خرابی‌های تصادفی سخت‌افزاری : این نوع خرابی ناشی از فرسودگی، خوردگی یا نقص ذاتی قطعات هستند و زمان وقوع آن‌ها غیرقابل پیش‌بینی است. این خرابی‌ها با نرخ λ مدل شده و در محاسبات شاخص‌هایی نظیر PFDavgو تأیید سطح یکپارچگی ایمنی (SIL) لحاظ می‌شوند. ضمنا کنترل این نوع خرابی از طریق انتخاب معماری افزونگی مناسب، تست‌های دوره‌ای و رویه های صحیح نگهداشت پیشگیرانه میسر می گردد.

انواع خرابی های تصادفی سخت افزاری :



ب-خرابی‌های سیستماتیک :ناشی از خطاهای طراحی، مهندسی، نصب، راه‌اندازی یا بهره‌برداری هستند که می‌توانند منجر به خرابی‌های با علت مشترک (CCF) شوند. این نوع خرابی برخلاف خرابی های تصادفی سخت افزاری با داده های آماری قابل کمی سازیی نیست و کنترل آن‌ها با رعایت اصول طراحی مستقل و متنوع، اجرای کامل چرخه عمر ایمنی و استفاده از تجهیزات با قابلیت سیستماتیک (SC) امکان‌پذیر است.

اگرچه خرابی‌های سیستماتیک به‌طور مستقیم وارد محاسبات کمی ایمنی نمی‌شوند، اما اثر آن‌ها بر عملکرد معماری‌های افزونگی با به‌صورت غیرمستقیم و محافظه‌کارانه در تحلیل‌های ایمنی لحاظ می‌گردد. در این راستا، استاندارد IEC 61508-6 استفاده از مدل فاکتور β را برای در نظر گرفتن اثر خرابی‌های با علت مشترک توصیه می‌کند. این مدل، سهم خرابی‌های هم‌زمان ناشی از علل مشترک را از میان خرابی‌های تصادفی خطرناک پنهان جدا کرده و امکان ارزیابی واقع‌بینانه‌تری از عملکرد سیستم‌های افزونه را فراهم می‌سازد، بدون آن‌که اصل غیرقابل کمّی‌سازی بودن خرابی‌های سیستماتیک نقض شود.

در نهایت، دستیابی به سطح یکپارچگی ایمنی مورد نظر (SIL) مستلزم توجه هم‌زمان به هر دو جنبه خرابی‌های تصادفی و سیستماتیک است؛ به‌گونه‌ای که در محاسبات کمی سطح یکپارچگی ایمنی با لحاظ نمودن عواملی مانند :رعایت الزامات قابلیت سیستماتیک، استقلال اجزا و اجرای کامل چرخه عمر ایمنی تکمیل شده تا از بی‌اثر شدن افزونگی در برابر نقص های سیستماتیک , جلوگیری گردد .

توجه گردد در یک سیستم ابزار دقیق ایمنی که برای اولین بار به بهره‌برداری می‌رسد و فرآیند اعتبارسنجی (Validation) آن به طور کامل انجام شده باشد ، به معنی حذف کامل خرابی‌های سیستماتیک نمی‌باشد. بخشی از خرابی‌های سیستماتیک می‌تواند ناشی از خطاهای انسانی در تعیین مشخصه الزامات ایمنی , طراحی، مهندسی سخت‌افزار و نرم‌افزار، ساخت، پیاده‌سازی و نصب بوده که به صورت بالقوه در سیستم وجود داشته و باقی بماند .

این خرابی‌ها معمولاً به صورت خطاهای نهفته در سیستم وجود دارد و در صورت وقوع شرایط عملیاتی، محیطی یا منطقی خاص می‌توانند بروز یافته و به خرابی های بالفعل منجر شوند.

علاوه بر این، خرابی‌های سیستماتیک می‌توانند در فاز بهره‌برداری و نگهداشت از چرخه عمر نیز در اثر رویه‌های عملیاتی و نگهداشت نادرست , تغییرات کنترل‌نشده و یا استفاده خارج از محدوده طراحی به سیستم تحمیل شوند.

بنابراین، مطابق با استانداردهای IEC 61508 و IEC 61511 ، مدیریت و کاهش خرابی‌های سیستماتیک مستلزم به‌کارگیری اقدامات پیشگیرانه، کنترلی و مدیریتی در کل چرخه عمر ایمنی سیستم های SIS می‌باشد.

1-3 مفاهیم خرابی‌های با علت مشترک و فاکتور β در سیستم‌های ابزار دقیق ایمنی (SIS) :

در سیستم‌های ابزار دقیق ایمنی(SIS) ، خرابی‌های تصادفی سخت‌افزاری می‌توانند تحت تأثیر یک علت مشترک، عملکرد چند جزء در معماری افزونگی را به طور هم‌زمان مختل کنند .مدل فاکتور(Beta Factor) β ، معرفی‌شده توسط Fleming (1975) و مورد استفاده در IEC 61508-6 ، سهم خرابی‌های هم‌زمان ناشی از علل مشترک را در محاسبات کمی به‌صورت محافظه‌کارانه ای در نظر می‌گیرد.

برای یک تابع ابزاردقیق ایمنی با M جزء موازی:

از اینرو در لحاظ نمودن اثر خرابی ها با علت مشترک (فاکتورβ) می توان نرخ خرابی های پنهان خطرناک را برای هر تجهیز که در معماری افزونگی استفاده گردیده را به صورت زیر بیان نمود:

$$\lambda_{CCF} = \beta \times \lambda$$

و

$$\lambda = \lambda_{ccf} + \lambda_{independent} = \beta\,\lambda + (1-\beta)\,\lambda$$

به عنوان مثال در معماری افزونگی 1OO2 با در نظر گرفتن اثر خرابی ها با علت مشترک (فاکتورβ) میزان $PFD_{(1OO2)}$ به صورت زیر اصلاح می گردد:

$$PFD_{(1OO2)} = \beta\, PFD_{single} + (1-\beta).\,(PFD_{single})^2$$

که در آن:

- λ : نرخ خرابی تصادفی سخت‌افزاری هر جزء
- λCCF : نرخ خرابی ناشی از علت مشترک
- $\lambda_{independent}$: نرخ خرابی مستقل
- β: کسری از خرابی‌هایی است که بیش از یک جزء را تحت تأثیر قرار می‌دهد
- PFDsingle : احتمال خرابی در صورت تقاضا برای هر تجهیز منفرد است.

فاکتور β صرفاً برای خرابی‌های تصادفی سخت‌افزاری کاربرد دارد و نه برای خرابی‌های سیستماتیک. با این حال، خرابی‌های سیستماتیک می‌توانند منشأ خرابی‌های با علت مشترک (CCF) شوند، به‌ویژه زمانی که نقص‌های مشابه در طراحی، نصب یا بهره‌برداری چند کانال را هم‌زمان تحت تأثیر قرار دهند. کاهش خرابی‌های سیستماتیک از طریق رعایت اصول استقلال، تنوع و انتخاب تجهیزات با قابلیت سیستماتیک(SC) ، به کاهش CCF و در نتیجه کاهش نرخ توقفات کاذب (STR) کمک می‌کند.

