ارزیابی سطح یکپارچگی ایمنی

Assessing the level of safety integrity

در کتب لغت واژه «حادثه» به معنای **رویداد، واقعه** و یا **پیشامد** در نظر گرفته می شود و منظور از آن عمل و یا اتفاق ناخوشایند و خارج از نظمی می باشد که ممکن است خسارات مالی و یا جانی در بر داشته باشد. بنابر عقیده برخی، حادثه اتفاقی پیش بینی نشده و ناگهانی است که بدون دخالت خود شخص و در اثر یک نیروی خارجی بوجود می آید. به عبارت دیگر آنچه انسان را ناخواسته از مسیر زندگی طبیعی منحرف ساخته و برای او ایجاد ناراحتی جسمی و روانی و یا خسارات مالی نماید، حادثه نامیده می شود.

با توجه به تعریف حادثه در دایره المعارف سازمان بین المللی کار، حادثه عبارت است از یک اتفاق پیش بینی نشده و خارج از انتظار که سبب صدمه و آسیب گردد. علاوه بر تعریف کلی برای حوادث مختلف که در بالا بدانها اشاره شده در تعریف حادثه ناشی از کار، می توان به آنچه در قانون کار و تأمین اجتماعی آمده است اشاره نمود:

حوادث ناشی از کار عبارت از حوادثی است که در حین انجام وظیفه و به سبب آن برای بیمه شده اتفاق می افتد.

مقصود از **حین انجام وظیفه** تمام اوقاتی است که بیمه شده در کارگاه، موسسات وابسته، ساختمان ها و محوطه آن مشغول به کار باشد و یا به دستور کارفرما در خارج از محوطه کارگاه مأمور انجام کاری می شود. ضمنا اوقات رفت و آمد بیمه شده از منزل به کارگاه و یا بلعکس جزو این اوقات محسوب می شوند. همچنین حوادثی که حین اقدام برای نجات سایر بیمه شدگان آسیب دیده و مساعدت به آنان اتفاق می افتد حادثه ناشی از کار محسوب می گردد».

اهمیت حوادث ناشی از کار

هر ساله میلیونها حادثه ناشی از کار در دنیا اتفاق می افتد. برخی از این حوادث باعث مرگ و برخی دیگر موجب از کار افتادگی موقت می شوند که ممکن است ماهها دوام داشته باشند. حوادث ناشی از کار سبب ناراحتی افراد و زیان های اقتصادی می گردند و جامعه متحمل خسارات فراوان می شود. به همین جهت جلوگیری از این حوادث وظیفه ای مهم و اساسی است.

امروزه نیز در جهان ده ها میلیون کارگر قربانی حوادثی می شوند که منجر به کشته شدن و یا از کار افتادگی تعداد کثیری از آنها می گردد و بسیاری از فجایع صنعتی در همین کشورهای توسعه یافته روی داده است که نشان از عدم پیش بینی برخی از حوادث است، جایی که فرایندهای شناسایی مخاطرات و ارزیابی ریسک جایگاه ویژه ای پیدا می کند.

آمار حوادث ناشی از کار منجر به فوت		
سال	سازمان پزشکی قانونی (نفر)	سازمان تامین اجتماعی (نفر)
۸۷	۱۴۸۱	۸۳
۸۸	۱۲۲۴	۱۱۰
۸۹	۱۲۹۰	۱۰۹
۹۰	۱۵۰۷	۸۵
۹۱	۱۷۹۶	۱۱۳
۹۲	۱۹۹۴	۱۱۷
۹۳	۱۸۹۱	۱۲۱
۹۴	۱۴۹۴	۱۰۸

طبق آمار منتشر شده در کشورهای پیشرفته صنعتی سالانه از هر ده هزار نفر کارگر، یگی دچار سانحه شده و در نتیجه اینگونه سوانح ۵ درصد از روزهای کاری به هدر می رود. از این رو حوادث ناشی از کار از سویی سبب ناراحتی خود کارگر و یا افراد خانواده وی شده و از سوی دیگر موجب از بین رفتن سرمایه و تزلزل بنیان اقتصادی جامعه می گردد. لذا اینگونه حوادث از جنبه های زیر دارای اهمیت زیادی می باشند:

از نظر انسانی: هرگونه حادثه ناشی از کار، حتی جزئی، سبب درد و ناراحتی شخص کارگر و افراد خانواده اش گردیده و در صورتیکه حادثه شدید بوده و منجر به مرگ یا از کارافتادگی دائمی شود، این مسئله اهمیت بیشتری پیدا می کند.

از نظر اجتماعی: از آنجا که پیشرفت و ترقی هر جامعه بستگی به نیروی کار آن جامعه دارد، لذا محصول کار هر کارگر نه تنها مایه امرار معاش زندگی خود و خانواده اوست، بلکه سرمایه و پشتوانه اقتصاد یک جامعه نیز می باشد. بصورت تخمینی نزدیک به ۵۰ تا ۶۰ درصد افراد هر جامعه را افراد در سنین کار تشکیل میدهند، ولی در اصل افراد فعال جامعه، مخصوصا در کشورهایی با رشد جمعیت کم، در حدود یک چهارم کل جمعیت میباشد. حال اگر بخشی از این

افراد نیز به علت حوادث ناشی از کار نتوانند کار خود را انجام دهند، این امر سبب تزلزل در وضعیت اجتماعی جامعه می گردد.

از نظر اقتصادی: حوادث به هر صورت و درجه ای که باشد برای کارگر، کارفرما و جامعه زیان های اقتصادی در بردارد. از جمله این زیانها می توان به خسارات ناشی از وقفه در کار به علت حادثه، هزینه های درمانی و بالاخره خسارات پرداختی در مورد کارافتادگی موقت، دائم و یا فوت اشاره نمود.

آنچه همواره باید در سازمانها مورد توجه قرار گیرد، آنست که حوادث ناشی از کار ناشی از اعمال و شرایط ناایمنی است که پیش بینی آنها می تواند منجر به تدوین برنامه ها و انجام اقدامات پیشگیرانه گردد. برد طی تحقیقات خود و با بررسی حوادث مختلف در ۲۱ نوع صنعت و فعالیت مختلف، ۱.۸ میلیون حادثه و ۳ میلیارد نفر ساعت کار، نسبت رویدادهای ناشی از نقص و کوتاهی در انجام وظایف و خطاهای انسانی را با حوادث بزرگ بدست آورد که نتیجه آن را در شکل مشاهده می نمایید.

تفکر کنید...!!!

330000000 ..... 3000000 .....

17.5 B$ ..... 4% .....

3200000000 ..... 400000000 ..... 8000000000 .....

شکل زیر نشان می دهد که چگونه شناسایی مخاطرات و خطاها می تواند حوادث بزرگ را پیش بینی و سازمان را برای پیشگیری و مقابله آماده کند.

چرا نیاز به شناسایی خطرات داریم؟

شناسایی مخاطرات بالقوه: قلب نظام مدیریت HSE است.

شناسایی خطرات یک عمل ذاتی در انسانهاست. از زمان پیدایش انسان، همیشه خطراتی انسان و کسب وکارش را تهدید میکرد. چه خطرات حیوانات وحشی و درنده و حوادث طبیعی سیل و زلزله و آتش فشان و چه تغییرات آب و هوایی . انسان با کسب تجربه توانست خطرات را بشناسد و با تکنیک صحیح و خطا روشهایی برای محافظت از خود دربرابر خطرات ابداع و اعمال کند.

شاید بتوان گفت اگر مهارت شناسایی خطرات و مدیریت ریسک در انسان نبود در همان ابتدا دچار انقراض میشد. روال زندگی انسان ها در طول اعصار مختلف تغییر کرد و حالا انسان با یک زندگی مدرن روبروست. اما در این زندگی مدرن نیز خطراتی او را تهدید میکند.

ما همچنان نیاز داریم خطرات را بشناسیم. بدون آگاهی از یک خطر امکان مقابله و مدیریت آن وجود ندارد.

؟؟؟ Risk and Error تفاوت خطر و خطا؟؟؟

با پیشرفت علم خطرات بیشتری شناسایی شده است.علاوه بر خطراتی که انسان را تهدید میکند، خطراتی که کسب و کارش را تهدید میکند نیز تغییر کرده و بسیار متنوع و پیچیده تر شده است. به همین علت است که امروزه نمیتوان خطرات را به سبک گذشته ارزیابی و شناسایی کرد و نیاز به تخصص و دانش دارد.

مدیریت ریسک چیست؟

خطرات همیشه قابل حذف نیستند. انسان همیشه در بستر خطرات قرار دارد. بهترین راه افزایش سلامت و ایمنی انسان در برابر خطراتی که خودش و کسب و کارش را تهدید میکند کسب مهارت در مدیریت ریسک این خطرات است.

به زبان ساده مدیریت ریسک یعنی اول خطرات را شناسایی کن. اگر میتوانی آن را حذف کن. چنانچه قابل حذف نبود سعی کن آن را با خطر کمتری جایگزین کنی. در صورتی که قابل جایگزینی هم نبود سعی کن اقداماتی انجام دهی که آسیب کمتری ببینی. و در نهایت از وسایل محافظت کننده استفاده کن.

به بیان دیگر مراحل مدیریت ریسک بصورت ذیل است:

۱. شناسایی خطرات
۲. ارزیابی ریسک
۳. ارزشیابی ریسک
۴. اقدامات مدیریتی یا مدیریت ریسک
۵. بازنگری

اقدامات مدیریت ریسک که در مرحله ۴ فرایند مدیریت ریسک آمد نیز شامل ۵ مرحله است:

- **حذف خطر**
- **جایگزینی خطر**
- **اقدامات مهندسی**
- **اقدامات مدیریتی**
- **استفاده از تجهیزات حفاظت فردی**

همانطور که مشاهده کردید، همه چیز از شناسایی خطرات شروع می شود:

انواع مخاطرات شغلی:

انواع مخاطرات شغلی شامل ۵ دسته فیزیکی، مکانیکی، شیمیایی، ارگونومی و بیولوژیکی است.

