نهمین همایش بین‌المللی
توسعه فناوری در نفت، گاز، پالایش و پتروشیمی
9th International Conference on
Technology Development in Oil, Gas, Refining and Petrochemicals
www.oil.bcnf.ir

حفظ یکپارچگی ایمنی در سیستم‌های ابزار دقیق ایمنی (SIS) و نقش تست اثبات عملکرد در کاهش ریسک های فرآیندی

رضا عباسی لرکی

بازرس فنی برق و ابزاردقیق - شرکت پتروشیمی امیرکبیر
abbasilarkireza@yahoo.com

چکیده

در صنایع حیاتی کشور مانند نفت، گاز و پتروشیمی، ایمنی فرآیند فراتر از یک الزام فنی بوده و با حفاظت از جان انسان‌ها، محیط زیست و صیانت از سرمایه‌های ملی گره خورده است. سیستم‌های ابزار دقیق ایمنی، به ویژه سیستم‌های توقف اضطراری (Emergency Shutdown Systems – ESD) به عنوان یک لایه حفاظتی مستقل , نقش حیاتی در کاهش ریسک‌های فرآیندی دارند و عملکرد صحیح و ایمن آنها در شرایط بحرانی تعیین‌کننده ایمنی کل فرآیند است.با توجه به اینکه توابع ابزاردقیق ایمنی مورد استفاده در صنایع مورد اشاره , غالبا در حالت Low Demand (تقاضای کم) عمل می نمایند ، احتمال بروز خرابی‌های پنهان در طول زمان افزایش می‌یابد و فقدان تست‌های دوره‌ای اثبات عملکرد (Proof Test) می‌تواند اعتبار سطح یکپارچگی ایمنی (SIL) را کاهش دهد. اجرای منظم تست‌های اثبات عملکرد توابع ابزاردقیق ایمنی ، ضمن کشف به‌موقع خرابی‌ها و کاهش احتمال خرابی در هنگام تقاضا (PFDavg)، اطمینان می‌دهد که سیستم‌های ابزاردقیق ایمنی در هنگام بروز شرایط بحرانی عملکردی ایمن، پایدار و مطابق با سطح یکپارچگی ایمن طراحی‌شده ارائه می دهند .این پژوهش به بررسی ساختار، عملکرد و چالش‌های نگهداری سیستم‌های ابزار دقیق ایمنی می‌پردازد و نقش حیاتی تست‌های اثبات را در تضمین عملکرد ایمن و قابل اعتماد این سیستم ها برجسته می‌سازد .

واژه های کلیدی

۱-SIS -(Safety Instrumented System): بر اساس IEC 61511-1 ، بند ۳.۲.۶۷, سیستم ابزار دقیق ایمنی مجموعه‌ای از تجهیزات شامل حسگرها، پردازشگر منطقی و عناصر نهایی است که به‌صورت مستقل از سیستم های کنترل فرآیند پایه عمل می‌کند و به منظور تشخیص شرایط خطرناک و انجام اقدامات ایمنی لازم , در جهت کاهش ریسک های فرآیندی طراحی و اجرا می گردند.
۲-SIF – (Safety Instrumented Function): بر اساس استاندارد IEC 61511-1 ، بند ۳.۲.۶۶:یک تابع ابزار دقیق ایمنی , عملکرد ایمنی مشخص است که توسط سیستم ابزار دقیق ایمنی اجرا می‌شود. هر SIF شامل سه بخش اصلی است: حسگر برای تشخیص

شرایط ناایمن، پردازشگر منطقی برای تصمیم‌گیری، و عنصر نهایی برای اقدام اصلاحی (هر SIF بدارای سطح یکپارچگی ایمنی (SIL) مشخص است).

۳- IPL - (Independent Protection Layer):لایه‌ای حفاظتی که مستقل از سایر حفاظت ها و به‌تنهایی قادر به جلوگیری یا کاهش قابل‌توجه پیامد یک خطر است.

۴- failure (شکست /خرابی): خاتمه توانایی یک تابع ابزاردقیق ایمنی برای ارائه عملکرد یا عملیات مورد نیاز (عملکردی غیر از آنچه که مورد نیاز است).

۵-Demand (تقاضا) : بروز شرایط یا رویدادی که نیاز به عملکرد ایمن یک تابع ابزاردقیق ایمنی را ایجاد می نماید .

۶- PDF_{avg} (Average probability of failure on demand): متوسط احتمال خرابی در صور ت تقاضا , احتمال این است که یک تابع ابزاردقیق ایمنی به طور خطرناکی از کار بیفتد

۷-RRF (Risk reduction factor): ضریب کاهش ریسک که به صورت $1/PFD_{avg}$ بیان می شود و معرف میزان اثر بخشی SIF نسبت به سطح یکپارچگی ایمنی و در دسترس بودن حفاظت تعیین شده است .

۸-SIL (Safety integrity level): بر اساس استاندارد IEC 61511-1 ، سطح یکپارچگی ایمنی عددی از ۱ تا ۴ که میزان قابلیت اطمینان مورد نیاز یک تابع ابزاردقیق ایمنی (SIF) را جهت کاهش ریسکی مشخص تعیین می‌کند , بنابراین SIL بالاتر نشان‌دهنده نیاز به سطح ایمنی بیشتر است.

۹-Availability (در دسترس بودن) : در دسترس بودن معیار آمادگی یک تابع ابزاردقیق ایمنی جهت انجام عملکرد ایمن مورد نیاز در صورت تقاضا است .

مقدمه

در صنایع فرآیندی مانند صنایع نفت، گاز و پتروشیمی، مدیریت ریسک و کاهش پیامدهای حوادث احتمالی با رویکردی لایه‌ای انجام می‌شود. این رویکرد بر این اصل استوار است که هیچ لایه حفاظتی به‌تنهایی در برابر خرابی یا شکست در عملکرد مصون نیست. به همین دلیل، چندین لایه مستقل و موازی طراحی می‌شود تا در صورت نقص در یک لایه، سایر لایه‌ها بتوانند به‌طور مستقل وارد عمل شده و از وقوع حادثه جلوگیری کنند. چنین ساختاری، تاب‌آوری در برابر خرابی‌ها را افزایش می‌دهد و احتمال بروز حوادث جدی را به حداقل می‌رساند.
در میان انواع لایه‌های حفاظتی، سیستم‌های ابزار دقیق ایمنی (SIS) جایگاهی ویژه دارند. یک سیستم ابزاردقیق ایمنی باید در طول چرخه عمر ایمن (Safety Lifecycle) همواره آماده‌به‌کار باشد و در کسری از ثانیه، فرآیند را به وضعیت ایمن از پیش تعیین‌شده هدایت کند.

توابع ابزار دقیق ایمنی (SIF) بر اساس میزان کاهش ریسک مورد نیاز برای هر رویداد طراحی می‌شوند تا مطابق با سطح یکپارچگی ایمنی (SIL)تعیین‌شده، فرآیند را در شرایط ایمن حفظ نمایند . این توابع باید از قابلیت اطمینان بالا برخوردار باشند و احتمال خرابی در هنگام تقاضا (Probability of Failure on Demand – PFD) در آنها به حداقل برسد تا تضمین شود که سیستم همواره قادر به کاهش ریسک به سطح قابل قبول خواهد بود .