گام‌های کمی‌سازی CCF بر اساس: IEC 61508-6 Annex D

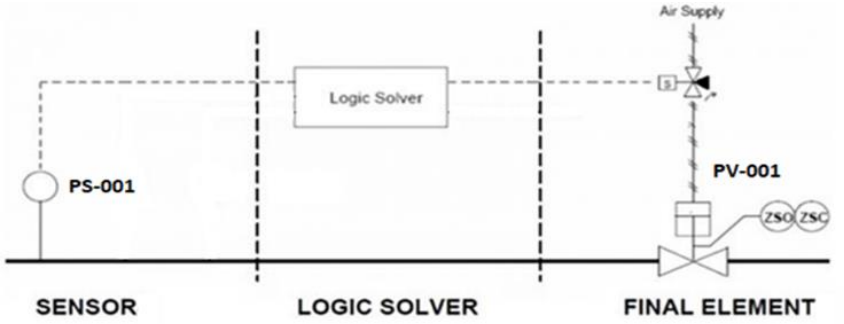
۱. تفکیک SIF به زیرسیستم‌ها :سنسورها، پردازشگر منطقی و عناصر نهایی
۲. شناسایی عوامل مؤثر بر CCF :ارزیابی کیفی طراحی، نصب و نگهداشت
۳. امتیازدهی به معیارها :تعیین سطح کنترل خرابی‌های علت مشترک
٤. محاسبه امتیاز کل (Total Score) :شاخص بلوغ مهندسی و کنترلCCF
٥. تبدیل Score به βint: کسری از خرابی‌های تصادفی اختصاص‌یافته بهCCF

٦. تعدیل βint بر اساس معماری افزونه :با توجه به نوع افزونگی و ترتیب رأی‌گیری، βنهایی محاسبه می‌شود
پس از تعیین β نهایی، نرخ خرابی با علت مشترک برای هر زیرسیستم به‌صورت زیر به‌دست می‌آید:

$$\lambda_{CCF} = \beta \times \lambda$$

این روش امکان ارزیابی کمی واقع‌بینانه از تأثیر CCF بر PFDو STRدر معماری‌های افزونگی را فراهم می‌کند و تضمین می‌کند که افزونگی سخت‌افزاری به‌درستی در برابر خرابی‌های علت مشترک عمل نماید.
نکته : توجه گردد مقادیر PFD و STR برای هر زیر سیستم از یک تابع ابزاردقیق ایمنی تعیین می شود به طوری که برای هر تابع ابزاردقیق ایمنی . این زیرسیستم‌ها شامل موارد زیر هستند:

- **سنسورها(Sensors)**
- **پردازشگر منطقی(Logic Solver)**
- **عناصر نهایی(Final Elements)**



safety instrumented function(SIF)

۲- سطح یکپارچگی ایمنی(SIL) و ارتباط آن با میزان احتمال خرابی در صورت تقاضا:

سطح یکپارچگی ایمنی توابع ابزار دقیق ایمنی در مرحله تحلیل خطر و ارزیابی ریسک از چرخه عمر ایمنی(Safety Lifecycle) ، پس از شناسایی مخاطرات فرآیندی و تحلیل پیامدهای آن‌ها، تعیین می‌شود.
در این فرآیند، پس از شناسایی سناریوهای خطرناک و برآورد ریسک ذاتی(Initial Risk) ، میزان اثربخشی، قابلیت اطمینان و استقلال لایه‌های حفاظتی موجود در کاهش ریسک ناشی از هر سناریوی خاص مورد بررسی و اعتبارسنجی قرار می‌گیرد. سپس ریسک باقی‌مانده (Residual Risk) محاسبه شده و با معیار ریسک قابل تحمل (Tolerable Risk) مقایسه می‌شود.
در صورتی که ریسک باقی‌مانده بیش از سطح قابل تحمل تشخیص داده شود، نیاز به کاهش ریسک مضاعف مطرح می‌گردد. در این حالت، بر اساس میزان کاهش ریسک لازم و سطح عملکرد مورد انتظار از تابع ابزار دقیق ایمنی، سطح یکپارچگی ایمنی (SIL) مورد نیاز برای یک تابع ابزاردقیق ایمنی (SIF) تعیین و مستند می‌شود.
صنایع فرآیندی مانند نفت , گاز و پتروشیمی نمونه بارزی از حالت کار با تقاضای کم (Low Demand Mode) می باشد ، در این حالت، احتمال خرابی در صورت تقاضا (PFD) معیار اصلی و کمی برای ارزیابی عملکرد ایمن , توابع ابزاردقیق ایمنی (SIF) و تعیین

سطح یکپارچگی ایمنی (SIL) می باشد. این شاخص احتمال خرابی و یا عدم عملکرد صحیح و به موقع لایه حفاظتی در زمانی که به عملکرد ایمن آن نیاز است را نشان می‌دهد.

SIL for Low Demand Mode	
Safety Integrity Level (SIL)	**Average probability of a dangerous failure on demand of the safety function (PFD_{avg})**
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

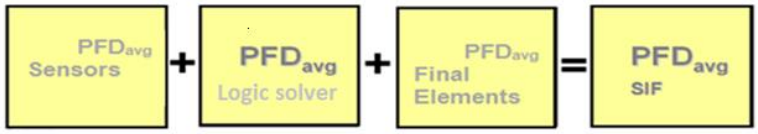
بنابراین با در نظر گرفتن فاصله زمانی مابین تست های دوره ای اثبات و نرخ خرابی های خطرناک شناسایی نشده می توان متوسط احتمال خرابی در صورت تقاضا را جهت یک تابع ابزار دقیق ایمنی به شرح زیر بدست آورد:

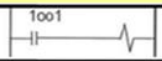
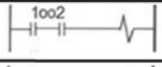
$$PFDavg \propto \lambda du * T$$

λdu = Dangerous undetected Failure Rate (نرخ خرابی های خطرناک شناسایی نشده)

T = Proof Test Interval (فاصله زمانی مابین تست های اثبات عملکرد)

در زیر تاثیر نوع افزونگی بر میزان احتمال خرابی در صورت تقاضا نشان داده شده است :



ترتیب رای گیری MOON	(PFDavg)	معماری
1oo1	$\lambda_{du} * T/2$	
1oo2	$\frac{(\lambda_{du})^2 * T^2}{3}$	
2oo2	$\lambda_{du} * T$	
2oo3	$(\lambda_{du})^2 * T^2$	

توجه گردد در این بخش روابط ارائه شده جهت محاسبه احتمال خرابی درصورت تقاضا (PFD_{AVG})براساس نوع معماری افزونگی , به صورت ایده آل و بدون در نظر گرفتن اثر خرابی ها با علت مشترک (CCF) می باشد. توجه گردد شاخص PFDavg تنها نماینده سهم خرابی‌های تصادفی سخت‌افزاری است و خرابی‌های علت مشترک به‌عنوان زیرمجموعه‌ای از این دسته خرابی‌ها در نظر گرفته شده و با استفاده از مدل فاکتور β در محاسبات وارد می‌شود.

اما اگرچه β یک پارامتر کمی در مدل تصادفی است ولی مقداردهی آن مبتنی بر ارزیابی کیفی عوامل سیستماتیک انجام می‌شود.(در محاسبات , فاکتور βدر بازه $0< \beta \leq 1$ قرار می گیرد که $\lim \beta \to 0$ به طور ایده آل به معنی حذف تمامی عواملی است که منجر به خرابی باعلل مشترک می گردد و نهایتا باعث دستیابی به بالاترین سطح SIL و در دسترس پذیری خواهد شد , در

مقابل با افزایش مقدارβ ، سهم غالب PFD به خرابی‌های علت مشترک اختصاص یافته و اثربخشی افزونگی کاهش می‌یابد؛ به‌طوری‌که در حالت حدی$\beta=1$ ، رفتار سیستم افزونه معادل یک تجهیز منفرد خواهد بود.

از اینرو در لحاظ نمودن اثر خرابی ها با علت مشترک (فاکتورβ) می توان نرخ خرابی های پنهان خطرناک برای هر تجهیز را به صورت زیر بیان نمود:

$$\lambda du = \lambda_{ccf} + \lambda_{independent} = \beta\, \lambda du + (1-\beta)\, \lambda du$$

به عنوان مثال در معماری افزونگی 1OO2 با در نظر گرفتن اثر خرابی ها با علت مشترک (فاکتورβ) میزان $PFD_{(1OO2)}$به صورت زیر اصلاح می گردد:

$$PFD_{(1OO2)} = \beta\, PFD_{single} + (1-\beta).\, (PFD_{single})^2$$

PFD_{single} میزان احتمال خرابی در صورت تقاضا برای هر تجهیز منفرد است.

بدین ترتیب، استاندارد IEC 61508-6 با رویکردی منسجم و محافظه‌کارانه، ارتباط میان خرابی‌های تصادفی، خرابی‌های علت مشترک و ملاحظات سیستماتیک را در تحلیل قابلیت اطمینان توابع ابزار دقیق ایمنی برقرار می‌کند , بدون آنکه ماهیت غیرتصادفی خرابی‌های سیستماتیک نقض شود.