مخاطرات فیزیکی

خطرات فیزیکی خطراتی هستند مانند سر و صدا، نور ، سرما و گرما، تشعشعات و...

خطرات فیزیکی خطرات ناشی از محیط هستند که بدون دخالت و اشتباه افراد هم وجود دارند.خطرات فیزیکی در محیط فیزیکی اطراف فرد وجود دارد.

مخاطرات مکانیکی

پرتاب اجسام، خطر گیر کردن در ماشین آلات ، برخورد با بیل مکانیکی و...

این خطرات خطراتی هستند که به واسطه حرکت و انرژی که در مواد پیرامونی ما قراردارند به وجود آمده اند. این خطرات عموما به واسطه خطای فرد یا اشتباه کارگران به وجود می آیند. خطرات مکانیکی عموما در ارتباط با فرد و ابزارآلات و ماشین آلات اتفاق میافتد.

مخاطرات شیمیایی

خطرات شیمیایی آن دسته از خطراتی هستند که در مواجهه با مواد شیمیایی وجود دارد. مواجهه با اسید ها یا گازهای سمی و موارد مشابه آن در این طبقه بندی قرار میگیرد.

مخاطرات ارگونومی

خطراتی که سلامتی انسان را به واسطه پوسچر نامناسب هنگام کار تهدید میکند در این دسته میگنجد. این خطرات هم در کارهای بدون حرکت و تقریبا ثابت و هم در کارهای پر تحرک میتواند وجود داشته باشد. غالبا این تصور وجود دارد که در هنگام کار با کامپیوتر باید پوسچر مناسب داشته باشیم اما پوسچر مناسب در حمل بار و هرکار دیگری نیز باید رعایت شود.

نحوه صحیح انجام کار در بهترین حالت ممکن برای هر نوع فعالیتی قابل اجراست.

مخاطرات بیولوژیکی

عوامل بیولوژیکی مثل قارچ ها، ویروس ها، باکتری ها و عوامل بیماری زای دیگر خطرات بیولوژیکی هستند.

مخاطرات روانی

این دسته از خطرات در برخی منابع به عنوان یک دسته بندی جداگانه در نظر گرفته نمیشوند. به هر حال امروزه توجه زیادی به تنش ها و مسائل روانی محیط کار میشود.همانطور که میدانید استرس شغلی یکی از خطرات روانی شایع و مخرب در میان انواع محیط های کاری است. استرس شغلی و هیجانهای منفی روانی در محیط های کاری مثالهایی از خطرات روانی محسوب میشوند.

قانون کار ماده ۹۰ ماده ۹۵ ماده ۹۱

تامین اجتماعی ماده ۶۰ ماده ۶۵

انواع روش های شناسایی خطر

برای شناسایی خطرات در محیط های کار چند روش وجود دارد. توصیه میشود از همه این روشهای استفاده شود. استفاده همزمان از این ابزارها کمک میکند تا هیچ خطری از چشم شما پنهان نماند. ممکن است بعضی از استانداردها سخت گیرانه تر باشد. اولویت در شناسایی خطرات باید طبق نظر مدیریت اعمال شود.

مقررات و آیین نامه ها

عموما در آیین نامه ها تمام خطرات فعالیتها مشخص میشود. با توجه به الزاماتی که در این مستندات موجود است حتی اگر به طور مستقیم به خطرات اشاره نشده باشد به طور ضمنی قطعا اشاره شده است. باید این مستندات را به دقت مطالعه کنید تا هیچ نکته ای از قلم نیفتد.

استفاده از دستورالعمل ها و روش های اجرایی

دستورالعمل ها و روش های اجرایی هر شرکت و یا کارفرمای آن شرکت، همیشه مرجع مورد استفاده قابل اطمینانی محسوب میشود. عموما این دستورالعمل ها را بر اساس حوادث سابق و متون مرجع یا راهنمای سازنده های دستگاهها و مواد تدوین میکنند.

استفاده از چک لیست ها

چک لیست ها یکی از مراجع متنوع برای شناسایی خطر است. انواع چک لیست ها برای هر فعالیت یا دستگاهی وجود دارد که با الگو برداری از موارد آن پی به خطرات و حتی نحوه کنترل آنها میبرید.

استفاده از استانداردها

استانداردهای جهانی یا ملی مختلفی در امور مختلف وجود دارد که حتی میتواند شامل استانداردهای آموزشی و سرفصل های مورد تایید باشند نیز مرجع شناسایی مخاطرات شغلیست.

بعد از اینکه خطرات محیط های کاری مشخص شدند وارد مرحله ارزیابی ریسک میشویم. خطراتی که در مرحله قبل کشف شدند در ارزیابی ریسک باید به دقت مورد مطالعه قرار گیرند و عدد ریسک آنها و سطح ریسک انها طبق یک روش مناسب محاسبه شود.

مقدمه ای بر تحلیل ریسک و یکپارچگی سطوح ایمنی

آنالیز خطر فرآیند (PHA)

Process Hazard Analysis یا تجزیه و تحلیل خطر فرآیند

معمولاً اولین تلاش در فرایند آنالیز ایمنی سیستم به منظور شناسایی و طبقه بندی خطرات مرتبط با فعالیت یک سیستم، فرایند یا روش کار است که ترجیحاً در فاز توازن و ایده و تفکر از چرخه عمر سیستم اجراء می شود.

یک سیستم در طول مدت زندگی خود، مراحل گوناگون و برهه های زمانی را پشت سر می گذارد. به برهه های زمانی و مراحلی که یک سیستم در طول مدت فعالیت خود از احساس نیاز اولیه به سیستم تا فعالیت و در نهایت متروک شدن سیستم می گذراند چرخه حیات یا چرخه عمر سیستم می گویند. هر برهه زمانی و مرحله چرخه حیات سیستم، خصوصیات خاصی را دارد.

فازهای عمر یک سیستم که در آنها لازم است با به کارگیری روش های مناسب به شناسایی خطرات پرداخته شود عبارت اند از:

۱. **فاز نظری، ایده یا تفکر**: در این فاز اهداف و روند و مسیر پروژه مشخص می شود. همچنین توصیف کلی پروژه و اینکه چه نتایجی موردنظر بوده و همین طور شناسایی خطرات و لیست کردن آنها صورت می گیرد. جمع آوری این اطلاعات با استفاده از سوابق و اطلاعات کارخانه های مشابه صورت خواهد گرفت. مدیریت ایمنی در این مرحله برنامه ایمنی سیستم را تدوین می کند و دستگاه های موردنیاز ایمنی و تست های لازم مشخص شده و برای تهیه آنها اقدام می شود.

۲. **فاز طراحی**: در فاز نظری طرحی کلی از پروژه وجود دارد ولی در فاز طراحی، طرحهای پروژه به صورت اختصاصی تدوین می شود که در این طراحی مشخصات طراحی، سنجه های مختلف، نمودارها و نقشه ها ایجاد می گردد. در نهایت پس از ارائه طرح، طرح بازنگری شده و به مرحله بعدی یعنی ساخت وارد می شود.

۳. **فاز ساخت**: در این مرحله به تمام برنامه ها و طرحها جامه عمل می پوشانند و باید دقت داشت که عملیات ساخت دقیق صورت گیرد، زیرا ساخت اشتباه با ایمنی مغایرت دارد.

۴. **فاز تولید یا بهره وری**: در این فاز تسهیلات و دستگاه های ساخته شده مورد استفاده و بررسی قرار می گیرند.

بررسی قرار دهند، یعنی اینکه در این مرحله نظارت بسیار اهمیت دارد. در این مرحله ریسک خطر (محاسبه ریسک) باید انجام شود و چک لیست های مربوطه پر شود و شرایط خطر آفرین مشخص گردد.

۵. **فاز کنارگذاری یا انهدام**: در این فاز عمر مفید دستگاه ها تمام می شود. این فاز برای کارخانه هایی که از مواد خطرناک استفاده می کنند بسیار مهم است. از لحاظ ایمنی باید فاز دفع نیز دقیق بررسی شده و باید جایگاه مهمی را در دوره عمر یک سیستم برای این فاز قائل شد. پس از گذشت مدت زمانی از فعالیت سیستم، نیازهای جدید ایجاد شده، محیط و شرایط کاری تغییر می کند و سیستم نمی تواند انتظارات و توقعات را برآورده کند. سیستم به شکل نادرستی کار می کند. استفاده کنندگان از سیستم ارباب رجوع و کارکنان از عملکرد سیستم ناراضی هستند. سیستم با سختی حرکت می کند. این مرحله را متروک شدن سیستم می گویند. متروک شدن سیستم به معنای متوقف شدن سیستم نیست. ممکن است یک سیستم سالها به حالت متروک شده ولی به کار خود ادامه دهد.

در برخی منابع اجرای لیست مقدماتی خطر (PHL) یا Preliminary Hazard List مقدم بر PHA شمرده شود. لیست مقدماتی خطر یک روش مقدماتی شناسایی خطرات موجود مرتبط با طراحی سیستم است که با استفاده از ابزارهایی نظیر چک لیستها، ماتریس خطر، توصیف و تشریح تجهیزات، گزارش حوادث و رویدادها، بررسی سوابق مشاغل ارزیابی می شود.

پس از بررسی کلیه اطلاعات موجود می توان اقدام به تهیه لیست مقدماتی خطر کرد. یک PHL خوب را می توان برای تشکیل پایه و اساسی برای اجرای یک مطالعه PHA بیش از پیش گسترش داد. از آنجائیکه هدف اولیهPHA ، مستند سازی و انجام یک ارزیابی اولیه از خطرات شناسایی شده در مراحل بسیار ابتدائی فرایند است لذا اجرای مطالعه لیست مقدماتی خطر، در همان مراحل اولیه از چرخه عمر سیستم الزامی خواهد بود.

تکنیک PHA یا تجزیه و تحلیل خطر فرایند، مخفف عبارت Process Hazard Analysis است. در صنایع پرخطر، مانند صنایع شیمیایی و تولیدی، تدابیری برای کمک به جلوگیری از خطرات و حوادث بزرگ مانند انفجار، آتش‌سوزی و انتشار مواد شیمیایی سمی در نظر گرفته شده است؛ اما این تدابیر همیشه موثر واقع نمی‌شود. اکثر مقررات ایمنی فرایند در سراسر جهان، پس از وقوع حوادث ایمنی بزرگ وضع شده‌اند.