یکی از چالش‌های اساسی در فاز بهره‌برداری و نگهداشت از چرخه عمر یک سیستم ابزاردقیق ایمنی، شناسایی خرابی‌های پنهان خطرناک است که در صورت عدم تشخیص، می‌توانند عملکرد توابع ابزاردقیق ایمنی را مختل کرده و ایمنی فرآیند را تهدید نمایند . تجربه عملی نشان می‌دهد که حتی طراحی اصولی و اجرای دقیق یک سیستم ابزار دقیق ایمنی ، بدون برنامه‌ریزی مناسب جهت انجام تست‌های اثبات عملکرد (Proof Tests)و پایش مستمر، قادر به حفظ سطح یکپارچگی ایمنی (SIL) مورد انتظار نیست. اجرای منظم تست‌های اثبات عملکرد، با کشف به‌موقع خرابی‌ها، کاهش PFD_{avg} و تضمین سطح SIL طراحی‌شده، نقش حیاتی در عملکرد پایدار و ایمن سیستم های ابزاردقیق ایمنی ایفا می‌کند و امکان به‌روزرسانی داده‌های قابلیت اطمینان را نیز فراهم می‌آورد.

اجرای تست‌های اثبات عملکرد دوره‌ای(Periodic Proof Tests) ، همراه با طراحی مهندسی دقیق، ارزیابی سیستماتیک ریسک و نگهداری پیشگیرانه، ستون فقرات تضمین عملکرد ایمن و قابل اعتماد سیستم‌های ابزار دقیق ایمنی در طول چرخه عمر آن‌هاست. این تست‌ها با شبیه‌سازی شرایط بحرانی و بررسی پاسخ سیستم، اطمینان می‌دهند که توابع ابزاردقیق ایمنی حتی پس از گذشت زمان طولانی و در مواجهه با وضعیت‌های واقعی فرآیندی، قادر به عملکرد سریع و ایمن هستند و سطح یکپارچگی ایمنی (SIL) مورد انتظار حفظ می گردد.

۱- تعاریف و مفاهیم پایه درخصوص سیستم‌های ابزاردقیق ایمنی :

سیستم‌های ابزاردقیق ایمنی (SIS) یکی از ارکان حیاتی مدیریت ایمنی فرآیند در صنایع هستند که با هدف پیشگیری از وقوع رویدادهای خطرناک طراحی و پیاده‌سازی می‌شوند. این سیستم‌ها در لایه حفاظتی کنترل فرآیند (Process Control Layer) قرار دارند و وظیفه انجام اقدامات ایمنی خودکار و سریع در مواجهه با شرایط غیرعادی یا ناایمن فرآیند را بر عهده دارند.

برای راهنمایی طراحی و پیاده‌سازی این سیستم‌ها، کمیسیون بین‌المللی الکتروتکنیک (IEC) استاندارد IEC 61508را تدوین نموده است. این استاندارد تحت عنوان «ایمنی عملکردی سیستم‌های مرتبط با ایمنی الکترونیکی، الکتریکی و قابل برنامه‌ریزی» ارائه شده و مجموعه‌ای از الزامات فنی و رویه‌های چرخه عمر ایمن را جهت سخت‌افزار و نرم‌افزار سیستم SIS تعریف می‌کند.

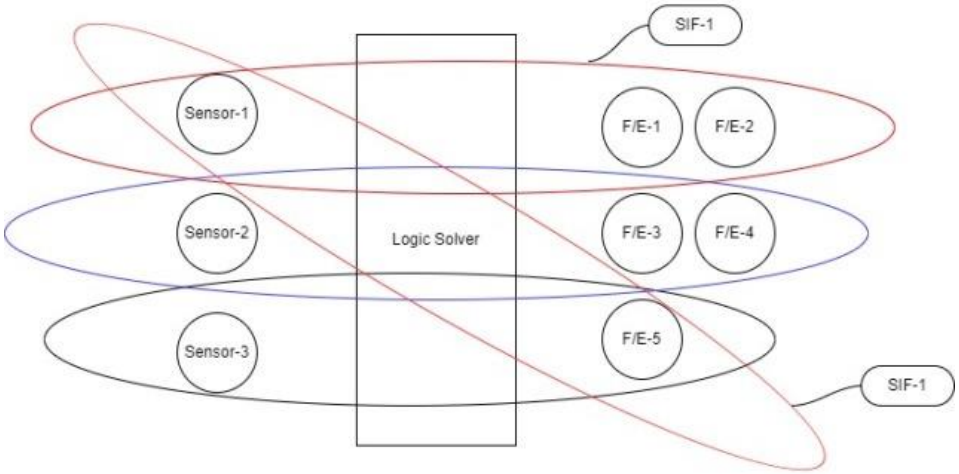
همچنین، این استاندارد به‌عنوان معیار ارزیابی برای تأمین‌کنندگان تجهیزات SIS مورد استفاده قرار می‌گیرد تا تأیید سطح یکپارچگی ایمنی SILتجهیزات برای کاربرد در سیستم‌های رتبه‌بندی‌شده , در هنگام طراحی و اجرا تضمین گردد.

یکی از نمونه‌های کاربردی SIS در صنایع نفت , گاز وپتروشیمی، سیستم های توقف اضطراری (Emergency Shutdown – ESD) است.

یک SIS از سه بخش کلیدی تشکیل شده است:

- حسگرها (Sensors) : جهت پایش مستمر پارامترهای فرآیندی و شناسایی شرایط ناایمن.

- حل‌کننده منطقی (Logic Solver) :شامل پردازنده منطقی قابل برنامه‌ریزی که داده‌های ورودی حسگرها را تحلیل و تصمیمات ایمنی لازم را صادر می نماید.
- عناصر نهایی (Final Elements) :مانند شیرهای قطع اضطراری، که اجرای فرمان های صادره از حل‌کننده منطقی را برعهده دارند.