۳- مفاهیم تقاضای کاذب و نرخ توقفات کاذب (ایمن) :

تقاضای کاذب (False Demand) به شرایطی اطلاق می‌شود که در آن سیستم ابزاردقیق ایمنی (SIS) ، در پاسخ به داده ایی نادرست یا تفسیر اشتباه از شرایط واقعی، به اشتباه تصور می‌کند که یک وضعیت خطرناک رخ داده و به تبع آن تابع ابزاردقیق ایمنی را فعال می‌سازد که منجر به خاموشی کامل یا بخشی از فرآیند می شود.

به عبارت دیگر در توقف کاذب، سیستم به اشتباه تصور می‌کند که شرایطی خطرناک بوجود آمده و با عملکرد ایمن , اقدام به توقف یا Shutdown فرآیند می نماید، در حالی که شرایط کاملاً ایمن بوده است . به‌عنوان مثال، بازتاب نور خورشید که توسط یک آشکارساز شعله به اشتباه به عنوان شعله آتش شناسایی می شود، می‌تواند باعث فعال شدن نابه‌جای SIF و توقف کل فرآیند گردد. همچنین براساس استاندارد IEC 61511 ، در شرایطی که سطح تحمل خرابی برای یک SIF یا اجزای آن لحاظ نشده باشد، بروز خرابی‌های تصادفی ایمن (Safe Failures) منجر به فعال‌سازی ناخواسته تابع ابزاردقیق ایمنی و انتقال فرآیند به وضعیت ایمن می‌شوند. این موضوع ممکن است منجر به خاموشی ناخواسته فرآیند گردد. بر اساس راهنمای ANSI/ISA TR84.00.02 ، این خاموشی‌ها تحت عنوان خاموشی غیرمنتظره فرآیند (Unscheduled Process Shutdown) طبقه‌بندی می‌شوند.

نکته حائز اهمیت آن است که اگرچه یک Spurious Trip ممکن است از دیدگاه یک تابع ابزاردقیق ایمنی خاص، ایمن تلقی گردد، اما این وضعیت می‌تواند در تعامل با سایر توابع ایمنی یا بخش‌های مختلف فرآیند منجر به ایجاد شرایط ناایمن و خطرناک شود.

توقفات کاذب، به ویژه در صنایع حساس مانند نفت، گاز، پتروشیمی و هسته‌ای، نه تنها منجر به زیان‌های مالی گسترده ناشی از توقف تولید می‌شوند، بلکه از منظر ایمنی نیز تهدید محسوب می‌گردند. در این صنایع، دو وضعیت عملیاتی توقف غیرمنتظره فرآیند (Trip)و راه‌اندازی مجدد (Start-Up) جزء پرریسک‌ترین حالات فرآیندی محسوب شده و باید به حداقل ممکن محدود شوند.

نرخ توقفات کاذب (STR) از شاخص های کلیدی قابلیت اطمینان و معیاری است برای سنجش تعداد دفعاتی که یک تابع ابزاردقیق ایمنی (SIF) به صورت ناخواسته و کاذب , در نبود تقاضای واقعی فعال می‌شود و باعث توقف یا خاموشی فرآیند می‌گردد.

اصطلاح نرخ توقفات کاذب یا ایمن (STR) در استاندارد ISA-TR84.00.02 بعنوان سنجشی بر احتمال بروز توقفات نادرست یا کاذب که بدلیل بروز خرابی های ایمن اجزای یک سیستم ابزاردقیق ایمنی ایجاد می گردد ,تعریف می شود .

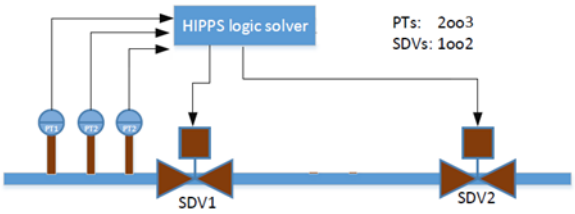
بنابراین طبق تعریف، نرخ توقفات کاذب(ایمن) عبارتست از میزان خرابی های ایمنی (λS) که در طول دوره عملیاتی (زمان بهره برداری به صورت سالیانه) در اجزای یک تابع ابزاردقیق ایمنی می تواند اتفاق بیافتد و منجر به توقفات کاذب گردد.

نکته : STR میزان در دسترس پذیری عملیاتی یک جزء یا یک تابع ابزاردقیق ایمنی را توصیف می نماید و هر چه STR عدد کوچتری باشد , میزان در دسترس بودن یک تابع ابزاردقیق ایمنی بیشتر خواهد بود.

نرخ توقفات کاذب به طور جداگانه برای هر زیر سیستم مربوط به یک تابع ابزاردقیق ایمنی(SIF) شامل : تجهیزات اندازه گیری, پردازشگر های منطقی و عناصر نهایی (شامل محرک ها) به طور جداگانه محاسبه می شود .

بنابراین نرخ توقفات کاذب کلی برای یک تابع ابزاردقیق ایمنی از حاصل جمع جبری STR زیر سیستم ها به دست می آید.

$$STR_{SIF} = \sum STR_{sensor} + \sum STR_{logic\ solver} + \sum STR_{final\ element}$$



$$STR_{SIF} = STR_{PTs} + STR_{LS} + STR_{SDVs}$$

۱-۳- ارتباط نوع معماری افزونگی با نرخ توقفات کاذب و مفاهیم قابلیت اطمینان :

در سیستم‌های ابزار دقیق ایمنی(SIS) ، خرابی‌های تصادفی سخت‌افزاری که منجر به فعال‌سازی ناخواسته توابع ابزاردقیق ایمنی (SIF)و متعاقباً توقف و خاموشی فرآیند یا رساندن آن به وضعیت ایمن از پیش‌تعریف‌شده می‌شوند، اصطلاحاً خرابی‌های ایمن (Safe Failures)نامیده می‌شوند.

اگرچه این نوع خرابی‌ها از منظر کاهش ریسک مطلوب به نظر می‌رسند، اما در واقع می‌توانند منجر به توقفات کاذب (Spurious Trips)شوند که در بسیاری از فرآیندهای حساس ، آثار منفی اقتصادی، عملیاتی و حتی ایمنی قابل‌توجهی به همراه دارند.

بر اساس استاندارد IEC 61511 ، وقوع یک توقف کاذب به دلیل خرابی ایمن، به‌ویژه در مراحل راه‌اندازی مجدد یا خاموشی (Startup / Shutdown)، ممکن است خود منشأ خطرات جدیدی باشد، چرا که بسیاری از حوادث صنعتی در این شرایط رخ می‌دهند. از اینرو، کاهش نرخ توقفات کاذب نه‌تنها جنبه‌ای اقتصادی بلکه جنبه‌های ایمنی را پوشش می دهد.

برای دستیابی همزمان به سطح یکپارچگی ایمنی مورد نظر (SIL) و حداقل‌سازی توقفات ناخواسته، یکی از راهکارهای کلیدی، استفاده از معماری های افزونگی(Redundancy) با ترتیب رای گیری مناسب در طراحی توابع ابزار دقیق ایمنی است. افزونگی به

این معناست که بیش از یک کانال یا یک تجهیز برای نظارت بر یک پارامتر بحرانی به‌کار گرفته شود. در این معماری ها، بروز خرابی های خطرناک در یک تجهیز منفرد منجر به از دست رفتن ایمنی نخواهد شد ، زیرا تجهیزات دیگر همچنان می‌توانند عملکرد ایمن را تضمین نمایند.

در این راستا، منطق رأی‌گیری (Voting Logic) در طراحی افزونه توابع ابزاردقیق ایمنی، تعیین‌کننده نحوه پاسخ سیستم به شرایط ایمن یا خطرناک است. این منطق به‌صورت مدل NooM (N out of M) تعریف می‌شود؛ که در آن بخش اول (N)تعداد تجهیزاتی است که باید "رای" به فعال شدن یک تابع ابزاردقیق ایمنی دهند و در نتیجه می تواند باعث ایجاد توقف و یا وضعیت ایمن گردد و بخش دوم(M) تعداد کل تجهیزات موجود در افزونگی است.