PHA چیست؟

PHA روشی برای ارزیابی ریسک فنی است. این تکنیک، فرایندهای صنعتی را برای شناسایی موقعیت‌های خطرناک و ارزیابی تأثیر بالقوه آن‌ها در صورت مدیریت نادرست، تجزیه‌وتحلیل می‌کند.

همان‌طور که اشاره شد اگر فرایند یا ماده با دقت مدیریت نشود، خطرات ایمنی فرایند می‌تواند منجر به پیامدهای فاجعه‌باری شود؛ بنابراین انجام یک تکنیکPHA ، برای شناسایی خطرات فرایند در اسرع وقت و اعمال اقداماتی برای کنترل آن‌ها بسیار مهم است.

تاریخچه تکنیک PHA

به‌عنوان‌مثال، یک کارخانه شیمیایی در هند به‌طور ناخواسته مواد شیمیایی خطرناکی را منتشر کرد که باعث مرگ هزاران نفر در سال ۱۹۸۴ شد. در سال‌های پس از این حادثه، هند قانون حفاظت از محیط‌زیست را تصویب کرد. موارد مهمی از این قبیل در دهه ۱۹۸۰، اداره ایمنی و بهداشت شغلی ایالات متحده را بر آن داشت تا مقررات مدیریت ایمنی فرایند (در ارتباط با مدیریت ریسک) را اجرا کند.

چرا از تکنیک PHA استفاده می‌کنیم؟

PHA توسط مقررات PSM و RMP OSHA در ایالات متحده و مقررات ایمنی فرایند و مدیریت ریسک در سراسر جهان مورد نیاز است.

این تکنیک یک تمرین مهندسی خوب است که به محافظت در برابر خطرات فرایند، آسیب به اموال، مشکلات کیفیت محصول و تبلیغات نامطلوب ناشی از حوادث کمک می‌کند. هزینه‌های مالی حوادث فاجعه‌بار، فوق‌العاده بالا است و PHA را می‌توان نوعی بیمه ارزان قیمت در نظر گرفت.

اهداف PHA

آنالیز مقدماتی خطر یک روش آنالیز نیمه کمی است که به منظور اهداف زیر صورت می پذیرید:

- شناسایی خطرات بالقوه و رویدادهای اتفاقی که ممکن است به بروز حادثه ای منجر شود.
- شناسایی اثرات این عناصر و شرایط خطرناک بر روی زیر سیستمها، سیستم، کل پروژه
- رده بندی رویدادهای شناسایی شده بر حسب ریسک آنها
- تعیین کنترلهای لازم برای خطرات و شناسایی اقدامات اصلاحی
- داده های بدست آمده از PHA یک ورودی مفید و موثر برای

بطور کلی یکسری سوالات اساسی وجود دارند که باید در هنگام اجرای PHA پاسخ داده شوند. هرچند که ممکن است تعدادی از سوالات یاد شده بسیار ساده و آشکار بنظر رسند ولی با این

وجود لازم است مورد توجه قرار گیرند زیرا در غیر این صورت پرسنل ارزیابی کننده ایمنی سیستم قادر به درک کامل و شناخت دقیق سیستم مورد مطالعه نخواهند بود. بعضی از این سوالات عبارتند از:

- فرایند یا سیستم مورد مطالعه چیست؟
- آیا افراد نیز با فرایند یا سیستم مورد نظر در ارتباطند؟
- وظیفه اصلی و همیشگی سیستم چیست؟
- آن چیزی که سیستم نبایستی هرگز آن را انجام دهد کدام است؟
- آیا قوانین و استانداردهایی در زمینه سیستم مورد مطالعه وجود دارد؟
- آیا سیستمی مشابه سیستم تحت مطالعه قبلاً مورد استفاده قرار گرفته است؟
- محصول سیستم چیست؟
- درون داد سیستم چیست؟
- برون داد سیستم کدام است؟
- منابع و حفاظ های انرژی در سیستم چه بوده و کجا قرار دارند؟
- خطرات اصلی سیستم کدامند؟
- چگونه می توان کنترل را بهبود بخشید و آیا این امر مورد قبول مدیریت واقع خواهد شد؟

نحوه انجام تکنیک PHA

- ❖ از آن‌جایی‌که روش‌های مختلفی برای انجام PHA وجود دارد، مهم است که ابتدا تیمی از متخصصان را برای هدایت فرایند انتخاب کنید. تیم‌های PHA باید شامل مهندسان، اپراتورها، تعمیر و نگهداری، سرپرستان و سایر کارکنان یا کارگرانی باشند که به خوبی با فرایند عملیاتی مورد بررسی آشنا هستند.
- ❖ رهبر تیم به‌طورکلی مناسب‌ترین روش را برای ارزیابی فرایند انتخاب می‌کند. با توجه به ایمنی فرایند و حفاظت از محیط‌زیست، یافتن خطرات مربوطه می‌تواند اولین گام در یک

PHAباشد؛ سپس انتخاب صحیح ساختاریافته‌ترین روشی که امکان شناسایی تا حد امکان خطرات را فراهم می‌کند مهم است.

❖ بطور کلی یکسری سوالات اساسی وجود دارند که باید در هنگام اجرای PHA پاسخ داده شوند. هرچند که ممکن است تعدادی از سوالات یاد شده بسیار ساده و آشکار بنظر رسند ولی با این وجود لازم است مورد توجه قرار گیرند زیرا در غیر این صورت پرسنل ارزیابی کننده ایمنی سیستم قادر به درک کامل و شناخت دقیق سیستم مورد مطالعه نخواهند بود. بعضی از این سوالات عبارتند از:

- ✓ فرایند یا سیستم مورد مطالعه چیست؟
- ✓ آیا افراد نیز با فرایند یا سیستم مورد نظر در ارتباطند؟
- ✓ وظیفه اصلی و همیشگی سیستم چیست؟
- ✓ آن چیزی که سیستم نبایستی هرگز آن را انجام دهد کدام است؟
- ✓ آیا قوانین و استانداردهایی در زمینه سیستم مورد مطالعه وجود دارد؟
- ✓ آیا سیستمی مشابه سیستم تحت مطالعه قبلاً مورد استفاده قرار گرفته است؟
- ✓ محصول سیستم چیست؟
- ✓ درون داد سیستم چیست؟
- ✓ برون داد سیستم کدام است؟
- ✓ منابع و حفاظ های انرژی در سیستم چه بوده و کجا قرار دارند؟
- ✓ خطرات اصلی سیستم کدامند؟
- ✓ چگونه می توان کنترل را بهبود بخشید و آیا این امر مورد قبول مدیریت واقع خواهد شد؟

روش‌های متداول برای PHA

روش‌های متداول برای تکنیک PHA شامل: تجزیه‌وتحلیلBowtie ، حالت شکست و تجزیه‌وتحلیل اثراتFMEA ، مطالعات خطر و عملکرد HAZOPs ، آنالیز پاپیونی، تجزیه‌وتحلیل درخت خطا FTA ، تحلیل‌های «what if» و ... هستند. در ادامه مروری کوتاه بر برخی از این روش‌های متداول داریم:

تکنیکFTA

تجزیه‌وتحلیل درخت خطا یا FTA با فهرست‌کردن پیامدهای ناموفق بالقوه و کارهای عقب‌مانده، برای شناسایی علل احتمالی شروع می‌شود.

تکنیکFMEA

یک FMEA با شناسایی «حالت‌های شکست» یا نحوه انجام یک عملیات با توجه به شکست‌های احتمالی، به ارزیابی خرابی‌های طراحی کمک می‌کند. سپس تجزیه‌وتحلیل اثرات برای ترسیم نتایج حالت‌های شکست انجام می‌شود.

تکنیک HAZOP

HAZOP ابزار سیستماتیکی است که برای ارزیابی یک فرایند صنعتی و انحرافات احتمالی با شکستن آن در مراحل کوچک و قابل مدیریت استفاده می‌شود.

تکنیک what if

تجزیه‌وتحلیل "what if" یک جلسه طوفان‌فکری ساختاریافته در مورد آنچه که ممکن است در یک فرایند عملیاتی، از خطای انسانی گرفته تا خرابی تجهیزات، رخ دهد است. هدف، شناسایی سناریوهای خطر و اطمینان از وجود اقدامات حفاظتی برای جلوگیری از وقوع این سناریوها است.

مراحل انجام تکنیک PHA

۱. انتخاب فرایند برای تجزیه و تحلیل: در این مرحله، فرایند مورد نظر را برای انجام تحلیل تجزیه و تحلیل خطر فرایند PHA انتخاب می‌کنیم.

۲. تشکیل تیم تجزیه و تحلیل خطر فرایندPHA : تیمی از افراد متخصص و متنوع را برای انجام تحلیل تجزیه و تحلیل خطر فرایند PHA مشخص می‌کنیم. اعضای تیم شامل مهندسان، اپراتورها، تعمیر و نگهداری، سرپرستان و سایر کارکنان یا کارگرانی است که با فرایند مورد بررسی آشنایی دارند.

۳. برنامه‌ریزی جلسات: جلسات مورد نیاز برای انجام تکنیک تجزیه و تحلیل خطر فرایند PHA را برنامه‌ریزی می‌کنیم که شامل تعیین زمان و مکان جلسه، تهیه دستور جلسه و تعیین وظایف اعضای تیم می‌شود.

۴. انتخاب روش: در این مرحله، یک روش تحلیلی را برای انجام تجزیه و تحلیل خطر فرایند PHAانتخاب می‌کنیم. می‌توان از روش‌های متنوعی مانندHAZOP ، FMEA، Bowtieو غیره استفاده کرد.

۵. اجرایPHA : در این مرحله، تحلیل PHA با استفاده از روش انتخاب شده انجام می‌شود. تیم PHA با توجه به روش مورد استفاده، خطرات مربوطه را شناسایی و ارزیابی می‌کنند.