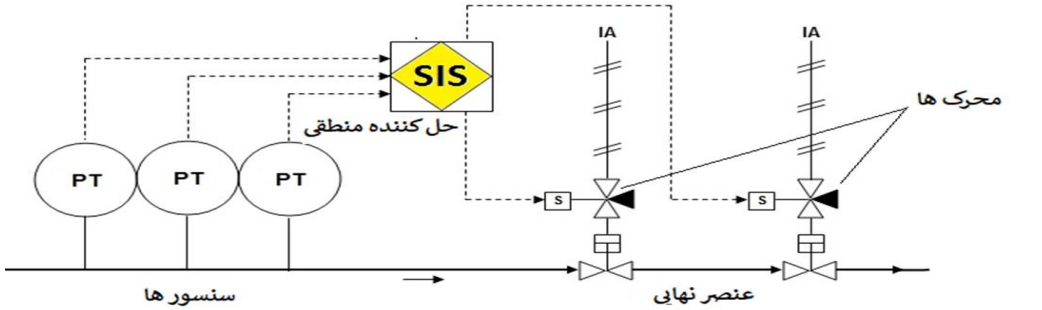


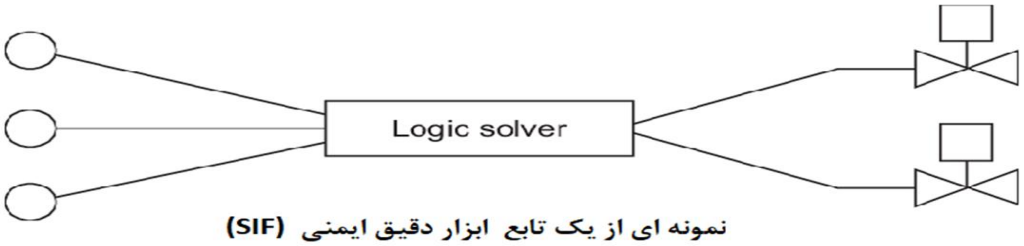
SIS

هر SIS از تعدادی حلقه کنترلی مستقل تشکیل شده است که به هر حلقه، یک تابع ابزاردقیق ایمنی (Safety Instrumented Function – SIF) گفته می‌شود .وظیفه اصلی هر SIF کاهش ریسک ناشی از یک رویداد فرآیندی مشخص و بازگرداندن فرآیند به وضعیت ایمن از پیش تعیین شده است.

ویژگی‌های کلیدی یک تابع ابزاردقیق ایمنی (SIF) شامل موارد زیر است:

- وظیفه ایمنی مشخص (Safety Function) :عملکرد ایمنی مشخص در برابر سناریوهای خطرناک خاص.
- عملکرد خودکار (Automatic Action) :بازگرداندن فرآیند به وضعیت ایمن از پیش تعیین شده بدون نیاز به دخالت اپراتور.
- سطح یکپارچگی ایمنی (Safety Integrity Level – SIL) :عملکرد ایمن تعریف شده بر اساس شدت پیامدها، فرکانس وقوع و میزان کاهش ریسک مورد انتظار.





نمونه ای از یک تابع ابزار دقیق ایمنی (SIF)

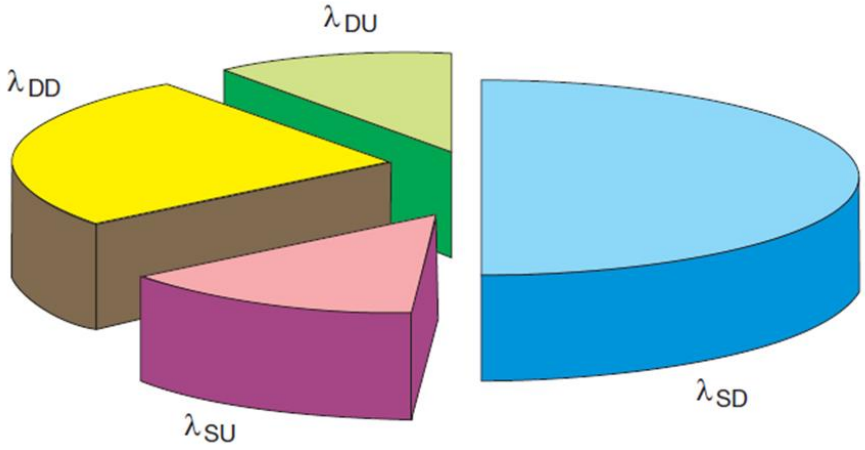
۲- انواع خرابی در سیستم های ابزاردقیق ایمنی :

۲-۱- خرابی‌های تصادفی(Random Failures) : این نوع خرابی در زمان نامشخص و بطور ناگهانی رخ می دهد که از یک یا چند مکانیسم تخریب ناشی می شود.خرابی‌های تصادفی معمولاً ناشی از عوامل فیزیکی مانند پیری قطعات,سایش، خوردگی و امثال آنها می باشند . این خرابی‌ها با طراحی ایمن , بهینه‌سازی معماری های سخت‌افزاری (استفاده از افزونگی) و فعالیت های پیشگیرانه ، قابل کاهش می‌باشند .

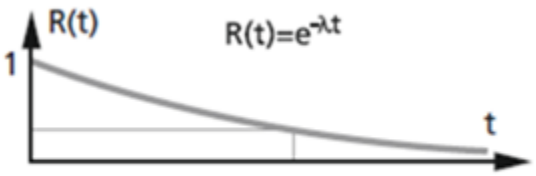
نرخ خرابی‌های تصادفی(Failure Rate – λ) : نرخ خرابی‌های تصادفی در سیستم‌های ابزاردقیق ایمنی با λنمایش داده می‌شود و بسته به خطرناک یا ایمن بودن و آشکار یا پنهان بودن به چهار دسته تقسیم می‌شوند:

۱. خرابی‌های خطرناک شناسایی شده (λ_{dd}) :خرابی‌هایی که عملکرد ایمن SIF را مختل می‌کنند، اما قابل شناسایی هستند.
۲. خرابی‌های خطرناک شناسایی نشده (λ_{du}) :خطرناک‌ترین نوع خرابی که عملکرد ایمن SIF را مختل می‌کند و تا زمان تقاضا قابل شناسایی نیست.
۳. خرابی‌های ایمن شناسایی شده(λ_{sd}) : خرابی‌هایی که منجر به عملکرد ایمن SIF می‌شوند و قابل شناسایی هستند.
۴. خرابی‌های ایمن شناسایی نشده (λ_{sdu}) :خرابی‌هایی که منجر به عملکرد ایمن SIF می‌شوند، اما قابل شناسایی نیستند (این نوع خرابی باعث بروز توقفات کاذب می گردد).

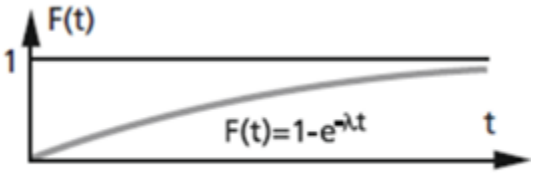
بنابراین خرابی هایی تحت عنوان "خطرناک" طبقه بندی می شوند که در هنگام تقاضا ,منجر به عدم عملکرد صحیح و ایمن یک تابع ابزاردقیق ایمنی گردد .



همانطور که از منحنی وان حمامBathtub Curve بر می آید , نرخ خرابی ثابت وجود ندارد و نرخ خرابی های تصادفی در توابع ابزاردقیق ایمنی با گذشت زمان افزایش خواهد یافت , بنابراین تابع احتمال خرابی و قابلیت اطمینان یک SIF برحسب زمان را می توان به صورت زیر تعریف نمود:



R(t) تابع قابلیت اطمینان



F(t) تابع احتمال خرابی

۲-۲- خرابی‌های سیستماتیک(Systematic Failures) :

خرابی‌های سیستماتیک عمدتا ناشی از نقص و خطا در طراحی، نحوه پیاده‌سازی، نصب، نگهداری یا مدیریت تغییرات می‌باشند و برخلاف خرابی‌های تصادفی، قابل پیش‌بینی هستند.

از اینرو خرابی های سیستماتیک عموما به دلیل خطاهای انسانی در مراحل مختلف از ساخت و طراحی تا اجرای سخت افزار یا نرم افزار سیستم های ابزاردقیق ایمنی (SIS) ایجاد می شوند.