به‌عنوان نمونه، در معماری 2OO3 (دو از سه) از میان سه تجهیز موجود، دست‌کم دو تجهیز باید شرایط خطرناک را تأیید کنند تا منجر به تحریک تابع ابزاردقیق ایمنی شود. این نوع معماری افزونگی موجب افزایش دردسترس پذیری (Availability) و کاهش نرخ توقفات کاذب (Spurious Trip Rate - STR) می‌گردد؛ به عنوان مثال ترتیب رای گیری در معماری های افزونه مانند1OO3 (یک از سه) , 1OO2 (یک از دو) یا 1OO1 (یک از یک) حساسیت بالاتری به خرابی‌های ایمن دارند و احتمال توقفات کاذب در آن‌ها بیشتر است، گرچه ممکن است قابلیت تشخیص سریع‌تری نسبت به خطرات واقعی داشته باشند. بنابراین، انتخاب ترتیب رأی‌گیری و نوع افزونگی باید بر مبنای موازنه‌ای مهندسی بین موارد زیر صورت گیرد:

الف-الزامات سطح ایمنی مورد نیاز(SIL)

ب-نرخ خرابی های تصادفی تجهیزات

ج- پیامدهای توقفات کاذب (خطر ایمنی، هزینه ها و...)

د- الزامات بهره‌برداری و شیوه های نگهداشت

۴- مدیریت چرخه عمر ایمنی در ایجاد متعادل میان حفظ سطح یکپارچگی ایمنی و کاهش نرخ توقفات کاذب :

در صنایع فرآیندی مانند نفت، گاز و پتروشیمی ، مدیریت چرخه عمر سیستم‌ها اهمیت ویژه‌ای دارد؛ زیرا مستقیماً بر کاهش ریسک‌های فرآیندی، افزایش قابلیت اطمینان و بهینه‌سازی هزینه‌ها در بلندمدت تأثیر می‌گذارد. سیستم‌های ابزار دقیق ایمنی (SIS) با تبعیت از استانداردهای بین‌المللی نظیر IEC 61508 و IEC 61511 از رویکرد چرخه عمر ایمن (Safety Lifecycle) بهره می‌برند تا تمام فعالیت‌های مرتبط با یکپارچگی ایمنی ، از طراحی مفهومی تا بروزرسانی و یا از رده خارج نمودن آن ، به‌صورت ساختار یافته و کنترل‌شده انجام شود.

این رویکرد تضمین می‌کند که توابع ابزار دقیق ایمنی (SIF) در تمامی مراحل چرخه عمر ، عملکرد مورد انتظار را حفظ کرده و ریسک های فرآیند در محدوده قابل تحمل سازمان باقی می مانند.

یکی از چالش‌های کلیدی در مدیریت چرخه عمر ایمن، ایجاد تعادل میان کاهش نرخ خرابی‌های خطرناک پنهان و به تبع آن حفظ سطح یکپارچگی ایمنی هدف در مقابل کنترل نرخ توقفات کاذب و ناخواسته است.

تمرکز بیش از حد بر کاهش احتمال خرابی در صورت تقاضا (PFD) و کاهش نرخ خرابی های خطرناک پنهان به منظور افزایش سطح یکپارچگی ایمنی منجر به افزایش نرخ توقفات کاذب و به تبع آن کاهش دسترس‌پذیری عملیاتی می‌شود.

در مقابل تمرکز بیش از حد بر کاهش نرخ توقفات کاذب ، بدون در نظر گرفتن معماری مناسب، پوشش تشخیصی و تست های دوره‌ای، می‌تواند احتمال عدم عملکرد ایمن در هنگام تقاضا را افزایش دهد و منجر به نقض سطح یکپارچگی ایمنی مورد انتظار می شود.

بنابراین، ایجاد تعادل میان حفظ سطح یکپارچگی ایمنی و کنترل نرخ توقفات کاذب جهت تضمین دسترس پذیری و قابلیت اطمینان عملیاتی ، یکی از چالش‌های کلیدی در مدیریت چرخه عمر سیستم‌های ابزار دقیق ایمنی (SIS) محسوب می‌شود.

هدف از تعیین SIL آن است که اطمینان حاصل شود تابع ابزاردقیق ایمنی توانایی کاهش احتمال وقوع سناریوی خطرناک تا سطح قابل‌قبول سازمان را دارد . در واقع، SIL نشان‌دهنده‌ی میزان اثر بخشی و اطمینان از عملکرد ایمن SIF در کاهش ریسک تا محدوده قابل‌قبول است. بنابراین هر چه فاصله بین ریسک باقی مانده و ریسک قابل‌قبول بیشتر باشد، سطح بالاتری از SIL موردنیاز خواهد بود .

۵- مقایسه معماری های افزونگی بر مبنای نرخ توقفات کاذبSTR و شاخص PFD :

در طراحی سیستم‌های ابزاردقیق ایمنی(SIS) ، انتخاب نوع افزونگی و ترتیب رأی‌گیری , نقشی اساسی در تعیین سطح یکپارچگی ایمنی(SIL) ، احتمال خرابی در صورت تقاضا (PFDavg) و همچنین نرخ توقفات کاذب (Spurious Trip Rate – STR) دارد. معماری‌های مختلف، مزایا و محدودیت‌های متفاوتی دارند و انتخاب صحیح آن‌ها باید بر اساس الزامات ایمنی، نیاز های فرآیندی و ملاحظات اقتصادی انجام گیرد.

نکته 1 - بر اساس استاندارد6-IEC 61508 ، خرابی‌های علت مشترک در معماری‌های افزونه با استفاده از مدل فاکتور β شبیه سازی می‌شوند. احتمال متوسط خرابی در هنگام تقاضا (PFDavg) برای یک زیرسیستم با معماری افزونگی به‌صورت مجموع سهم خرابی‌های علت مشترک هر یک از تجهیزات شرکت کننده در معماری افزونگی که با $\beta \cdot PFD\_single$ نمایش داده می‌شود و سهم خرابی‌های مستقل، که با $(1-\beta) \cdot (PFD\_single)$ بیان می‌گردد، محاسبه می‌شود. اگرچه فاکتور β در محاسبات بر مبنای نرخ خرابی‌های خطرناک تصادفی سخت‌افزاری اعمال می‌شود، اما مقدار آن بر اساس ارزیابی کیفی عوامل سیستماتیک مانند میزان شباهت در طراحی سخت افزاری ، شرایط نصب و رویه‌های بهره‌برداری و نگهداشت تعیین می‌گردد.

نکته۲- در محاسبه نرخ توقفت کاذب STR براساس نوع افزونگی , همانند آنچه که در مورد تاثیر خرابی ها با علت مشترک بر میزان PFD بیان شد , نرخ توقفت کاذب STR , برای یک زیرسیستم دارای افزونگی به‌صورت مجموع سهم خرابی‌های علت مشترک ، که با $\beta \cdot STR$ یا به عبارت دیگر $\beta \times (\lambda S + \lambda DD)$نمایش داده می‌شود و سهم خرابی‌های مستقل که با $STR_{independent}$بیان می‌گردد محاسبه می‌شود.

بنابراین در معماری افزونگی بیش از 1oo2 با در نظر گرفتن سهم خرابی های مستقل , سهم خرابی ها با علت مشترک و همچنین سهم خرابی های سیستماتیک ایمن , می توان نرخ توقفات کاذب جهت یک معماری افزونگی را به صورت زیر بیان نمود :

$$STR_{(MOON)} = STR_{independent} + \beta \cdot STR + STR_{\text{safety Systematic failure}}$$

نکته : نرخ توقفات کاذب ناشی از خرابی های سیستماتیک ایمن STR safety Systematic failure :

مطابق با رویکرد توصیه‌شده در استاندارد IEC 61511 و راهنمایISA-TR84.00.02 ، این نرخ صرفاً بر اساس داده‌های واقعی بهره‌برداری و از طریق تحلیل رخدادهای ثبت‌شده توقفات کاذب تعیین می‌گردد. در این چارچوب، کلیه توقفات کاذبی که منشأ آن‌ها به خرابی‌های سیستماتیک ایمن نسبت داده می‌شود، در طول یک بازه مشخص بهره‌برداری شناسایی، طبقه‌بندی و ثبت شده و بر مبنای آن‌ها نرخ مربوطه STRSSFاستخراج می‌شود.