۶. مستندسازی یافته‌ها: نتایج و یافته‌های حاصل از تحلیل PHA باید به‌طور کامل و دقیق مستندسازی شوند. این اطلاعات برای استفاده‌های آینده و به منظور توسعه برنامه‌های اقدام مورد استفاده قرار می‌گیرند.

۷. توسعه برنامه اقدام: با توجه به یافته‌های تحلیل PHA، برنامه اقدامات مناسب برای مدیریت و کاهش خطرات شناسایی شده تهیه شده که شامل اقدامات ایمنی، بهبود عملکرد، آموزش و آگاهی کارکنان می باشد.

چالش‌های تجزیه‌وتحلیل خطر فرایند

تجزیه‌وتحلیل خطر در فرایندها ابزاری اساسی برای ایجاد ایمنی و کاهش خطرات است و ممکن است چالش‌هایی در این فرایند وجود داشته باشد که در ادامه به آنها اشاره می‌کنیم:

کمبود داده‌های کافی: یکی از چالش‌های اساسی در تجزیه‌وتحلیل خطر، کمبود داده‌های کافی و دقیق است. برای انجام تجزیه‌وتحلیل دقیق خطرات، نیاز به داده‌های جامع و کاملی داریم که معمولاً در محیط‌های تجاری به دلیل محدودیت‌های مختلف، به‌دست‌آوردن آن‌ها مشکل است.

پیچیدگی فرایندها: بسیاری از فرایندها و فعالیت‌ها در سازمان‌ها به حدی پیچیده هستند که تجزیه‌وتحلیل خطر آن‌ها دشوار می‌شود. این پیچیدگی ممکن است باعث ایجاد تأخیر در انجام تجزیه‌وتحلیل گردد یا اطلاعات اشتباه تجزیه‌وتحلیل شود.

ارزیابی دقیق احتمال وقوع خطرات: ارزیابی دقیق احتمال وقوع خطرات یکی از مهم‌ترین مراحل تجزیه‌وتحلیل خطر است. اما تخمین این احتمال باتوجه‌به تعدادی عوامل ناشناخته می‌تواند دشوار باشد و به نتایج نادرستی منجر شود.

تفسیر نتایج: تجزیه‌وتحلیل خطر ممکن است به نتایج پیچیده و حجیمی منجر شود. تفسیر این نتایج و تشخیص اولویت‌ها و اقدامات مناسب نیاز به تخصص و تجربه دارد.

راهکارهای مواجهه با چالش‌ها

باتوجه‌به اینکه تجزیه‌وتحلیل خطر فرایند با چالش‌هایی روبه‌رو است، استفاده از راهکارهای مناسب که در ادامه معرفی می‌کنیم می‌تواند به بهبود عملکرد این ابزار کمک کند:

جمع‌آوری دقیق داده‌ها: جمع‌آوری داده‌های کافی از فرایند و حوادث گذشته می‌تواند به انجام تجزیه‌وتحلیل دقیق‌تر کمک کند.

همکاری تیمی: تجزیه‌وتحلیل خطر یک فرایند تخصصی است که نیاز به همکاری بین اعضای مختلف تیم دارد. همکاری و تبادل نظر در این زمینه می‌تواند به بهبود نتایج کمک کند.

۱- مقدمه

ALARP[۱] مجموعه قوانین پذیرش ریسک در کشور انگلستان است. این اصل بر اساس حذف یا کاهش ریسک سیستم‌ها تا حدی که عملی و از لحاظ هزینه‌ای معقول باشد بنا شده است. مطابق اصل ALARP لازم است میزان ریسک در هر سیستم تا حدی کاهش یابد که از لحاظ هزینه‌ای منطقی باشد. همچنین، ALARP را می‌توان پایین‌ترین حدی که به طور معقول عملی است، تعریف کرد.

۲- کاربرد اصل ALARP

کاربرد اصل ALARP بدین معنی است که بهترین کاری که می‌توان در شرایط فعلی انجام داد، باید صورت گیرد. مسئولین باید اقدام عملی برای کاهش ریسک را انجام دهند مگر آنکه ثابت شود این کار از نظر اقتصادی عملی نیست. بر اساس این اصل سه محدوده برای ریسک سیستم‌ها تعریف می‌شود.

۲-۱- ریسک قابل قبول[۲]

ریسک‌هایی که در زندگی روزمره و عادی وجود دارد و قابل چشم‌پوشی است. بنابر اصل ALARP، در مورد این دسته از ریسک‌ها نیز در صورت امکان و توجیه‌پذیری اقتصادی، سیاست‌های کاهش ریسک اعمال می‌گردد تا ریسک به کمترین حد عملی ممکن برسد.

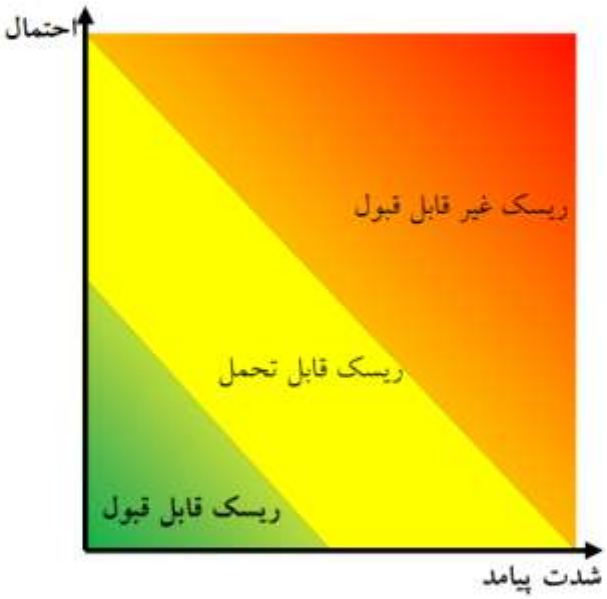
۲-۲- ریسک قابل تحمل[۳]

[۱] **A**s **L**ow **A**s **R**easonably **P**racticable
[۲] Broadly acceptable region
[۳] Tolerability region

این دسته از ریسک‌ها به دلیل اینکه از لحاظ هزینه‌ای، کاهش بیشتر آنها مقرون به صرفه نیست و همچنین دارای منفعت بیشتری در مقایسه با ریسک حاصل هستند، در صورتی که از ابزارهای کنترل ریسک، مانند برچسب‌های هشدار دهنده استفاده گردد، مورد پذیرش قرار می‌گیرند.

۲-۳- ریسک غیر قابل قبول[۴]

این ریسک‌ها تنها در موارد خاص از قبیل آتش‌نشانی و نجات غریق پذیرفته می‌شوند. در سایر موارد، به دلیل اهمیت مبحث ایمنی و جان انسان‌ها، سیستم‌های با این سطح ریسک به هیچ عنوان مجوز بهره‌برداری دریافت نمی‌کنند، مگر اینکه ریسک خود را تا حد قابل قبولی کاهش دهند.



شکل ۱- اصل ALARP

همانطور که در نمودار شکل ۱ دیده می‌شود آن دسته از ریسک‌ها که احتمال وقوع آنها بالا بوده و نیز عواقب وخیمی به دنبال دارند، غیر قابل قبول هستند. این در حالی است که ریسک‌هایی با احتمال وقوع کم و عواقب ناچیز پذیرفته می‌شوند، زیرا هیچ سیستمی وجود ندارد که فاقد هر

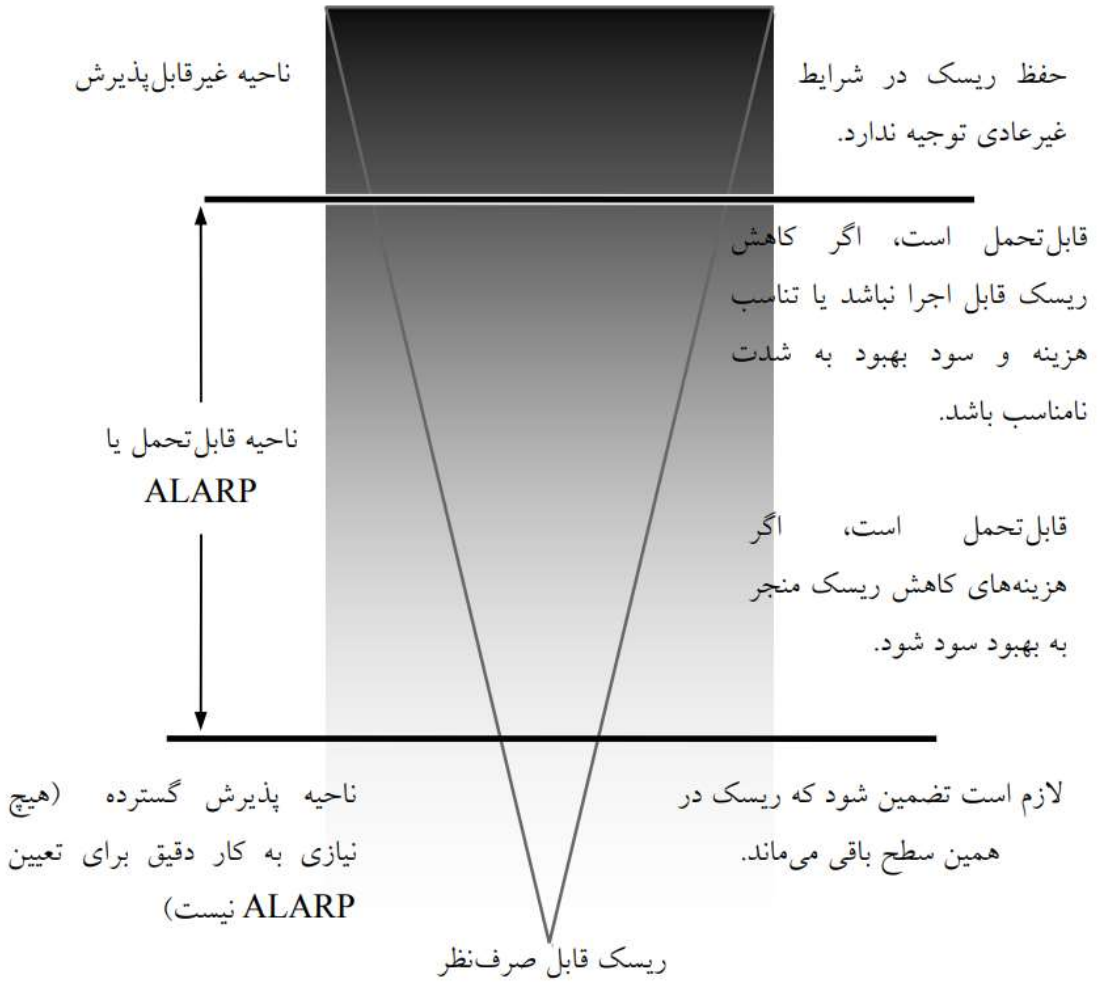
[۴] Unacceptable region

گونه ریسک باشد. آن دسته از ریسک‌ها که به دلیل عدم توجیه‌پذیری اقتصادی، کاهش بیشتر آنها مقرون به صرفه نیست در محدوده ریسک‌های قابل تحمل قرار می‌گیرند.