نکته : توجه گردد که خرابی های سیستماتیک در محاسبات نرخ خرابی تجهیزات (محاسبه احتمال خرابی در هنگام تقاضا) لحاظ نمی شود و از این جهت مورد توجه این مقاله نمی باشد.

۳-یکپارچگی ایمنی(Safety Integrity) :

یکپارچگی ایمنی شاخصی است که توانایی یک تابع ابزاردقیق ایمنی (SIF) را در حفظ عملکرد ایمن تحت تمامی شرایط عملیاتی و در طول دوره زمانی مشخص اندازه‌گیری می‌کند. این شاخص، ترکیبی از عملکرد صحیح تجهیزات، دسترس‌پذیری مناسب و پاسخ تابع ابزاردقیق ایمنی در مواجهه با شرایط خطرناک است و مستقیماً با کاهش ریسک فرآیندی مرتبط می‌باشد.

یکپارچگی ایمنی نه‌تنها بر قابلیت اطمینان سخت‌افزار و نرم‌افزار تأکید دارد، بلکه تعامل اجزای یک سیستم ابزاردقیق ایمنی (SIS) شامل حسگرها، حل‌کننده منطقی و عناصر نهایی را نیز در نظر می‌گیرد .

۱-۳- سطح یکپارچگی ایمنی(Safety Integrity Level – SIL) :

سطح یکپارچگی ایمنی (SIL) معیاری کمی برای سنجش قابلیت اطمینان توابع ابزاردقیق ایمنی در کاهش ریسک فرآیندی به سطح قابل قبول است و شامل چهار سطح(از SIL 1 تا SIL 4) می‌باشد. هرچه سطح یکپارچگی ایمنی بالاتر باشد، تابع ابزاردقیق ایمنی ملزم است , میزان یکپارچگی ایمنی و کاهش ریسک به مراتب بیشتری را ایجاد نماید.

هر سطح یکپارچگی ایمنی (SIL) با دو شاخص کلیدی مشخص می‌شود:

الف-میانگین احتمال خرابی در صورت تقاضا (PFD_{avg}) :این شاخص , احتمال شکست عملکرد ایمن و خرابی تابع ابزاردقیق ایمنی در هنگام وقوع تقاضای واقعی را نشان می‌دهد. این شاخص ترکیبی از خرابی‌های خطرناک (پنهان) و تأثیر تست‌های اثبات عملکرد (Proof Test)می باشد .

ب-ضریب کاهش ریسک (Risk Reduction Factor – RRF) :این شاخص , میزان کاهش ریسک فرآیند توسط یک تابع ابزاردقیق ایمنی را نشان می‌دهد که با رابطه زیر تعریف می‌شود:

$$\frac{1}{PFD_{avg}} = RRF$$

به عبارت دیگر هرچه PFDavg کمتر باشد، RRFبالاتر است و SIF عملکرد ایمن قوی‌تری دارد.

۲-۳- مفهوم تقاضا(Demand) :

Demand (تقاضا) , بروز شرایط یا رویدادی است که نیاز به عملکرد ایمن یک تابع ابزاردقیق ایمنی را ایجاد می نماید . در این شرایط، تابع ابزاردقیق ایمنی وظیفه دارد به‌طور خودکار فرآیند را به وضعیت ایمن از پیش تعیین‌شده برساند.

در صنایع نفت، گاز و پتروشیمی، توابع ابزاردقیق ایمنی معمولاً در حالت Low Demand استفاده می‌شوند. این بدان معناست که احتمال وقوع تقاضا برای عملکرد ایمن به ندرت و کمتر از یک بار در سال یا دو برابر فرکانس تست اثبات آن است.

در چنین شرایطی محاسبه سطح یکپارچگی ایمنی و ارزیابی قابلیت اطمینان تابع ابزاردقیق ایمنی بر اساس PFDavg انجام می‌شود و تمرکز بر مدیریت خرابی‌های خطرناک پنهان تجهیزات می باشد تا عملکرد ایمنی سیستم همواره تضمین گردد.

SIL	محدوده PFDavg	ضریب کاهش ریسک (RRF)
SIL1	10^{-2} تا 10^{-1}	10 تا ۱۰۰
SIL2	10^{-3} تا 10^{-2}	100 تا ۱۰۰۰
SIL3	10^{-4} تا 10^{-3}	1000 تا ۱۰,۰۰۰
SIL4	10^{-5} تا 10^{-4}	10,000 تا ۱۰۰,۰۰۰

۴- تعیین و ارزیابی سطح یکپارچگی ایمنی(SIL) :

سطح یکپارچگی ایمنی برای هر تابع ابزار دقیق ایمنی (SIF) در مرحله تحلیل خطر و ارزیابی ریسک از چرخه عمر ایمن (Safety Lifecycle) تعیین می‌شود. این فرآیند به‌طور نظام‌مند پس از شناسایی خطرات فرآیندی و تحلیل پیامدهای آن انجام می‌شود.

۴-۱- مراحل تعیین سطح یکپارچگی ایمنی :

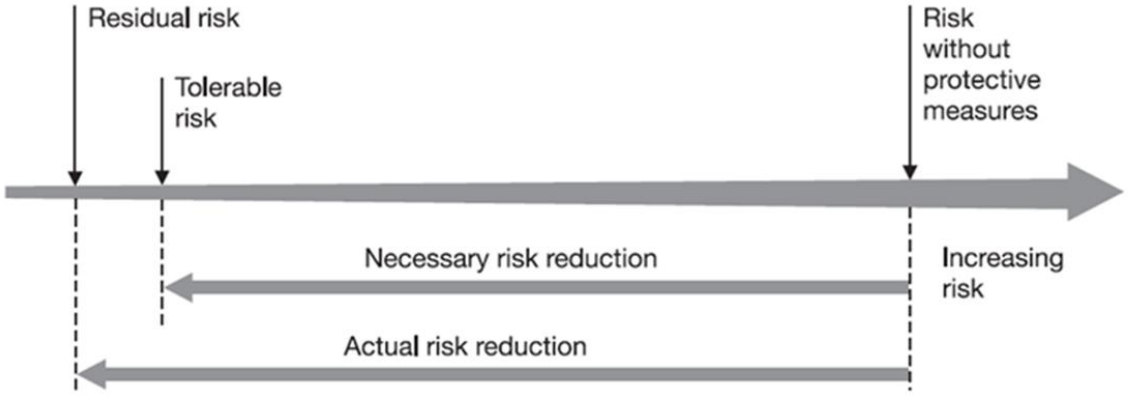
الف- شناسایی خطرات فرآیندی و تحلیل پیامدها (Hazard & Consequence Analysis) :استفاده از روش‌های معتبر مانند HAZOP و FMEA به منظور شناسایی سناریوهای خطرناک و ارزیابی پیامدهای احتمالی آنها.

ب-ارزیابی ریسک ذاتی (Inherent Risk Assessment) : تعیین احتمال وقوع و شدت پیامدهای هر سناریو پیش از اعمال لایه‌های حفاظتی، به‌منظور شناخت و ارزیابی سطح ریسک فرآیند.