الف :ترتیب رای گیری 1oo1 :

ساده‌ترین نوع معماری زیر سیستم های یک تابع ابزاردقیق ایمنی ، پیکربندی 1OO1 است که تنها از یک تجهیز منفرد تشکیل می‌شود. این معماری اگرچه از نظر نصب و نگهداری, ساده و کم‌هزینه است، اما به دلیل وابستگی کامل به یک تجهیز منفرد، سطح یکپارچگی ایمنی پایینی دارد. در این حالت، خرابی‌های خطرناک شناسایی‌نشده می‌توانند مانع از عملکرد ایمن تابع ابزاردقیق ایمنی شوند و بروز خرابی‌های ایمن یا تشخیص نادرست تجهیز ، باعث ایجاد توقفات کاذب و از دست رفتن تولید خواهد شد.
از دیدگاه ایمنی، این معماری نسبت به خرابی‌های خطرناک کشف‌نشده بسیار حساس است، زیرا وقوع چنین خرابی‌هایی می‌تواند مانع از عملکرد تابع ایمنی در هنگام تقاضا شود. به همین دلیل، مقدار PFDavg در معماری 1oo1نسبتاً بالا بوده و معمولاً دستیابی به سطوح بالای SIL را محدود می‌کند.

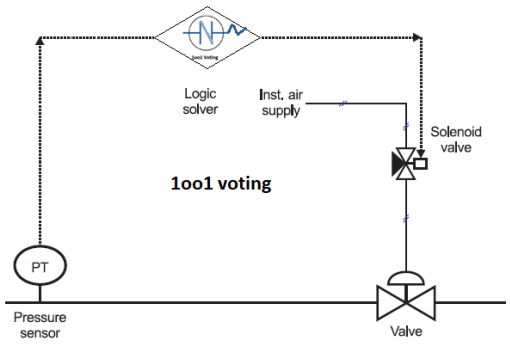
محاسبه میزان احتمال خرابی در صورت تقاضا در معماری 1oo1 :

$$\boldsymbol{PFD(1OO1)} = \boldsymbol{\lambda du} \times \frac{\boldsymbol{T}}{\boldsymbol{2}}$$

از منظر عملیاتی ، هر خرابی ایمن یا خرابی خطرناک کشف‌شده که منجر به تغییر وضعیت خروجی ایمن تجهیز شود، مستقیماً باعث تحریک SIF و در نتیجه توقف کاذب فرآیند خواهد شد. بنابراین نرخ توقفات کاذب در این معماری تابع نرخ خرابی‌های ایمن(λS) ، خرابی‌های خطرناک کشف‌شده(λDD)و نرخ توقفات کاذب ناشی از خرابی های سیستماتیک ایمن(STR SSF) است .

محاسبه نرخ توقفات کاذب STR(1OO1) :

$$\boldsymbol{STR(1OO1) = \lambda S + \lambda DD + STR\ ssf}$$



ب-ترتیب رای گیری 1oo2 :

ترتیب رای گیری 1OO2 نسبت به 1OO1 سطح یکپارچگی ایمنی به مراتب بالاتری را فراهم می‌آورد. در این ترتیب رای گیری ، دو تجهیز به صورت موازی نصب می‌شوند و اگر یکی از آن‌ها رأی به تشخیص شرایط خطرناک بدهد، تابع ابزاردقیق ایمنی فعال خواهد شد .

محاسبه میزان احتمال خرابی در صورت تقاضا در معماری افزونگی 1oo2 :

$$\boldsymbol{PFD(1OO2)} = \frac{(\boldsymbol{\lambda du} \times \boldsymbol{T})^{\boldsymbol{2}}}{\boldsymbol{3}}$$

مطابق IEC 61508 ، در صورت استقلال مناسب کانال‌ها و انجام تست‌های دوره‌ای اثربخش، معماری 1oo2می‌تواند کاهش قابل‌توجهی در PFDavg نسبت به معماری 1oo1ایجاد کرده و امکان دستیابی به SIL بالاتر را فراهم آورد.
با این حال، از منظر توقفات کاذب، رفتار این معماری متفاوت است. در ساختار 1oo2، هر خرابی ایمن یا خرابی خطرناک کشف‌شده در هر یک از کانال‌ها می‌تواند منجر به فعال شدن خروجی ایمنی شود. در نتیجه، صرف افزایش افزونگی الزاماً به معنای بهبود قابلیت دسترس‌پذیری فرآیند نیست و نرخ توقفات کاذب معمولاً نسبت به معماری 1oo1افزایش می‌یابد.
علاوه بر این، استاندارد IEC 61508 تأکید می‌کند که بخشی از خرابی‌ها ممکن است ناشی از علل مشترک باشند که به‌طور هم‌زمان هر دو کانال (تجهیزات شرکت کننده در افزونگی) را تحت تأثیر قرار می‌دهند. این نوع خرابی‌ها با فاکتور بتا (β) مدل‌سازی می‌شوند. فاکتور β بیانگر سهم خرابی‌های تصادفی با علل مشترک است و تنها به خرابی‌هایی اطلاق می‌شود که منشأ یکسان داشته و هم‌زمان بر کانال‌های افزونه اثر می‌گذارند.

افزایش مقدار β موجب کاهش اثربخشی افزونگی، هم از نظر ایمنی و هم از نظر توقفات کاذب می‌شود. به همین دلیل، استاندارد ها بر ضرورت کاهش β از طریق جداسازی فیزیکی، استفاده از منابع تغذیه مستقل، تنوع تجهیزات، تفکیک مسیرهای سیگنال و کنترل شرایط محیطی تأکید دارد.

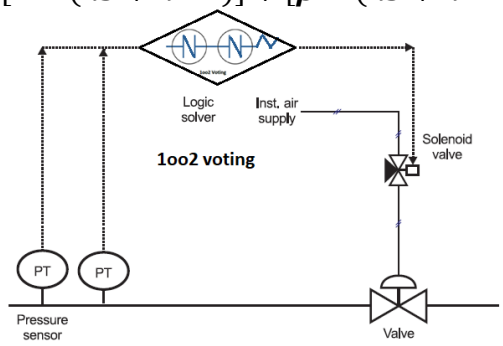
میزان PFD و نرخ توقفات کاذب با در نظر گرفتن فاکتور β :

میزان PFD (1OO2)

$$\boldsymbol{PFD(1OO2)} = \frac{(\boldsymbol{\lambda du} \times \boldsymbol{T})^{\boldsymbol{2}}}{\boldsymbol{3}} \times (\boldsymbol{1} - \boldsymbol{\beta})^{\boldsymbol{2}} + \frac{\boldsymbol{\lambda du} \times \boldsymbol{T}}{\boldsymbol{2}} \times \boldsymbol{\beta}$$

محاسبه نرخ توقفات کاذب STR(1OO2) :

$$STR(1OO2) = [2 \times (\lambda S + \lambda DD)] + [\beta \times (\lambda S + \lambda DD)] + \text{STR s s f}$$



ج-ترتیب رای گیری2oo3 :

در معماری (Two out of Three) 2oo3، سه تجهیز مشابه و مستقل به‌صورت موازی به‌کار گرفته می‌شوند و فعال‌سازی تابع ابزار دقیق ایمنی تنها زمانی انجام می‌شود که حداقل دو تجهیز از سه تجهیز به‌طور هم‌زمان شرایط خطرناک را تشخیص داده و رأی مثبت به فعال‌سازی تابع ایمنی بدهند.