۳- محدوده کاربرد اصل ALARP

شکل ۲ به مثلث ALARP معروف است و نشان دهنده سه سطح ریسک مورد اشاره در بالا است. در این شکل می‌توان به صورت دقیق محدوده اصل ALARP را درک کرد.

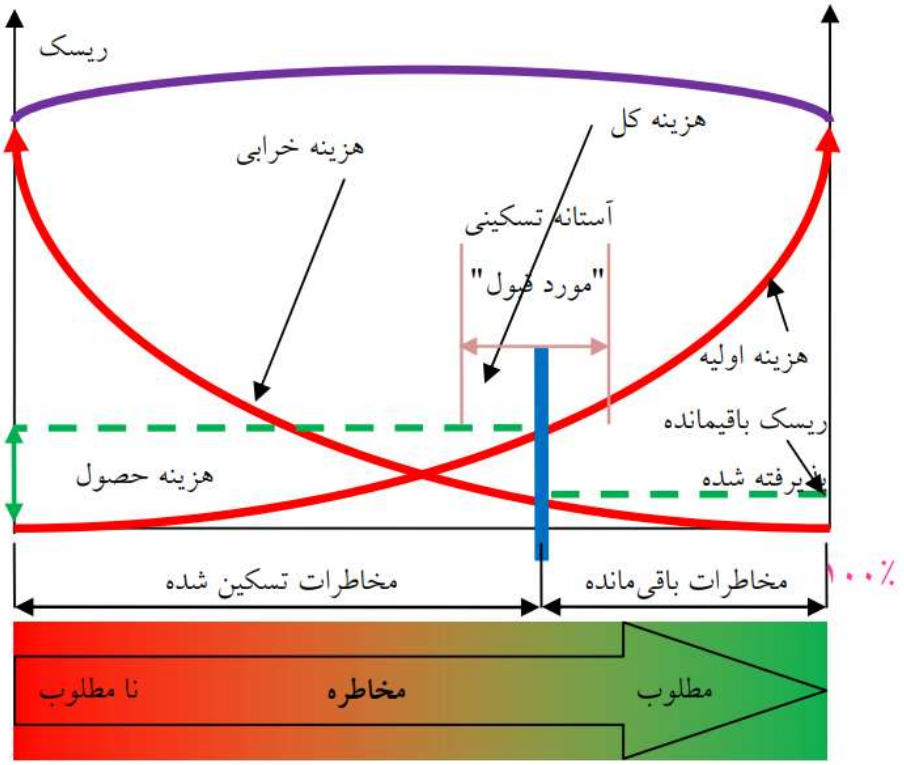
محدوده بین ریسک‌های بالا و پایین که در مثلث ALARP نشان داده شده است، شامل ریسک‌هایی است که نه آن‌چنان پایین هستند که مورد پذیرش قرار گیرند و نه آنچنان بالا هستند که غیرقابل قبول باشند. در این محدوده، تحلیل ریسک و بررسی توجیهی صورت می‌گیرد و در صورتی که منفعت طرح بیش از ریسک حاصل از اجرای آن باشد و کاهش بیشتر ریسک از نظر اقتصادی به صرفه نباشد، طرح مورد پذیرش قرار خواهد گرفت.



شکل ۲- مفاهیم ALARP

اصل ALARP، سطحی از ریسک را که قابل تحمل است فرض می‌کند و لازم است که ریسک حداقل در زیر این سطح قرار داشته باشد. اصطلاح اولیه "منطقی عملی" تعیین می‌کند که چگونه ریسک‌ها باید به سمت ریسک‌های قابل صرف‌نظر حرکت کنند. تلاش‌های بی‌نهایت می‌تواند ریسک‌ها را تا حد بی‌نهایت پایین کاهش دهد اما تلاش‌های بی‌نهایت، برای اجرا بی‌نهایت گران است. بنابراین ALARP سطحی از ریسک را در نظر می‌گیرد و هزینه برای کاهش بیشتر از آن سطح را نادرست می‌داند. در واقع، این بدان معنی است که تدابیر کاهش ریسک باید تا جایی اجرا شود که کاهش ریسک بیشتر از آن، با سرمایه‌گذاری بسیار یا سایر منابع هزینه‌ای ممکن باشد و در آن صورت میزان کاهش ریسک نامتناسب با هزینه انجام شده است.

شکل ۳ کاهش ریسک را در مقابل افزایش هزینه تسکین ریسک نشان می‌دهد. وقتی ریسک بسیار بالا است، عمدتاً سرمایه گذاری بسیار کوچک، کاهش ریسک سریعی را در پی دارد. در حالی که وقتی ریسک از سطح معینی پایین‌تر می‌آید، سرمایه‌گذاری برای کاهش ریسک افزایش پیدا می‌کند. نمودار ممکن است نقطه‌ای را نشان دهد، که آستانه پذیرش تسکین ریسک به صراحت بیان کند و نشان بدهد. برای اینکه کاهش کل نظری ریسک امکان داشته باشد، هزینه‌های تسکین به شدت بالا می‌رود. لازم به گفتن نیست که تعریف سطح ریسک و کاهش ریسک در بسیاری از صنایع معمول نیست.



شکل۳- ریسک و هزینه‌های تسکین

٤- رویکرد مبتنی بر ریسک با حضور ALARP

هدف مدیریت ریسک، اطمینان از وجود تدابیر کافی برای حفاظت افراد، محیط و دارایی‌ها از خسارت‌های پیامد پیشامدها است. نتیجه اطمینان این فعالیت‌ها می‌تواند اقتصاد پایدار یا جامعه

مطلوب باشد. مدیریت ریسک شامل دو راهکار جلوگیری از رویداد مخاطرات و کاهش پتانسیل آسیب است. با توجه به توضیحات گفته شده ریسک عبارت است از:

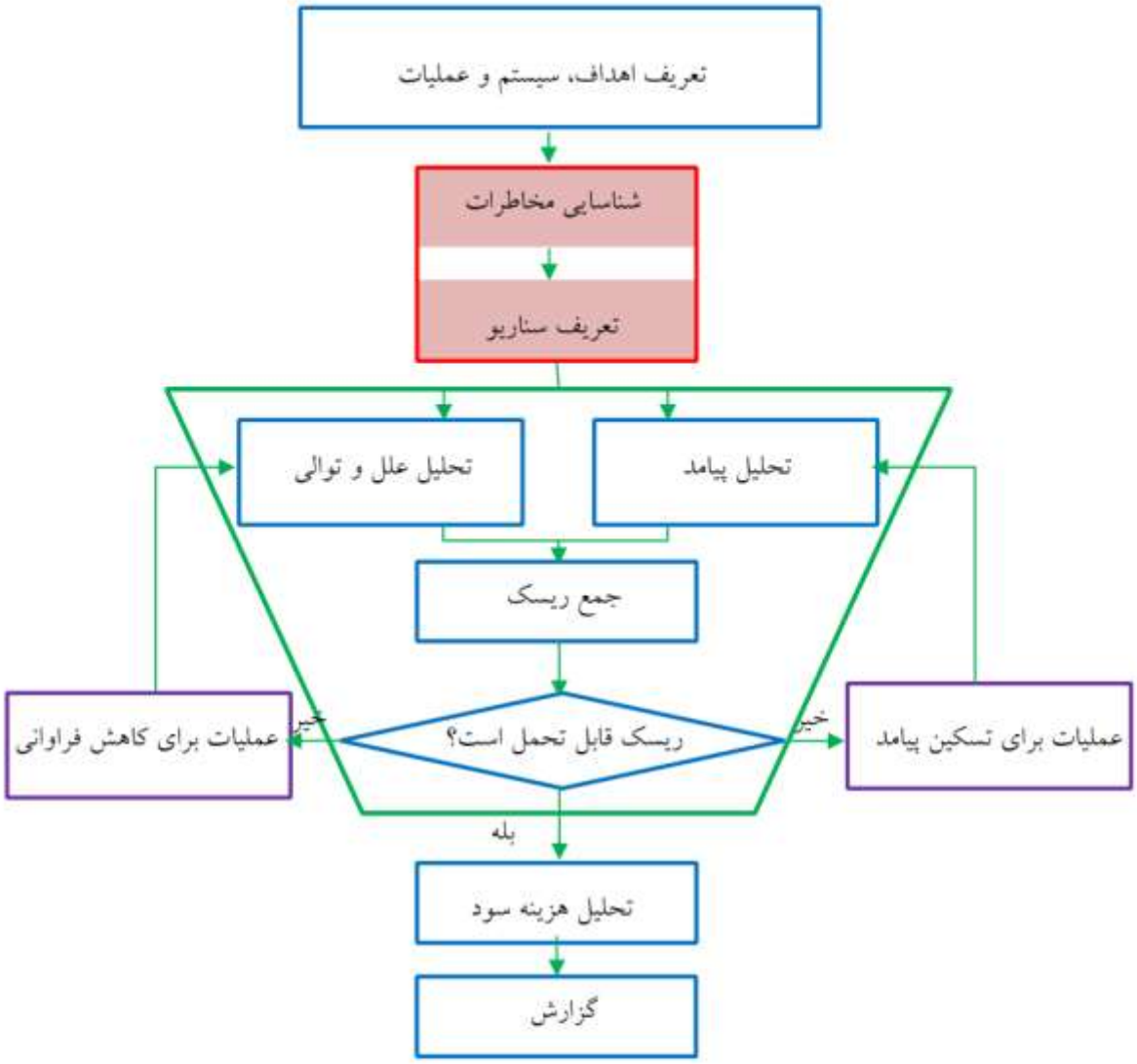
$$\boldsymbol{R = \sum_{i=1}^{n} P_{fi} \times C_{fi}}$$

R= ریسک [تلفات/سال]

Pf= احتمال خرابی در سال

Cf = پیامد پیشامد ناخواسته

بنابراین ریسک جمع تمامی مخاطرات ممکن همراه با پیامدهای آنان است.