ج-بررسی اثربخشی و استقلال لایه‌های حفاظتی موجود (Independent Protection Layer – IPL) :ارزیابی عملکرد لایه‌های حفاظتی موجود شامل سیستم های کنترل فرآیند پایه، سیستم های نظارت بر آتش و انتشار گاز(FGS)، توابع ابزاردقیق ایمنی موجود و سایرIPL ها در کاهش ریسک فرآیندی مورد نظر و بررسی میزان استقلال هر لایه .

د-محاسبه ریسک باقی‌مانده و مقایسه آن با ریسک قابل قبول (Residual Risk vs Tolerable Risk) :

تعیین اینکه , آیا ریسک باقی‌مانده با اعمال لایه‌های حفاظتی موجود، در محدوده قابل قبول قرار می گیرد و یا اینکه نیاز به اقدامات تکمیلی می باشد.



ه-تخصیص توابع ابزاردقیق ایمنی و بررسی اثربخشی آنها:

در صورتی که ریسک باقی مانده بیش از سطح ریسک قابل تحمل برای سازمان باشد , نیاز به کاهش ریسک تا سطح قابل قبول با استفاده از توابع ابزاردقیق ایمنی (SIF) می باشد و با تخصیص توابع ابزاردقیق ایمنی , اثربخشی جهت کاهش ریسک به سطح قابل قبول , مورد بررسی و ارزیابی قرار می‌گیرد.

و-محاسبه و مستندسازی SIL مورد نیاز:

پس از ارزیابی اثربخشی توابع ابزاردقیق ایمنی، سطح یکپارچگی ایمنی (SIL) مورد نیاز برای هر تابع ابزاردقیق ایمنی تعیین و مستند می‌شود. این مرحله شامل محاسبات کمی سطح یکپارچگی ایمنی , بر اساس شاخص‌هایی مانند احتمال خرابی در هنگام تقاضا (PFDavg)و ضریب کاهش ریسک (RRF) است .

۲-۴- اهمیت فرآیند ارزیابی و تعیین سطح یکپارچگی ایمنی (SIL) :

هدف اصلی این فرآیند، اطمینان از این است که هر تابع ابزار دقیق ایمنی در سطح SIL تعیین‌شده، قابلیت کاهش ریسک مطابق با طراحی را داشته باشد و خطرات فرآیندی به سطح قابل قبول کاهش یابند. اجرای دقیق این مراحل، پایه‌ای بر ایجاد برنامه‌های نگهداری، تست اثبات عملکرد و بازنگری‌های دوره‌ای را فراهم می آورد و تضمین‌کننده عملکرد ایمن و پایدار توابع ابزاردقیق ایمنی در طول چرخه عمر یک سیستم ابزاردقیق ایمنی است.

۵- حفظ یکپارچگی ایمنی و لزوم انجام تست‌های اثبات عملکرد (Proof Test) :

حفظ یکپارچگی ایمنی در فاز بهره‌برداری و نگهداشت جهت یک سیستم ابزاردقیق ایمنی(SIS) ، یکی از الزامات کلیدی استانداردهای IEC 61511 و ISA TR84.00 به شمار می‌رود. از اینرو به‌منظور کنترل و محدودسازی نرخ خرابی ها و همچنین کشف و رفع به‌موقع خرابی‌های خطرناک پنهان ,اجرای منظم تست‌های اثبات عملکرد (Proof Test) جهت توابع ابزاردقیق ایمنی یک ضرورت حیاتی محسوب می‌شود.

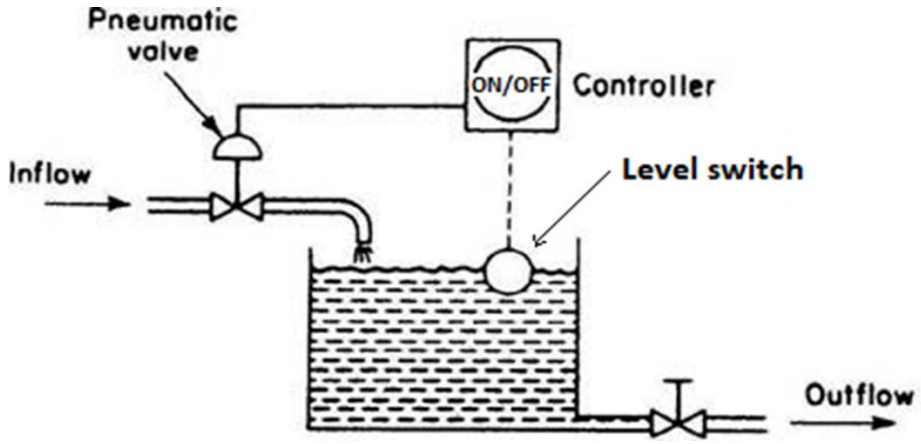
۵-۱- ضرورت انجام تست‌های اثبات عملکرد(Proof Test) :

تجهیزات ابزاردقیق ایمنی در طول چرخه عمر خود با نرخ خرابی‌های تصادفی (λ) مواجه هستند که این نرخ خرابی ها در مراحل مختلف عمر تجهیز ثابت نبوده و به‌ویژه در فاز فرسودگی (Wear-out Phase) به‌طور چشمگیری افزایش می‌یابد. از اینرو عدم اجرای به‌موقع تست‌های اثبات عملکرد جهت توابع ابزاردقیق ایمنی منجر به موارد زیر خواهد شد:

- افزایش میانگین احتمال خرابی در هنگام تقاضا(PFD avg)
- کاهش سطح دسترس‌پذیری (Availability) و عملکرد تجهیزات
- از بین رفتن اعتبار سطح یکپارچگی ایمنی (SIL) طراحی‌شده و عدم انطباق با الزامات استانداردی
- افزایش ریسک بروز حوادث فاجعه‌بار

در صنایع فرآیندی به ویژه صنایع نفت, گاز و پتروشیمی , توابع ابزار دقیق ایمنی(SIF) غالبا در حالت Low Demand عمل می‌کنند؛ یعنی تا زمانی که تقاضای واقعی از سمت فرآیند ایجاد نشود ,SIF عملاً غیرفعال است.

به عنوان مثال یک تابع ابزاردقیق ایمنی ساده را برای کنترل سطح یک مخزن که شامل یک سنسور اندازه گیری سطح و یک شیر قطع کننده در ورودی به آن می باشد , در نظر بگیرید که از سرریز شدن مخزن جلوگیری می کند. در صورتی که تقاضایی صورت نگیرد شیر قطع کننده باز است و هیچ راهی وجود ندارد که بدانیم در صورت تقاضا، قطعا شیر بسته خواهد شد یا خیر .