این پیکربندی یکی از متداول‌ترین و معتبرترین معماری‌های افزونگی برای دستیابی هم زمان به سطح بالای یکپارچگی ایمنی (SIL)و دسترس‌پذیری عملیاتی است، زیرا تعادل مناسبی میان کاهش میزان PFD و کاهش توقفات کاذب (Spurious Trips) ایجاد می‌کند. در این معماری حتی در صورت خرابی یک تجهیز، سیستم همچنان قادر به عملکرد ایمن خواهد بود؛ بنابراین نرخ خرابی‌های خطرناک شناسایی‌نشده کاهش چشمگیری یافته و همچنین احتمال توقفات ناخواسته تولید نیز به حداقل می‌رسد.

محاسبه میزان احتمال خرابی در صورت تقاضا در معماری افزونگی 2oo3 :

$$PFD(2OO3) = (\lambda du)^2 \times T^2$$

از دیدگاه تحلیل ایمنی عملکردی، مقدار PFDavg در معماری 2oo3به‌مراتب کمتر از معماری‌های 1oo1و 1oo2است و این معماری معمولاً امکان دستیابی به SIL 3را، مشروط به کنترل مناسب خرابی‌های علل مشترک، فراهم می‌آورد. استاندارد IEC 61508 تأکید می‌کند که اثربخشی این معماری به‌شدت وابسته به میزان استقلال کانال‌ها و کنترل خرابی‌ها با علل مشترک است. مقایسه این معماری با پیکربندی 1OO2 نشان می‌دهد که 2OO3 سطح یکپارچگی ایمنی (SIL) بالاتر و میزان دسترس‌پذیری بهتری فراهم می‌آورد، در حالی که همزمان نرخ توقفات کاذب را نیز کاهش می‌دهد. این ویژگی‌ها باعث شده است که 2OO3 گزینه‌ای مناسب برای فرآیندهایی با ریسک بالا و الزامات سخت‌گیرانه ایمنی و تولید باشد.

در این ساختار، تابع ابزاردقیق ایمنی قادر است خرابی یک تجهیز (اعم از ایمن یا خطرناک کشف‌شده) را بدون از دست دادن سطح یکپارچگی ایمنی یا ایجاد توقفات کاذب تحمل کند. به همین دلیل، احتمال وقوع خرابی‌های خطرناک کشف‌نشده که منجر به عدم عملکرد تابع ایمنی شوند به‌طور قابل توجهی کاهش می‌یابد. هم‌زمان، از آنجا که فعال‌سازی تابع ایمنی نیازمند رأی هم‌زمان دو تجهیز است، توقفات کاذب ناشی از خرابی‌های ایمن یک جزء منفرد , نیز به حداقل می‌رسند.

با این حال، نقطه‌ضعف اصلی معماری 2oo3، هزینه بالاتر طراحی، نصب، راه‌اندازی و نگهداری آن است. علاوه بر افزایش تعداد تجهیزات، کنترل و کاهش خرابی‌های علل مشترک میان سه کانال افزونه که مطابق IEC 61508-6 با فاکتور β مدل‌سازی می‌شوند , نیازمند به‌کارگیری تمهیدات مهندسی خاصی نظیر جداسازی فیزیکی، منابع تغذیه مستقل، تنوع تجهیزات و کنترل شرایط محیطی است. این الزامات، پیچیدگی طراحی و هزینه‌های اجرایی و نگهداری را افزایش می‌دهند .همچنین اجرای تست‌های دوره‌ای،

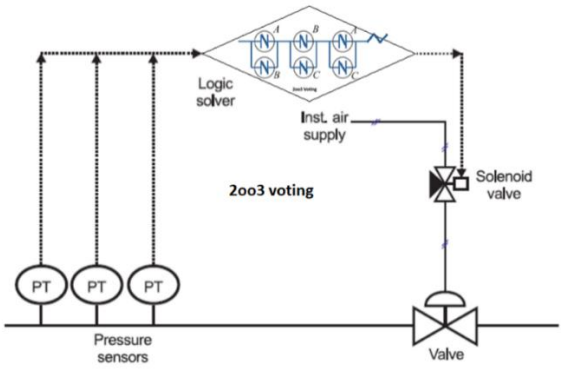
کالیبراسیون و مدیریت داده‌های نگهداری در این معماری به دلیل وجود سه تجهیز موازی و لزوم حفظ استقلال عملکردی ، پیچیده‌تر بوده و نیازمند برنامه‌ریزی دقیق‌تر و رویه‌های نگهداری ساخت‌یافته‌تری است .
میزان PFD و نرخ توقفات کاذب با در نظر گرفتن فاکتور β :

میزان PFD (2OO3)

$$\boldsymbol{PFD(2OO3) = (\lambda du \times T)^2 \times (1-\beta)^2 + \frac{(\lambda du \times T)}{2} \times \beta}$$

محاسبه نرخ توقفات کاذب $STR(2OO3)$:

$$\boldsymbol{STR(2OO3) = [6 \times (\lambda S) \times (\lambda S + \lambda DD) \times MTTR] + [\beta \times (\lambda S + \lambda DD)] + \text{STR ssf}}$$



د-ترتیب رای گیری2oo2 :

در معماری (Two out of Two) 2oo2، دو تجهیز به‌صورت موازی برای هر زیر سیستم استفاده می‌شود و فعال‌سازی تابع ابزار دقیق ایمنی تنها زمانی رخ می‌دهد که هر دو تجهیز به‌طور هم‌زمان شرایط خطرناک را تشخیص داده و رأی مثبت به اجرای تابع ایمنی بدهند.این ویژگی باعث می‌شود که خرابی ایمن یا عملکرد نادرست یک تجهیز به‌تنهایی منجر به فعال‌سازی ناخواسته سیستم نشود. در نتیجه، نرخ توقفات کاذب فرآیند در این معماری به‌طور قابل توجهی کاهش می‌یابد. از این منظر، معماری 2oo2برای فرآیندهایی که تداوم تولید و اجتناب از توقفات ناخواسته اهمیت زیادی دارد، از جذابیت بهره‌برداری بالایی برخوردار است.
از منظر ایمنی عملکردی، معماری 2oo2دارای ضعف ذاتی و جدی است. بطوری که در صورت بروز خرابی های خطرناک پنهان در هر یک از دو تجهیز، تابع ابزار دقیق ایمنی عملاً توانایی واکنش به شرایط خطرناک فرآیندی را از دست می‌دهد، زیرا فعال‌سازی تابع ایمنی مستلزم عملکرد ایمن و صحیح هر دو تجهیز است. در نتیجه، احتمال عدم عملکرد تابع ابزاردقیق ایمنی در هنگام تقاضا به‌شدت افزایش می‌یابد . از اینرو این معماری افزونگی کاهش معناداری در احتمال خرابی در صورت تقاضا (PFDavg) ایجاد نمی‌کند و عملا قادر به تأمین سطح قابل قبول یکپارچگی ایمنی (SIL) برای توابع ابزاردقیق ایمنی مستقل نیست. به همین دلیل، معماری 2oo2 به‌عنوان یک پیکربندی ایمنی مستقل برای فرآیندهای پرریسک توصیه نمی‌شود.
محاسبه میزان احتمال خرابی در صورت تقاضا در معماری افزونگی 2oo2 :

$$\boldsymbol{PFD(2OO2) = \lambda du \times T}$$

در عمل، استفاده از معماری افزونگی 2oo2تنها در شرایطی قابل توجیه است که سطح SIL مورد نیاز پایین باشد یا هدف اصلی , کاهش توقفات کاذب و افزایش دسترس‌پذیری فرآیند بوده و ریسک ایمنی از طریق لایه‌های حفاظتی مستقل دیگر کنترل شده باشد.