شکل٤- مدیریت ایمنی مبتنی بر ریسک

٥- اصول ALARP

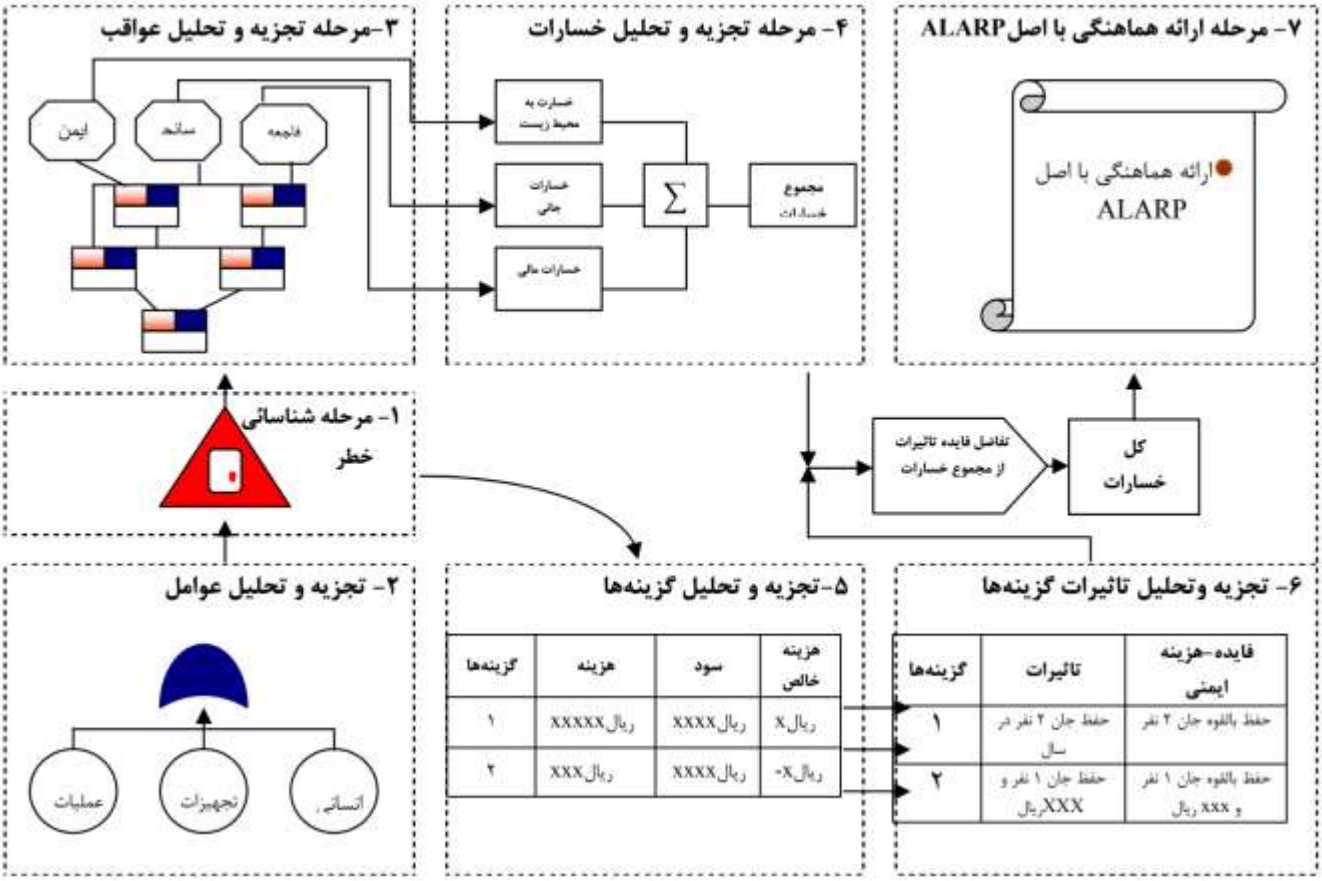
اصول ALARP دو جزء کلیدی دارد:

- کلیه تلاش‌ها باید برای کاهش ریسک تا پایین‌ترین سطح ممکن صورت بگیرد تا به نقطه‌ای برسیم که هزینه تدابیر ایمنی بیشتر، با سود ایمنی به دست‌آمده به شدت نامتناسب باشد.
- ریسک قابل تحمل است، تنها اگر پذیرش آن به وضوح دارای مزایایی باشد.

٦- اجرای اصل ALARP

هفت مرحله کلیدی برای اجرای اصل ALARP وجود دارد:

١. شناسایی و ارزیابی ماهیت ریسک
٢. بررسی و ارزشیابی کنترل‌های موجود
٣. درنظرگیری گزینه‌هایی برای کاهش ریسک بیشتر
٤. تصمیم در مورد این که کدام گزینه کنترل باید انطباق داده شود
٥. اجرای کنترل‌ها
٦. توسعه بحث ALARP
٧. پایش و بررسی ریسک‌های باقیمانده



هزینه خالص	سود	هزینه	گزینه‌ها
ریال X	ریال XXXX	ریال XXXXX	۱
ریال -X	ریال XXXX	ریال XXX	۲

فایده-هزینه ایمنی	تاثیرات	گزینه‌ها
حفظ بالقوه جان ۲ نفر	حفظ جان ۲ نفر در سال	۱
حفظ بالقوه جان ۱ نفر و xxx ریال	حفظ جان ۱ نفر و XXX ریال	۲

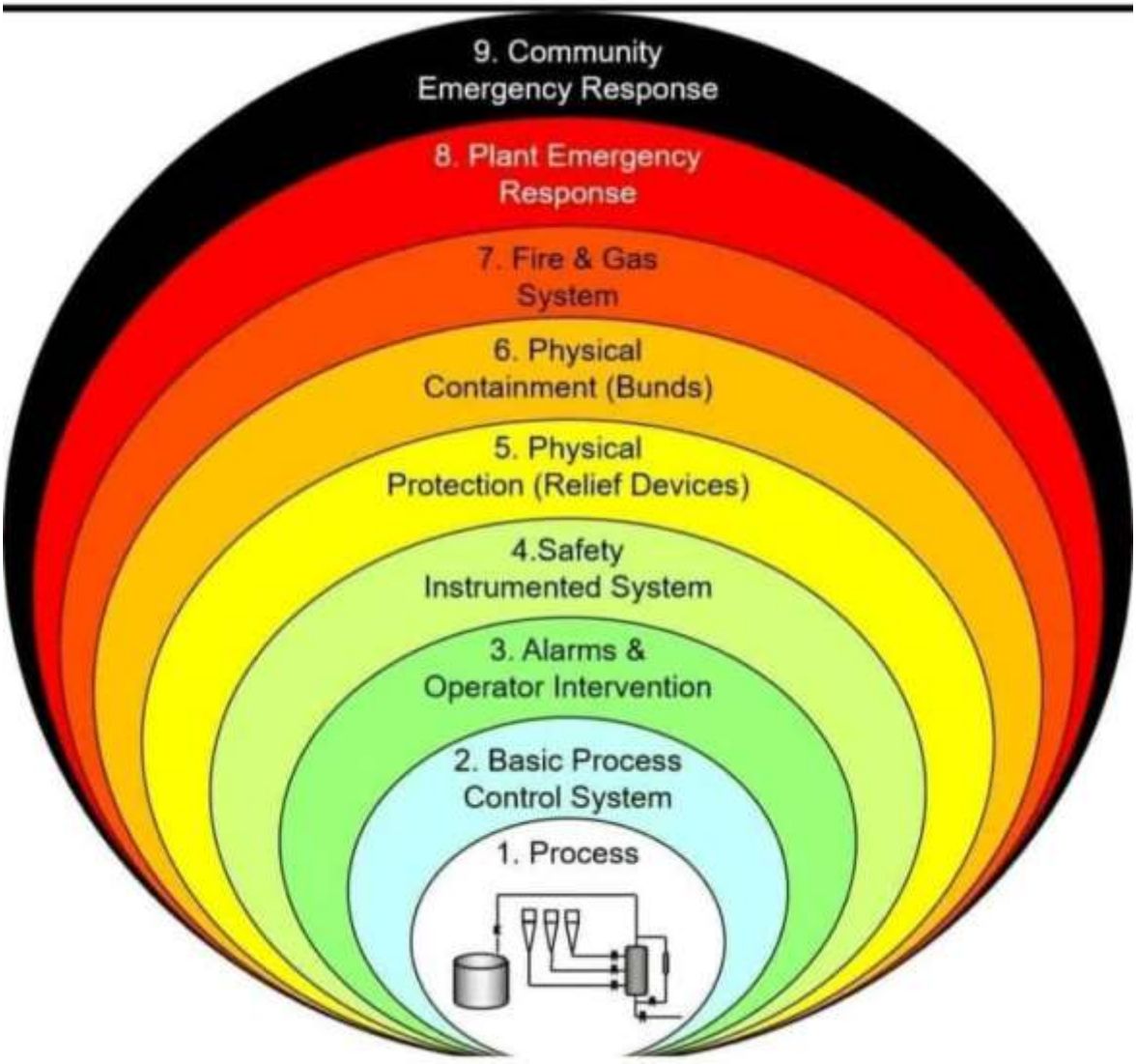
SIS SIL LOPA

IEC 61511 IEC 61508

Safety Instrumented System

Safety Integrity Level

Layers of Protection Analysis


9. Community
Emergency Response
8. Plant Emergency
Response
7. Fire & Gas
System
6. Physical
Containment (Bunds)
5. Physical
Protection (Relief Devices)
4.Safety
Instrumented System
3. Alarms &
Operator Intervention
2. Basic Process
Control System
1. Process

سطوح یکپارچگی ایمنی SIL چگونه تعریف می‌شود؟

سطوح یکپارچگی ایمنی گواهینامه SIL بر اساس استاندارد IEC 61508 تعریف می‌شود

IEC61508 یک استاندارد جهانی است که توسط کمیسیون بین‌المللی الکتروتکنیک انتشار یافته است. این استاندارد شامل روش‌هایی در مورد نحوه اعمال، طراحی، استقرار و نگهداری سیستم‌های حفاظت خودکار به نام سیستم‌های مرتبط با ایمنی (safety-related systems) است.