به طور ایده آل انتظار می رود که در صورت تقاضا شیر حتما بسته خواهد شد و از سرریز شدن مخزن جلوگیری می نماید , حال اگر سیستم به تازگی و به طور کامل تست و آزمایش شده باشد(تست اعتبار سنجی) در روز اول پس از راه اندازی ، احتمال بسته شدن شیر (در صورت تقاضا) بسیار زیاد است . با این وجود اگر تقاضای دیگری وجود نداشته باشد، احتمال بسته شدن شیر مورد نظر پس از گذشت ۳۶۵ روز (پس از ۱ سال) و یا ۳۶۵۰ روز (پس از گذشت ۱۰ سال) چقدر است؟

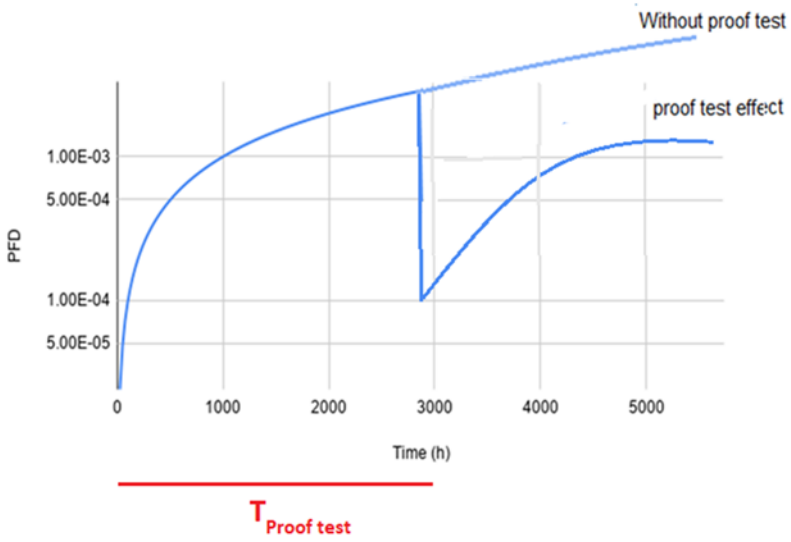
پاسخ به این سوال بسیار دشوار خواهد بود با این حال، به سهولت درک می شود که بدون انجام ارزیابی و سنجش صحت عملکرد , احتمال وجود یک خطای ناخواسته ویا خرابی های خطرناک آشکار نشده در یک سیستم ابزاردقیق ایمنی با گذشت زمان افزایش می یابد.

بنابراین حتی اگر سیستم در تست اعتبارسنجی(Validation Test) پیش از راه اندازی که تحت عنوان تست SAT نیز شناخته می شود عملکرد کاملا صحیح داشته و تایید شده باشد ، با گذشت زمان و عدم وجود تقاضاهای واقعی، احتمال وقوع خرابی‌های خطرناک آشکار نشده (Dangerous Undetected Failures)افزایش می‌یابد و با بالا رفتن PFD_{avg}، سطح یکپارچگی ایمنی مطابق طراحی دیگر معتبر نخواهد بود .این واقعیت نشان می‌دهد که حفظ ایمنی و اعتبار سطح طراحی، مستلزم اجرای برنامه‌های منظم تست اثبات عملکرد است.

۲-۵-دوره انجام تست اثبات :

فاصله زمانی میان دو تست اثبات عملکرد، که به آن $T_{Proof\ Test}$ گفته می‌شود، معمولاً در بازه‌ای بین ۱ تا ۵ سال بر اساس سطح یکپارچگی ایمنی مورد نظر ، سیاست‌های نگهداشت و تحلیل داده‌های قابلیت اطمینان تعیین می‌شود که انتخاب نادرست این بازه می‌تواند به دو پیامد منفی منجر شود:

- فواصل بیش‌ازحد طولانی ←افزایش احتمال خرابی‌های خطرناک پنهان و کاهش سطح یکپارچگی ایمنی
- فواصل بسیار کوتاه ←افزایش هزینه‌های نگهداشت و احتمال ایجاد توقف‌های کاذب.(Spurious Trips)



۵-۳-ارتباط دوره انجام تست اثبات باPFDavg :

برای یک تابع ابزاردقیق ایمنی(SIF) ، متوسط احتمال خرابی در هنگام تقاضا بر اساس فرمول زیر محاسبه می‌شود:

$$PFDavg=\lambda du \times T$$

که در آن:

- λduنرخ خرابی‌های خطرناک شناسایی‌نشده(Dangerous Undetected Failure Rate)
- Tفاصله زمانی بین تست‌های اثبات(Proof Test Interval)

این رابطه بیان می‌کند که افزایش بازه زمانی بین تست‌های اثبات به‌صورت مستقیم موجب افزایش احتمال خرابی پنهان و کاهش سطح یکپارچگی ایمنی (SIL)یک تابع ابزاردقیق ایمنی خواهد شد.

به بیان دیگر، اگر تجهیزات یک سیستم ابزاردقیق ایمنی تنها بر اساس استراتژی عملکرد تا خرابی (Run-to-Fail) نگهداری شوند و پس از پایان عمر مفید خود مورد ارزیابی و تست قرار نگیرند، سطح یکپارچگی ایمنی (SIL) طراحی شده دیگر معتبر نبوده و عملکرد ایمن سیستم به خطر می‌افتد.

اجرای منظم تست های اثبات به منظور حفظ یکپارچگی ایمنی، کاهش ریسک های فرآیندی و اطمینان از عملکرد قابل اعتماد سیستم‌های ابزاردقیق ایمنی در تمام طول چرخه عمر امری حیاتی است.

۴-۵- اهداف تست و ارزیابی دوره‌ای توابع ابزاردقیق ایمنی :

تست و ارزیابی دوره‌ای شامل بازرسی‌های برنامه‌ریزی‌شده، نگهداری پیشگیرانه و آزمون‌های اثبات عملکرد (Proof Test) است. اجرای این اقدامات در قالب یک برنامه جامع و مدون، مزایای عملی و قابل سنجش زیر را فراهم می‌آورد:

۱. شناسایی خرابی‌های پنهان و خطرناک قبل از وقوع حادثه، که به کاهش ریسک فرآیندی منجر می‌شود.
۲. تأیید عملکرد توابع ابزاردقیق ایمنیSIF ، به‌گونه‌ای که سیستم در مواجهه با تقاضای واقعی، عملکرد ایمن خود را حفظ نماید.
۳. حفظ سطح طراحی‌شده یکپارچگی ایمنی (SIL) و تضمین اعتبار سطح ایمنی در طول چرخه عمر سیستم.
٤. صحت‌سنجی عملکرد سیستم ابزاردقیق ایمنی در شرایط بروزخطا و سناریوهای بحرانی، که اطمینان از پاسخ ایمن در شرایط واقعی را افزایش می‌دهد.
٥. مستندسازی دقیق نتایج و اقدامات اصلاحی، که پایه‌ای جهت مدیریت چرخه عمر ایمن و ارتقای مستمر قابلیت اطمینان سیستم است.

.

۶- نحوه انجام تست اثبات:

بر اساس استاندارد ISA-TR-84-00-03 تست اثبات می تواند به سه روش انجام گردد: آنلاین (با فرآیندی در حال کار) , آفلاین (در هنگام توقف ویا خاموشی فرآیند) و یا ترکیبی از روش آنلاین و آفلاین

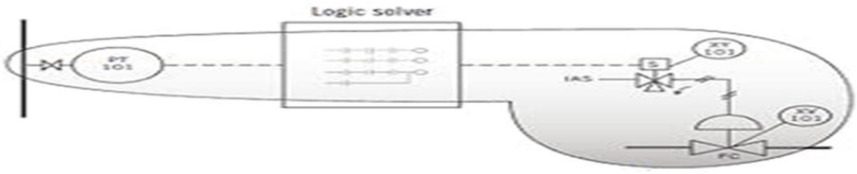
از اینرو بدلیل محدودیت های فرآیندی و یا ریسک هایی بالقوه ای که ممکن است , تست های آنلاین ایجاد نمایند , معمولا تست اثبات را به صورت آفلاین و در هنگام توقفات وخاموشی های برنامه ریزی شده انجام می دهند که به مراتب دارای فاکتور پوشش تست اثبات و کشف خرابی های احتمالی بالاتری نسبت به تست آنلاین می باشد.