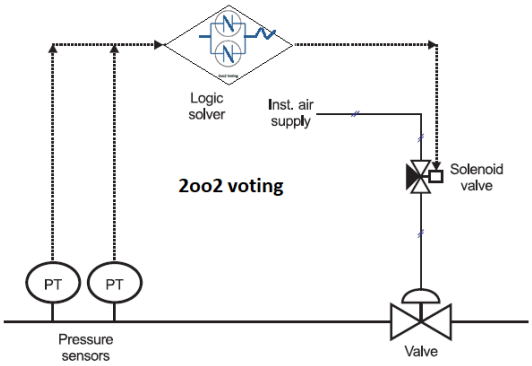
در چنین مواردی، اگرچه سطح ایمنی این معماری محدود است، اما کاهش چشمگیر نرخ توقفات کاذب می‌تواند توجیه‌گر انتخاب آن باشد.
از منظر توقفات کاذب، نرخ STR در معماری 2oo2بسیار پایین بوده و عمدتاً ناشی از خرابی‌های هم‌زمان ایمن یا خرابی‌های علل مشترک است. سهم خرابی‌های علل مشترک مطابق IEC 61508 با فاکتور β مدل‌سازی می‌شود و کنترل آن نیازمند تمهیدات مهندسی مناسب است.
میزان PFD و نرخ توقفات کاذب با در نظر گرفتن فاکتور β :

میزان PFD (2OO2)

$$\boldsymbol{PFD(2OO2) = (\lambda du \times T)^2 \times (1-\beta)^2 + (\lambda du \times T) \times \beta}$$

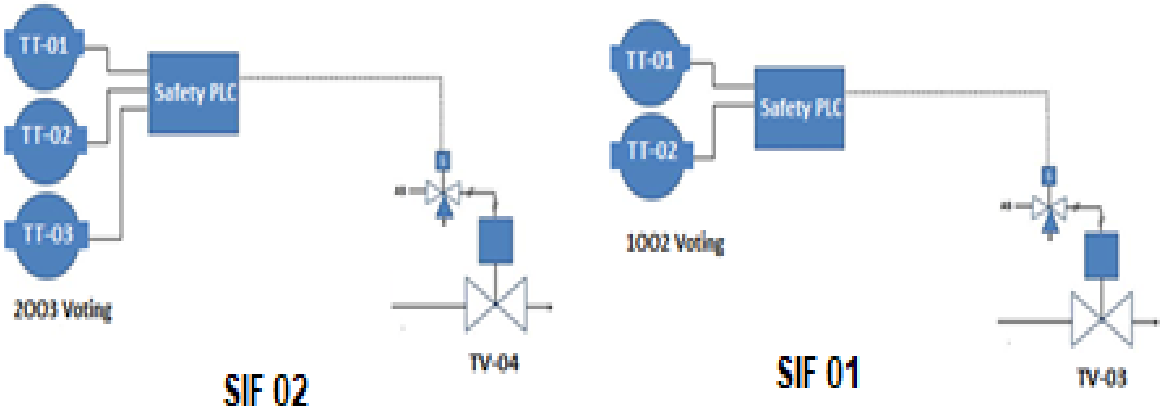
محاسبه نرخ توقفات کاذب $STR(2OO2)$:

$$\boldsymbol{STR(2OO2) = [2 \times (\lambda S) \times (\lambda S + \lambda DD) \times MTTR] + [\beta \times (\lambda S + \lambda DD)] + \text{STR ssf}}$$



۶-مثال کاربردی :

در یک واحد شیمیایی با دو راکتور کاملا مشابه که واکنش‌های گرمازا در آن‌ها انجام می‌گردد ، حفاظت در برابر افزایش بیش از حد دما از نظر ایمنی فرآیند بسیار حیاتی است. از این جهت برای هر راکتور یک تابع ابزار دقیق ایمنی (SIF) مستقل طراحی شده است. در هرSIF ، اندازه‌گیری توسط سنسورهای RTD و ترانسمیترهای دمای دارای تأییدیه SIL انجام می‌شود تا در صورت افزایش دما تا حدHigh-High ، فرمان توقف ایمن فرآیند (رساندن فرآیند به وضعیت ایمنی از پیش تعیین شده) صادر شود.
به منظور طراحی بخش تجهیزات اندازه‌گیری (سطح سنسور) این توابع ایمنی، دو گزینه معماری افزونگی برای مجموع سنسورها و ترانسمیترها در نظر گرفته شده است(معماری افزونگی با ترتیب رای گیری 1oo2و 2oo3).



هدف این مثال، مقایسه عملی دو معماری افزونگی 1oo2و 2oo3 در سطح سنسور برای توابع ابزاردقیق ایمنی مورد اشاره از منظر شاخص‌های کلیدی زیر است:

- **احتمال خرابی در صورت تقاضا(PFDavg)**
- **نرخ توقفات کاذب(STR)**
- **اثر خرابی‌های علل مشترک با در نظر گرفتن ضریب β (Beta Factor)**

مشخصات پایه :

پارامتر	مقدار
تجهیز	ترانسمیتر دمای(SIL-rated)+ RTD
λDU (خرابی خطرناک کشف‌نشده)	2×10^{-6} 1/h
λDD(خرابی خطرناک کشف‌شده)	1×10^{-6} 1/h
λS(خرابی ایمن)	5×10^{-6} 1/h

پارامتر	مقدار
Proof Test Interval (T)	1سال = ۸۷۶۰h
MTTR	8 h
βint تجهیزات	0.02
β معماری 1oo2	0.02
β معماری 2oo3	0.03
STR_{SSF}	تقریباً صفر

محاسبه PFD_{1OO2} و STR_{1oo2} سنسور و ترانسمیترهای دمای مورد استفاده در تابع ابزاردقیق ایمنی SIF01 :

ایده آل $PFD(1OO2) = \frac{(\lambda du \times T)^2}{3} = 1.023 \times 10^{-4}$ /h

با درنظر گرفتن فاکتور β $PFD(1OO2) = \frac{(\lambda du \times T)^2}{3} \times (1-\beta)^2 + \frac{\lambda du \times T}{2} \times \beta \approx 2.734 \times ۱۰-4$ /h

$STR(1OO2) = [2 \times (\lambda S + \lambda DD)] + [\beta \times (\lambda S + \lambda DD)] +$ STR s s f ≈۱.۲۱۲×۱۰−۵ /h

سال 9.4 :(MTBST) میانگین زمان بین توقفات کاذب

محاسبه PFD_{2OO3} و STR_{2oo3} سنسور و ترانسمیترهای دمای مورد استفاده در تابع ابزاردقیق ایمنی SIF02 :

ایده آل $PFD(2OO3) = (\lambda du)^2 \times T^2 = 3.07 \times 10^{-4}$

با درنظر گرفتن فاکتور β $PFD(2OO3) = (\lambda du \times T)^2 \times (1-\beta)^2 + \frac{(\lambda du \times T)}{2} \times \beta \approx 5.517 \times ۱۰^{-4}$ /h

$$STR(2OO3) = [6 \times (\lambda S) \times (\lambda S + \lambda DD) \times MTTR] + [\beta \times (\lambda S + \lambda DD)] + \text{STR ssf} \approx 3.014 \times 10^{-7}\ 1/h$$

سال 32 ≈ (MTBST) میانگین زمان بین توقفات کاذب

در مقایسه نتایج به‌دست‌آمده مشاهده می گردد که مقدار احتمال خرابی در صورت تقاضا (PFDavg) برای افزونگی با ترتیب رای گیری 1oo2برابر $2.734 \times 10^{-4}\ 1/h$ و برای ترتیب رای گیری 2oo3برابر $5.517 \times 10^{-4}\ 1/h$ محاسبه شده است؛ بنابراین در این مثال خاص، مقدار PFDavg در ترتیب رای گیری 2oo3تقریباً دو برابر 1oo2به دست آمده است.
با این حال، از نظر نرخ توقفات کاذب، معماری 2oo3عملکرد بسیار بهتری نشان می‌دهد، به‌طوری‌که مقدار STR در ترتیب رای گیری 1oo2برابر $1.212 \times 10{-}5\ 1/h$ (با میانگین زمان بین توقفات کاذب حدود ۹.۴ سال) , در حالی‌که در ترتیب رای گیری 2oo3 مقدار STR به حدود $3.014 \times 10{-}71/h$کاهش یافته (میانگین زمان بین توقفات کاذب به حدود ۳۲ سال افزایش یافته است) بنابراین این مقایسه نشان می‌دهد که اگرچه ترتیب رای گیری 1oo2از نظر PFD مقدار کمتری دارد، اما معماری 2oo3از نظر پایداری عملیاتی، کاهش توقفات ناخواسته و در دسترس پذیری , عملکرد برتری ارائه می‌دهد .