در استانداردهای ایمنی عملکردی (Functional safety) بر اساس استاندارد IEC 61508 ، چهار سطح برای گواهینامه SIL تعریف گردیده است که SIL4 قابل اعتمادترین و SIL1 کمترین سطح اعتماد را نشان می‌دهد. ایمنی عملکردی زمانی استفاده می‌شود که ایمنی به عملکرد صحیح یک سیستم کنترل بستگی دارد.

SIL مخفف عبارت Safety Integrity Level به معنای یکپارچگی سطح ایمنی می باشد. گواهینامه SIL یا SIL Certification ارزیابی میزان یکپارچگی سطح ایمنی در سیستم های الکترونیکی می باشدجدول زیر این چهار سطح و میزان ایمنی هر یک را نشان می دهد.

SIL level	PFD	Safety
4	0/001% to 0/01%	>99/99 %
3	0/01% to 0/1%	99/9% to 99/99%
2	0/1% to 1%	99% to 99/9%
1	1% to 10%	90% to 99%

در سطح ۱ میزان ایمنی ۹۰ تا ۹۹ درصد است یعنی میزان شکست سیستم ۱ تا ۱۰ درصد می باشد. Fail شدن عملکرد یک تجهیز PFD یا Probability of Failure on Demand به معنای احتمال شکست در لحظه تقاضا می باشد که با ایمنی (Safety) رابطه مستقیم دارد. یک ولو (شیر برقی) را در نظر بگیرید. فرض کنید از هر ۱۰ بار دستوری که به آن می دهیم یک بار دستور ما Fail شود. PFD این تجهیز ۱ بار در ۱۰ بار یعنی ٪۱۰ می باشد. هرچه PFD پایین تر باشد احتمال Fail شدن کمتر است. بنابراین هر چه سطح گواهینامه SIL یک تجهیز شماره بالاتری داشته باشد آن تجهیز ایمن تر است.

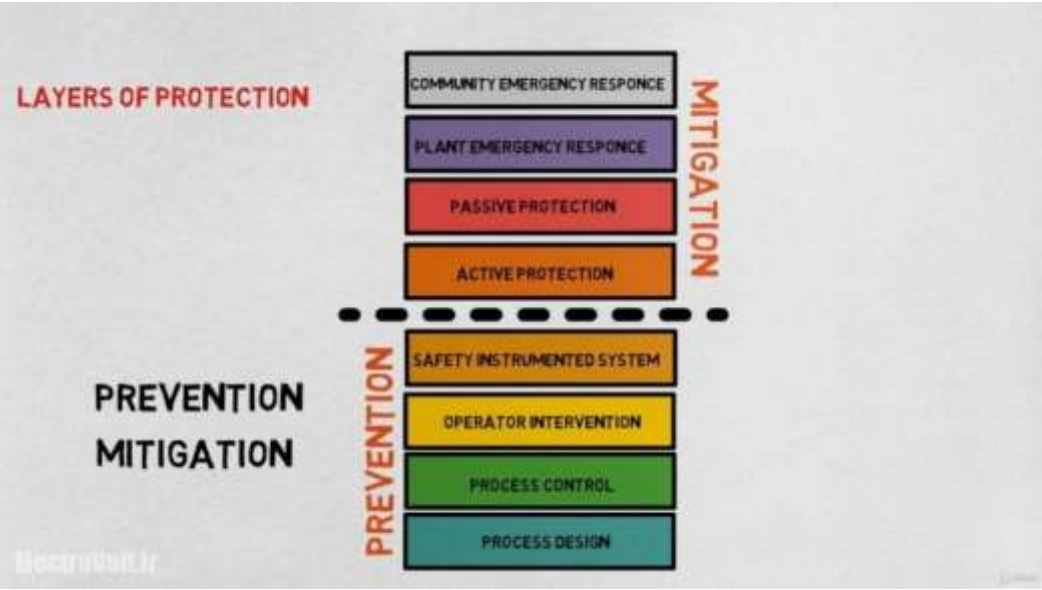
الزام دریافت گواهینامه SIL برای تجهیزات ایمنی در کاربردهای مختلف به صورت زیر تعریف می گردد:

- ✓ SIL1 کاربرد درجایی است که خسارت به تجهیزات و اموال کوچک می باشد.
- ✓ SIL2 کاربرد در جایی است که خسارت به تجهیزات و اموال بزرگ بوده و امکان مجروح شدن افراد وجود دارد.
- ✓ SIL3 کاربرد در جایی است که مجروح شدن افراد و جراحت منجر به فوت وجود دارد.
- ✓ SIL4 کاربرد در جایی است که امکان فاجعه با مرگ و میر زیاد و صدمات جدی به محیط زیست وجود دارد.

مزیت داشتن SIL بالاتر برای یک تجهیز یکی احتمال خطای کمتر آن و دیگری در دسترس بودن بالاتر عملکرد ایمنی آن تجهیز می باشد. ویژگی مهم SIL این است که بر روی کلیه توابع ایمنی پیاده سازی می شود نه بر روی یک تجهیز خاص. برای مثال یک Transmitter را در نظر بگیرید که SIL3 داشته باشد و درون شبکه ای کار کند که SIL1 باشد. در نتیجه کل شبکه SIL1 خواهد بود و صرف اینکه یک تجهیز دارای SIL3 باشد بهبودی در SIL کل شبکه ایجاد نمی شود.

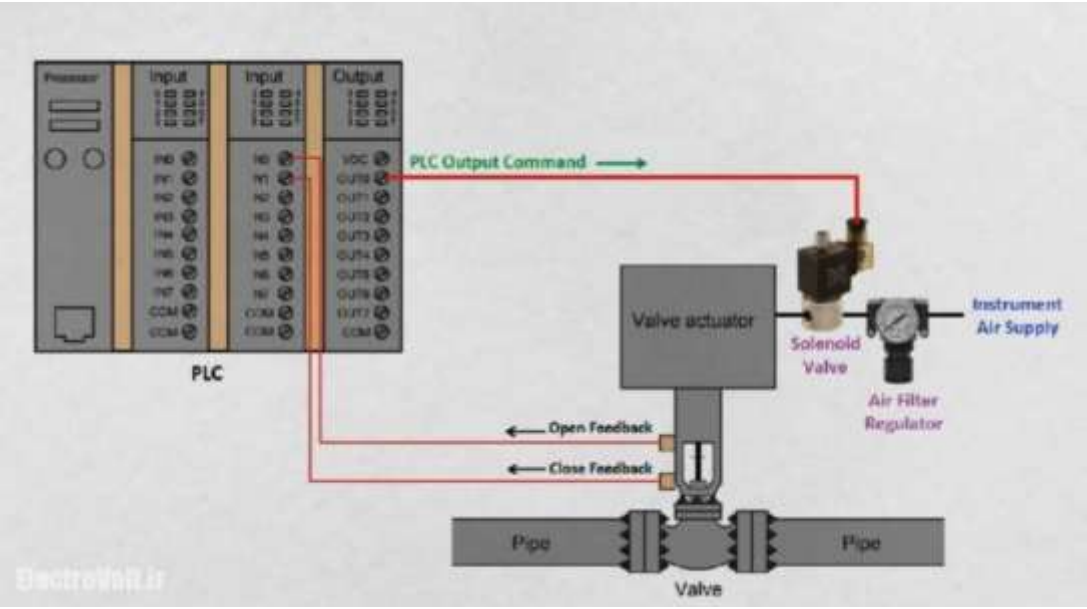
لایه های حفاظتی (Layer Of Protection)

از یک پروسه توسط لایه های مختلفی محافظت می شود تا در برابر هرگونه رخداد غیر مترقبه مقاوم باشد. به کلیه تمهیدات لازم (اعم از سخت‌افزاری و نرم‌افزاری) که برای جلوگیری از بروز حوادث یا کاهش ریسک و هم‌چنین ایمن‌سازی واحد فرآیندی بعد از بروز حادثه اندیشیده می‌شود، لایه حفاظتی گفته می‌شود به طوری‌که با استقرار این لایه‌ها، فرآیند در حاشیه امن قرار خواهد گرفت. بنابراین LOP در دو دسته اقدامات پیشگیرانه (Prevention) و اقدامات کاهشی (Mitigation) طبقه بندی می شوند که در شکل زیر مشاهده می کنید:



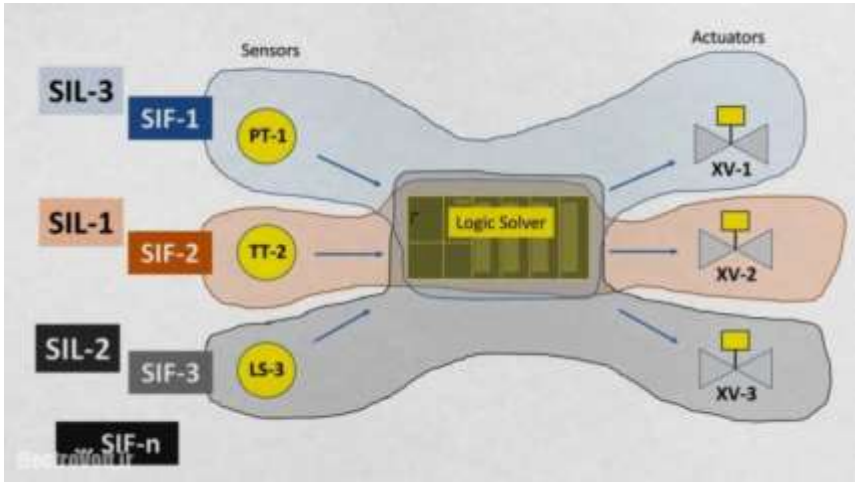
Process Design: برای پیشگیری از هر فاجعه ای اولین لایه محافظتی طراحی پروسه می باشد. پروسه باید طوری طراحی شده باشد که از مهندسین صد در صد محافظت نماید. طراحی پروسه ضعیف موجب تولیدات ضعیف، بهره وری پایین، خطای زیاد، ریسک عملیاتی بالاتر و آسیب به تجهیزات می شود.