ضمنا هر یک از روش های مورد اشاره می توانند به صورت کامل و یا جزئی انجام شوند:

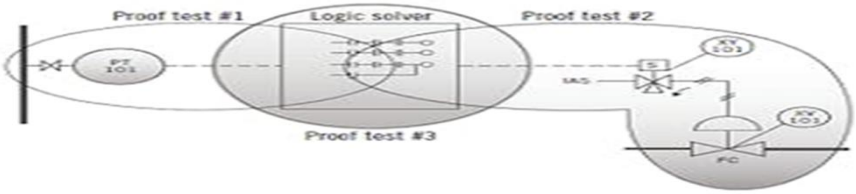
الف-تست اثبات کامل : این تست اثبات به صورت انتها به انتها ی یک حلقه (تابع ابزاردقیق ایمنی) انجام می گردد که با تحریک یک عامل ورودی به سنسور (در سطحی معادل شرایط ناایمن) و رصد نمودن تاثیر آن در منطق کنترلی و فعال شدن خروجی مورد نظر (مثلا بسته شدن یک ESDV مشخص در زمان تعیین شده) به طور هم زمان بررسی می گردد.

ب-تست اثبات جزئی : گاها انجام یک تست اثبات کامل بدلیل محدودیت های فرآیندی و ایمنی میسر نخواهد بود در این صورت تست اثبات را به صورت جزئی (بخش به بخش)انجام می دهند به عنوان مثال تست اثبات جزئی یک تابع ابزار دقیق ایمنی با تحریک یک عامل ورودی به سنسور (در سطحی معادل شرایط ناایمن) و رصد نمودن تاثیر آن در منطق کنترلی (ایجاد خروجی های لازم) در بخش اول و تحریک عناصر نهایی از طریق شبیه سازی سطح تریپ و اینترلاک ها در منطق کنترلی و فعال نمودن خروجی های مورد نظر (که به عنوان مثال باعث بسته شدن یک ESDV مشخص در زمان تعیین شده می گردد) در بخش دوم انجام می گردد .

تست اثبات کامل



تست اثبات جزئی

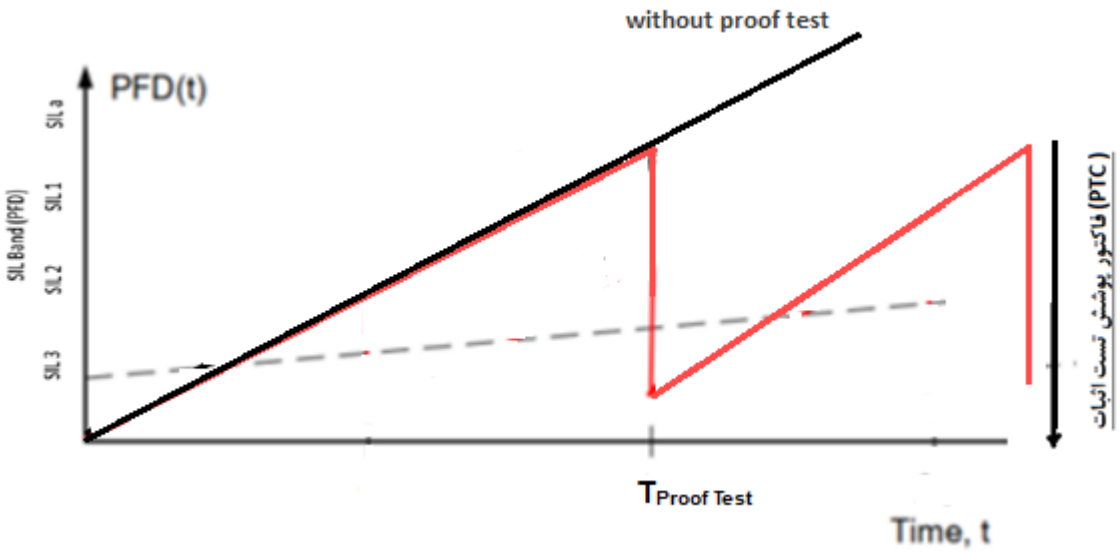


۶-۱- خلاصه روش اجرایی تست اثبات یک تابع ابزاردقیق ایمنی :

- تحریک تابع ابزاردقیق ایمنی مطابق با شرایط واقعی یا شبیه‌سازی تقاضا (تحریک سنسور به شرایط معادل تقاضا)
- بررسی عملکرد اجزای SIF شامل سنسورها، حل‌کننده منطقی و عناصر نهایی در تحریک تابع ابزاردقیق ایمنی
- بررسی عملکرد صحیح و به موقع هشدارها و نشانگرها
- مستند سازی فعالیت ها , ثبت نتایج، شناسایی خرابی‌ها و انجام اقدامات اصلاحی جهت رفع خرابی های کشف شده

۶-۲- میزان اثر بخشی تست اثبات در کاهش میزان احتمال خرابی در صورت تقاضا :

تصویر پایین , نمودار PFD بر حسب زمان مربوط به یک تابع ابزار دقیق ایمنی با سطح یکپارچگی SIL3 نشان می‌دهد که پس از حدود ۵ سال، تابع ابزار دقیق ایمنی دیگر نمی‌تواند سطح PFD را مطابق با SIL3 حفظ کند و PFD به مرز SIL1 می‌رسد که با انجام تست اثبات , مشاهده می شود میزان PFD مجددا به سطح SIL3 بر می گردد.



میزان اثر بخشی تست اثبات در کاهش PFDavg به آشکار شدن تعداد خرابی های خطرناک پنهان بستگی دارد که تحت عنوان فاکتور پوشش تست اثبا ت (PTC) بیان می گردد. در بین انواع تست های اثبات , تست آفلاین کامل , بالاترین سطح اثر بخشی را دارد و بطور ایده آل می تواند میزان PFDavg یک تابع ابزاردقیق ایمنی را به سطح اعتبار سنجی (اولین تست اثبات در زمان راه اندازی)برگرداند.

در مرحله طراحی و در غیاب تعیین روش‌های تست اثبات ، معمولاً طراح سیستم ابزاردقیق ایمنی فرض می‌کند که تمام تست های اثبات کامل و بی نقص با فاکتور پوشش ۱۰۰٪ انجام خواهند شد و هر بار که مؤلفه‌های توابع ابزاردقیق ایمنی تحت تست اثبات قرار می‌گیرند، سطح PFD به سطح SIL طراحی برمی‌گردد , اما این در حالی است که عملا دستیابی به یک تست اثبات بی نقص یا دستیابی به پوشش تست ۱۰۰٪ غیرممکن است. این یک نقص آشکار در فرآیند طراحی و مهندسی است که شکافی بین فاکتور پوشش ایده آل و واقعی در مرحله بهره برداری و تعمیر و نگهداری ایجاد می نماید .