۷-عوامل تاثیر گذار بر میزان اثر بخشی معماری های افزونگی :

الف-کاهش خرابی‌ها با علت مشترک (CCF) و مدیریت فاکتورβ : یکی از مهم‌ترین عوامل تعیین‌کننده اثربخشی واقعی معماری افزونگی، کنترل خرابی‌های با علت مشترک و مدیریت فاکتور β است. این فاکتور نشان‌دهنده سهم خرابی‌هایی است که می‌توانند به‌طور همزمان چند المان یک معماری افزونه را تحت تأثیر قرار دهند و در نتیجه مزیت افزونگی را محدود کنند. مقدار β تنها به مشخصات ذاتی تجهیزات وابسته نیست و به‌شدت تحت تأثیر کیفیت طراحی , میزان جداسازی فیزیکی و عملکردی , استفاده از تنوع فناوری یا سازنده تجهیزات، شرایط محیطی، رویه‌های نگهداشت و نحوه مدیریت مداخلات و خطا های انسانی قرار دارد. در صورت عدم مدیریت صحیح این عوامل، در زیر سیستم های دارای افزونگی , احتمال وقوع خرابی همزمان افزایش یافته و بهبود مورد انتظار در شاخص‌های ایمنی حاصل نخواهد شد.

ب- اجرای صحیح و منظمProof Test : اجرای تست های دوره‌ای Proof Test نقش کلیدی در کنترل PFDavg دارد، زیرا این تست ها با هدف کشف خرابی‌های خطرناک پنهان انجام می‌شوند و احتمال عدم عملکرد صحیح و ایمن یک SIF را در زمان تقاضا , کاهش می‌دهند. فاصله زمانی و روش اجرای این تست باید بر اساس تحلیلSIL ، شرایط بهره‌برداری و عملیاتی و الزامات استانداردی تعیین شود. در عین حال، طراحی و اجرای Proof testباید به‌گونه‌ای انجام شود که از ایجاد توقف‌های غیرضروری یا افزایش STR جلوگیری کند. علاوه بر این، هرچند این تست به‌طور مستقیم باعث کاهش مقدار β نمی‌شود اما اجرای صحیح و کنترل‌شده Proof test می‌تواند احتمال ایجاد خرابی‌های با علت مشترک ناشی از روی های نادرست نگهداشت و خطاهای انسانی را کاهش دهد.

ج- پوشش تشخیصی(Diagnostic Coverage – DC) :افزایش DC باعث کاهش سهم خرابی‌های خطرناک پنهان و تقلیل آن به وسیله تبدیل λdu به λdd می گردد که در نتیجه منجر به کاهش PFDavg می‌شود، زیرا تعداد بیشتری از خرابی های خطرناک قبل از وقوع شناسایی می‌گردند. با این حال، افزایش بیش از حد تاثیر تشخیص خرابی بر عملکرد توبع ابزاردقیق ایمنی می‌تواند به افزایش تحریک‌های غیرضروری سیستم ایمنی منجر شود که در عمل به صورت افزایش STR ظاهر می‌شود. بنابراین طراحی سیستم‌های تشخیصی باید به‌گونه‌ای انجام شود که تعادل بین کاهش PFD و عدم افزایش غیرمنطقی STR حفظ شود.
د- مدیریت Fault Handling : در استانداردهای ایمنی عملکردی طراحی سیستم SIS باید به‌گونه‌ای باشد که فعال‌سازی تابع

ابزاردقیق ایمنی تنها در مواجهه با شرایط واقعی رخ دهد. این امر مستلزم مدیریت دقیق منطق خطاها، فیلتر کردن نویزها و تداخلات ، کنترل خطاهای انسانی و تفکیک منطقی بین حالت‌های هشدار و Trip است.

نتیجه گیری :

عوامل موثر در بهینه‌سازی و تعادل میان PFDوSTR در معماری های افزونگی :

در سیستم‌های ابزار دقیق ایمنی، معماری افزونگی و ترتیب رأی‌گیری زیرسیستم ها یکی از پارامترهای اصلی و مؤثر بر احتمال خرابی خطرناک در صورت تقاضا (PFDavg) و نرخ توقف‌های کاذب (STR) است. نوع معماری افزونگی تعیین می‌کند چه تعداد خرابی برای از دست رفتن عملکرد ایمن لازم است و در مقابل چه تعداد سیگنال می‌تواند منجر به فعال شدن عملکرد ایمن یک تابع ابزاردقیق ایمنی شود .

در تحلیل‌های قابلیت اطمینان، در صورت فرض استقلال تجهیزات استفاده شده در معماری افرونه و سهم پایین خرابی‌ها با علت مشترک، افزایش تعداد کانال‌ها در معماری افزونگی می‌تواند احتمال خرابی خطرناک پنهان را کاهش دهد، به‌طوری‌که در شرایط ایده‌آل ترتیب رای گیری مانند 1oo2می‌تواند PFD کمتری نسبت به 1oo1داشته باشد. در مقابل، افزایش تعداد کانال‌ها و المان ها می‌تواند تعداد مسیرهای بالقوه ایجاد Trip ناخواسته را افزایش داده و منجر به افزایش STR شود. بنابراین انتخاب معماری افزونگی باید همواره بر اساس تحلیل کمی و در چارچوب الزامات مجموعه استانداردهای ایمنی عملکردی از جمله IEC 61508 ، IEC 61511و راهنماهای ISA انجام شود.

منابع :

1. IEC 61508 (2010). Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.

2- IEC 61508 (2011)Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

3. IEC 61511 (2016). Functional Safety – Safety Instrumented Systems for the Process Industry Sector.

4. ISA 84.00.01 (2004). Functional Safety: Safety Instrumented Systems for the Process Industry Sector

5. ISA TR84.00.02 (R2018). Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques.

6. ISA TR84.00.03 (2010, R2018). Guidelines for the Implementation of Layer of Protection Analysis (LOPA).

7. OREDA (2015). Offshore Reliability Data Handbook .

8-Maintaining Safety Integrity in Safety Instrumented Systems (SIS) and the Role of Proof Testing in Reducing Process Risks- Reza Abbasi Larki – Reg code : OIL093842763

Abstract

Safety Instrumented Systems (SIS), as an Independent Protection Layer (IPL), are key elements of process safety management and are designed and implemented to protect people, the environment,

and physical assets. Each SIS consists of one or more Safety Instrumented Functions (SIFs) that are designed and implemented to prevent initiating events in defined hazardous scenarios and to reduce risk to the organization's tolerable risk level. These functions continuously monitor process parameters and, upon demand (i.e., detection of an initiating event), act automatically to bring the process to a predefined safe state.

During the design process, a Safety Integrity Level (SIL) is assigned to each SIF based on the required risk reduction and the results of risk analysis and assessment methods such as Layer of Protection Analysis (LOPA). Since, in most process industries, safety instrumented functions operate in Low Demand Mode, the Probability of Failure on Demand (PFD) is used as the primary indicator for evaluating their safety performance. This metric represents the probability that the safety function will fail to operate correctly and in a timely manner when required (upon demand). Conversely, the unintended activation of safety instrumented functions in the absence of a real process demand, known as a Spurious Trip, is considered one of the major challenges in the design and operation of safety instrumented systems. This phenomenon may result from a false demand or from failures in components associated with the safety instrumented function, leading to consequences such as unplanned shutdowns, reduced system operational availability, and increased operational costs.

Therefore, effective safety lifecycle management of safety instrumented systems requires establishing an engineering balance between maintaining the required Safety Integrity Level (SIL) through reduction of the Probability of Failure on Demand (PFD) and controlling the Spurious Trip Rate (STR). Focusing solely on increasing the SIL without considering its impact on spurious trip rates may lead to reduced reliability and operational efficiency of the safety instrumented system.

Keywords:
-Safety Instrumented System (SIS)
-Safety Instrumented Function (SIF)
-Safety Integrity Level (SIL)
-Probability of Failure on Demand (PFD)
-Spurious Trip Rate (STR)
-Operational Availability
-Redundancy Architecture
-Random Hardware Failures
-Systematic Failures
-Common Cause Failures (CCF)