Process Control: از آن جایی که هیچ پروسه ای ۱۰۰ درصد ایمن نمی تواند باشد بنابراین لایه دوم محافظتی کنترل پروسه می باشد. برای این منظور از سیستم های کنترل پروسه BPCS مخفف (Basic Process Control System) استفاده می شود که می توانند به صورت دائم از پروسه اصلی فیدبک گرفته و آن را کنترل نمایند.

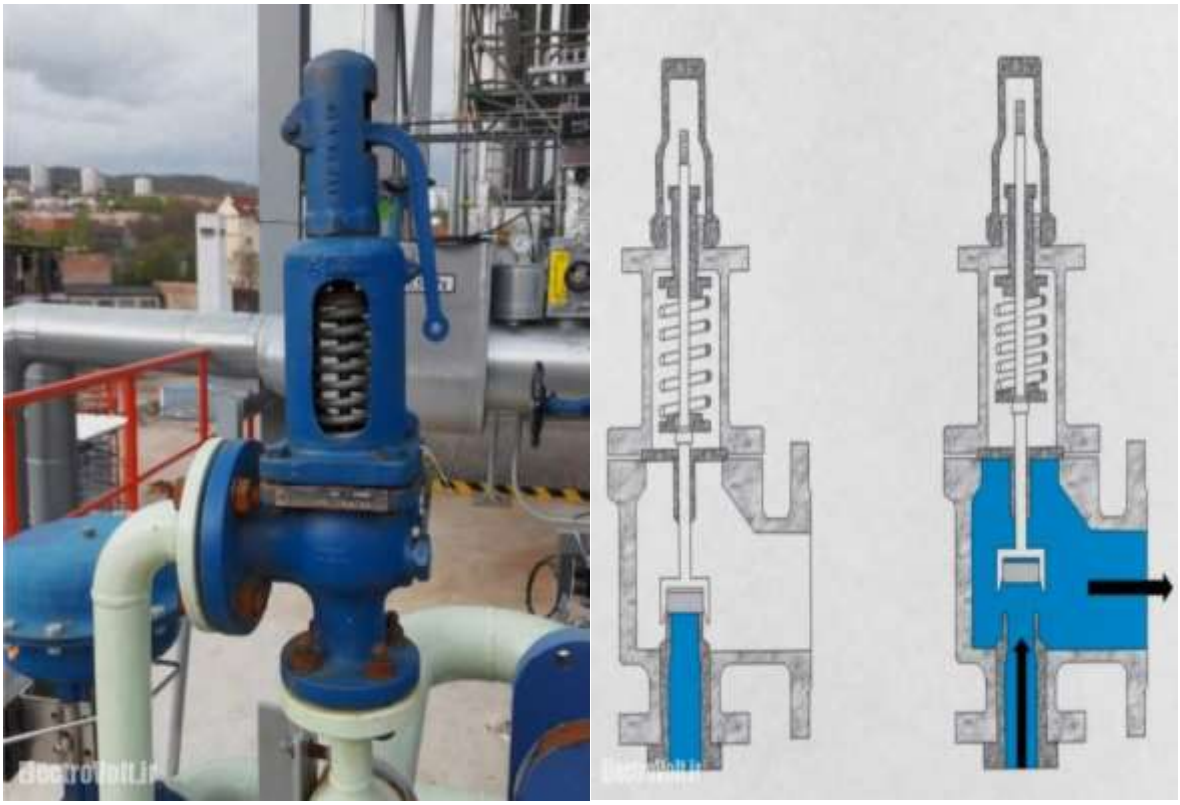


Operator Intervention: لایه سوم محافظتی، محافظت اپراتوری است که توسط کسانی که وظیفه آن ها محافظت از پروسه است صورت می گیرد. این افراد آموزش دیده اند تا در صورت بروز مشکل اقدام لازم را انجام دهند.

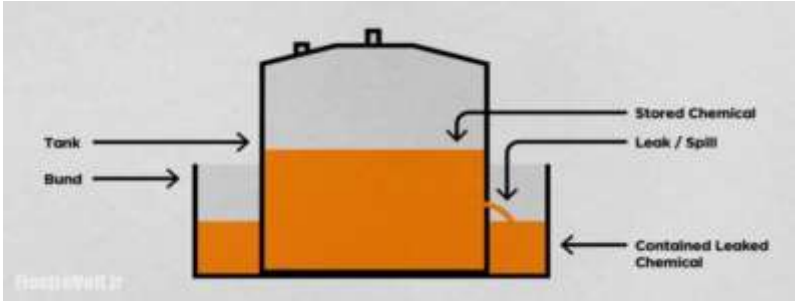
Safety Instrumented System: لایه چهارم محافظتی SIS ها می باشند. در صورتی که تمام لایه های قبلی موفق به کنترل پروسه نشوند سپس یک SIS شروع به کار می کند و با توجه به وضعیت اختلال بوجود آمده اقدام از پیش طراحی شده را اجرا می کند تا اینکه سیستم بتواند به سطوح محافظتی قبلی برگردد. در صورت عدم موفقیت این لایه دیگر بحث کاهش خسارت ها مطرح می شود.



Active Protection: در این لایه محافظتی یک سیستم همیشه فعال قرار می گیرد که در تمام طول پروسه فعال باقی می ماند. برای مثال یک شیر فشار شکن (Pressure reliefvalve) را در نظر بگیرید. در صورتی که فشار درون یک مخزن یا لوله زیاد از حد شود. دیسک کوچکی باز می شود و باعث تخلیه گاز اضافی و پایین آمدن فشار می شود.



Passive Protection: در این لایه محافظتی یک سیستم ایمنی Standby قرار می گیرد که تنها در مواقع بروز حادثه روشن (Run) می شود. برای مثال دیوار زیر را در نظر بگیرید که به منظور جلوگیری از ریختن محتویات مخزن مواد شیمیایی و نفتی روی پرسنل کارخانه استفاده می شود.



Plant Emergency Responce: در این لایه محافظتی تیم آموزش دیده و همواره آماده پالایشگاه به افراد و تجهیزات پاسخ اضطراری می دهند تا از حریق یا انفجار احتمالی جلوگیری شود.

Community Emergency Responce: در این لایه محافظتی آتش نشانی، آمبولانس و دیگر تیم های امدادی خارج از جایگاه به پرسنل و شهروندان در نزدیکی پالایشگاه در صورت بروز حادثه نظیر آتش سوزی و انفجار وارد عمل می شوند.

حالت های مختلف SIS

STATE OK: یعنی سیستم در حالت IDLE و بدون خطا می باشد.

STATE SAFE: یعنی SIS در حال اجرای عملکرد ایمنی به منظور دور کردن خطر است، تقاضا ها پاسخ داده می شود و پروسه تحت کنترل است.

STATE DANGEROUS: در حالتی که SIS نمی تواند تقاضا ها را پاسخ دهد و عملکرد ایمنی نمیتواند به درستی اجرا شود.

STATE INTERMEDIATE: حالتی که با وجود یک یا چند خطای درونی SIS میتواند تقاضا ها را تا حد امکان پاسخ دهد.

SIS STATE	PROCESS TO BE PROTECTED
OK	PROCESS IS AVAILABLE
SAFE	PROCESS HAS TRIPPED
DANGEROUS	PROCESS IS AVAILABLE, BUT, NOT PROTECTED
INTERMEDIATE	PROCESS IS AVAILABLE, SIS IS AVAILABLE, BUT IT IS TIME TO REPAIR IT

عناصر سیستم ابزار ایمنی

معمولا، سیستم ابزار ایمنی شامل ۳ عنصر است:

سنسورها:

از سنسور های میدانی برای جمع آوری اطلاعات لازم برای تعیین وضعیت اضطراری استفاده می شود. هدف این سنسورها اندازه گیری پارامترهای مورد استفاده برای تعیین ایمن بودن تجهیزات است. انواع سنسورها از سوئیچ های ساده پنوماتیک یا الکتریکی گرفته تا ترانسمیتر های هوشمند با عیب یابی روی برد متغیر است. این سنسورها به سیستم امنیتی سیستم SIS اختصاص داده می شوند.

لاجیک سالور:

هدف این عنصر در سیستم ابزار دقیق ایمنی SIS تعیین اقداماتی است که باید بر اساس اطلاعات جمع آوری شده انجام شود. از لاجیک سالورهای بسیار قابل اطمینان استفاده می‌شود که هم عملیات ایمن و هم تحمل خطا را ارائه می‌کنند. معمولاً این کنترلر است که سیگنال های سنسورها را می خواند و با دادن نتایج عناصر کنترلی به ریسک نهایی، اقدامات از پیش برنامه ریزی شده را انجام می دهد.

عنصر کنترل نهایی:

این عمل تعیین شده توسط لاجیک سالور را اجرا می کند. این آخرین عنصر کنترلی معمولاً یک شیر روشن/خاموش پنوماتیک است که توسط یک شیر برقی فعال می شود. هر سه جزء سیستم SIS باید به گونه‌ای عمل کنند که به ایزوله کردن ایمن کارخانه فرآیند در مواقع اضطراری منجر شود.