در واقع، به طور معمول یک تست اثبات خوب برای یک فرستنده فشار ممکن است ۹۰ درصد پوشش و برای یک دستگاه کنترل ولو ممکن است ۸۰ درصد پوشش داشته باشد , لذا این نقص در مقابل پوشش ۱۰۰ درصدی منجر به تجمع PFD (احتمال خرابی در صورت تقاضا) باقیمانده در طول زمان می گردد .

کما اینکه در نتیجه انجام تست های اثبات جزئی نیز ، تجمع PFD باقیمانده در طول زمان نسبت به تست اثبات کامل با شیب بیشتری افزایش می یابد و از آنجایی که تست اثبات جزئی تمام خرابی های پنهان خطرناک را آشکار نمی کند , میزان PFDavg مربوط به یک SIF با گذشت زمان افزایش خواهد یافت .

بنابراین از آنجایی که تست اثبات تأثیر قابل توجهی بر مقدار نهایی PFDavg دارد، ناقص بودن تست های اثبات قابل چشم پوشی نیست. اما چگونه می توان میزان تاثیر ناقص بودن یک تست اثبات را تعیین نمود؟

پاسخ : از آنجا که فاکتور پوشش تست اثبات(PTC) نشان دهنده میزان اثر بخشی و کشف خرابی های شناسایی نشده ای است که با انجام تست اثبات شناسایی می گردند , بنابراین نرخ خرابی های کشف نشده را می توان به دو بخش PT λ DU و NPT λ DU تقسیم نمود.

PT λ DU : میزان خرابی های خطرناک شناسایی نشده که می تواند با انجام تست اثبات آشکار گردد.

NPT λ DU: میزان خرابی های خطرناک کشف نشده که نمی توان آنها را با تست اثبات آشکار نمود.

PTC: فاکتور پوشش تست اثبات.

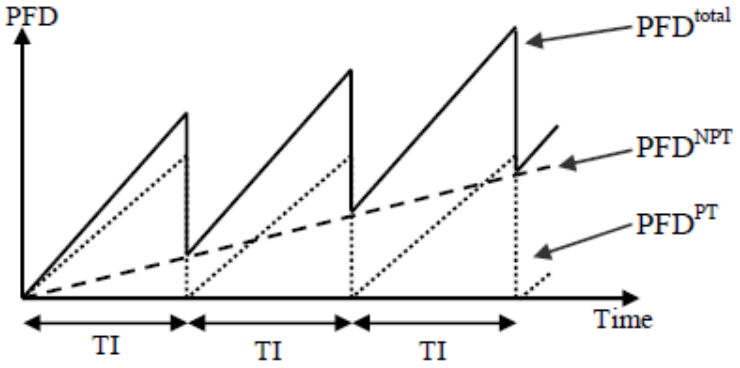
λDU :میانگین خرابی های خطرناک شناسایی نشده یک تابع ابزاردقیق ایمنی

در نتیجه از رابطه زیر می توان میزان PTC را محاسبه نمود:

$$PT\ \lambda DU = PTC \cdot \lambda_{DU}$$

$$NPT\ \lambda DU = (1 - PTC) \cdot \lambda_{DU}$$

بنابراین در محاسبه PFD کلی، باید دو نرخ احتمال خرابی در صورت تقاضا شامل PFD^{NPT} (احتمال خرابی در هنگام تقاضا ناشی از عدم آشکار شدن خرابی هایی که با تست اثبات آشکار نمی شوند) و PFD^{PT} (احتمال خرابی در هنگام تقاضا ناشی از آشکار شدن خرابی هایی که می توان با تست اثبات آشکار شوند) را محاسبه نمود و در نهایت با جمع جبری آنها در هر بخش از منحنی PFD بر حسب زمان ، می توان مقدار PFD کلی را بدست آورد (نمونه ای از آن در شکل زیر نمایش داده شده است):



همانطور که پیشتر به آن اشاره شد تست اثبات کامل به صورت انتها به انتها ی یک حلقه (تابع ابزاردقیق ایمنی) انجام می گردد که با تحریک یک عامل ورودی به سنسور (در سطحی معادل شرایط ناایمن) و رصد نمودن تاثیر آن در منطق کنترلی و فعال شدن خروجی مورد نظر (مثلا بسته شدن یک ESDV مشخص در زمان تعیین شده) به طور هم زمان بررسی می گردد. این نوع تست می تواند سطح PFD متوسط را به حد طراحی برساند .

۷- نتیجه‌گیری

سیستم‌های ابزار دقیق ایمنی (SIS) به‌عنوان یک لایه حفاظتی مستقل و حیاتی در صنایع نفت، گاز و پتروشیمی , نقشی تعیین‌کننده در کاهش ریسک‌های فرآیندی، حفاظت و صیانت از سرمایه‌های ملی و نیروی انسانی ایفا می‌کنند. تحلیل‌های این مقاله نشان می‌دهد که حفظ یکپارچگی ایمنی در توابع ابزار دقیق ایمنی (SIF) تنها با اتکا به طراحی اصولی آنها کافی نیست؛ بلکه نیازمند ترکیبی از ارزیابی دقیق ریسک و اجرای منظم تست‌های اثبات عملکرد (Proof Test) است .

بنابراین در غیاب تست‌های دوره‌ای اثبات , نرخ خرابی‌های خطرناک پنهان و PFD_{avg} به تدریج افزایش یافته و درپی آن سطح یکپارچگی ایمنی به شدت تضعیف می گردد ؛ نتیجه‌ای که مستقیماً اعتبار طراحی و عملکرد ایمن توابع ابزاردقیق ایمنی را از بین خواهد برد.

اجرای تست‌های دوره ای اثبات , حتی با پوشش جزئی نقشی بنیادین در آشکارسازی خرابی‌های پنهان، ارتقای دسترس‌پذیری و تضمین عملکرد ایمن توابع ابزاردقیق ایمنی در شرایط بحرانی دارد. تعیین فواصل بهینه تست‌های اثبات و پایش مستمر، بر پایه تحلیل‌های قابلیت اطمینان و داده‌های حاصل از آزمون‌های پیشین، تضمین می‌کند که سطح یکپارچگی ایمنی (SIL) طراحی حفظ شده و ریسک های فرآیندی در محدوده قابل قبول باقی می ماند .

در نهایت هم‌افزایی میان مهندسی دقیق، برنامه‌های نگهداری پیشگیرانه و تست های اثبات عملکرد، بنیان پایداری و قابلیت اطمینان سیستم های ابزاردقیق ایمنی را شکل می‌دهد و این اطمینان را ایجاد می کند که سیستم های ابزاردقیق ایمنی در طول چرخه عمر خود همواره آماده واکنش سریع، مؤثر و ایمن به تقاضاهای واقعی فرآیندی خواهند بود .

منابع :

1. IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.
2. IEC 61511: Functional Safety – Safety Instrumented Systems for the Process Industry Sector.
3. ISA TR84.00.02: Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques.
4. OSHA 29 CFR 1910.119: Process Safety Management of Highly Hazardous Chemicals.