شرکت ملی پالایش و پخش فرآورده‌های نفتی ایران

دستورالعمل مدیریت موانع بر مبنای مدل پاپیون

شماره: ۲۱۷۰۰۲۶

تاریخ تصویب/ بازنگری	شرح بازنگری
۱۴۰۵/۲/۱۶	

شرکت ملی پالایش وپخش فرآورده‌های نفتی ایران

فهرست

۱ - هدف:

هدف این دستورالعمل، تبیین روش استانداردِ تهیه نمودار پاپیون، ارائه راهنمایی‌های لازم برای شناسایی و حفظ کارایی لایه‌های حفاظتی ایمنی ـ با تأکید بر اثربخشی، استقلال و کفایت آنها ـ و نهایتا مدیریت خطرات دارای ریسک بالا و تحلیل حوادث مهم در طول چرخه عمر تأسیسات است. با اینکه این دستورالعمل به شناسایی عناصر حیاتی ایمنی منتهی می‌شود و زمینه توسعه روش‌های اجرایی عملیاتی، تعیین وظایف حیاتی، حفظ ایمنی تأسیسات و پیشگیری از وقوع حوادث بزرگ را فراهم می‌آورد، اما فرایند مدیریت تجهیزات حیاتی ایمنی (از جمله چگونگی شناسایی، رتبه‌بندی و شاخص‌های مربوط به آن) را به صورت کامل بیان نمی‌کند و کاربرد اصلی آن مدیریت ریسک و تحلیل حوادث فرایندی مهم می‌باشد.

۲- دامنه کاربرد

کلیه شرکت‌های فرعی تابعه (شرکت‌هایی که بیش از ۵۰٪ سهام آنها متعلق به شرکت ملی پالایش و پخش فرآورده‌های نفتی ایران است) و شرکت های پالایشی خصوصی و واگذار شده که شامل شرکت‌های ذیل می‌شوند:

- شرکت پالایش نفت آبادان
- شرکت پالایش نفت اصفهان
- شرکت پالایش نفت امام خمینی(ره) شازند
- شرکت پالایش نفت بندرعباس
- شرکت پالایش نفت تبریز
- شرکت پالایش نفت تهران
- شرکت پالایش نفت شیراز
- شرکت پالایش نفت کرمانشاه
- شرکت پالایش نفت لاوان
- شرکت نفت ستاره خلیج فارس

۳ - تعاریف

۱-۳- نمودار پاپیون[۱]: نوعی نمایشی گرافیکی است که چگونگی وقوع یک رویداد ناخواسته، پیامدهای بالقوه ناشی از آن و روش‌های کنترل یا کاهش آن را نشان می‌دهد. آنالیز پاپیون، تهدیدها و پیامدهای مرتبط با یک خطر خاص را شناسایی کرده و موانع یا لایه‌های حفاظتی لازم برای مدیریت ریسک را تعیین می‌کند.

۲-۳- خطر[۲]: ماده، فعالیت یا شرایطی است که توانایی ایجاد آسیب به افراد، دارایی‌ها، اختلال در کسب‌وکار، یا تأثیر منفی بر محیط‌زیست و اعتبار سازمان را داشته باشد.

۳-۳- خطر مهم[۳]: خطراتی که سطح ریسک آن‌ها بر اساس ماتریس پیوست «الف» این دستورالعمل، در محدوده قرمز یا زرد قرار می‌گیرد.

٤-۳- رویداد اصلی[٤]: در زنجیره رویدادهای منتهی به حادثه، رویداد اصلی لحظه رهاشدن خطر و وقوع یک رویداد فیزیکی غیر قابل برگشت است که پتانسیل ایجاد آسیب به افراد، خسارت به دارایی‌ها، اختلال در کسب‌وکار یا تأثیر بر محیط‌زیست و اعتبار شرکت را دارد. این رویدادها معمولاً نوعی ازدست‌رفتن مهار یا آزادشدن انرژی هستند که در صورت جلوگیری از وقوع آنها، خطر فاقد اثر یا پیامد خواهند بود.

۵-۳- تهدید[۵]: اولین رویداد در زنجیره رویدادهای منتهی به حادثه است که باعث رهایی خطر می‌شود و با خارج‌کردن فرایند از وضعیت عادی به یک وضعیت غیرعادی، سناریوی وقوع حادثه را آغاز می‌کند و در صورت عدم مدیریت صحیح می‌تواند به حادثه و پیامدهای آن منجر شود. تهدید مترادف با رویداد آغازین[٦] است و نمونه‌های آن عبارت‌اند از: خرابی یا عملکرد نادرست تجهیزات، خطای بهره‌بردار، انجام ندادن اقدام مناسب توسط بهره‌بردار، یا رویدادهای خارجی[۷] مانند زلزله، حوادث مجاور، خرابکاری، اقدامات تروریستی و ...

---

[۱] Bowtie
[۲] Hazard
[۳] Major Hazard
[٤] Top Event
[٥] Threat
[٦] Initiating Event
[۷] External event

۶-۳- پیامد[۸]: آثار فیزیکی انتشار خطر بر افراد، دارایی‌ها، محیط زیست یا اعتبار شرکت است. اثرات فیزیکی شار تشعشعی حریق، افزایش فشار بیش از حد به دلیل انفجار و افزایش غلظت مواد سمی به دلیل انتشار مواد سمی بر افراد، دارایی‌های شرکت و محیط زیست پیامدهای اولیه هستند که خود می‌توانند منجر به پیامدهای ثانویه شامل توقف تولید، کاهش فروش، کاهش کیفیت محصول، تخریب تجهیزات، نقض الزامات قانونی، از دست دادن اعتبار (در نظر عموم، مشتری‌ها، سهامداران شرکت و قانون‌گذار) شوند.

۷-۳- مانع[۹]: لایه‌های حفاظتی یا اقدامات کنترلی هستند.

- اگر مانع در سمت چپ نمودار پاپیون قرار گیرد می‌تواند جلوی رهاشدن خطر توسط تهدید و تبدیل تهدید به رویداد اصلی را بگیرد که در این صورت به آن «مانع پیشگیرانه» گفته می‌شود.
- اگر مانع در سمت راست نمودار پاپیون قرار گیرد می‌تواند پیامدهای وقوع رویداد اصلی را قطع یا محدود کند که به آن «مانع محدودکننده» یا «اقدامات بازیابی» گفته می‌شود.

۸-۳- مانع انسانی[۱۰]: موانعی هستند که برای جلوگیری از وقوع رویداد اصلی یا کاهش پیامدها به عملکرد یک انسان (به عنوان بخشی از مانع) متکی می‌باشند. موانع انسانی فقط می‌توانند یک مانع فعال باشند و معمولا همراه با سخت افزار به‌کار می‌روند (مانند پاسخ بهره‌بردار به آلارم).

۹-۳- موانع سخت افزاری[۱۱]: تجهیزات یا سیستم‌های ایمنی هستند که برای جلوگیری از وقوع رویدادهای اصلی یا محدود کردن پیامدها عمل می‌کنند. این موانع می‌توانند به دو دسته فعال یا غیرفعال طبقه بندی شوند.

۱۰-۳- مانع فعال[۱۲]: مانعی است که با اجزای خود می‌تواند شرایط نیازمند اقدام را تشخیص دهد، در مورد اقدام مورد نیاز تصمیم بگیرد و اقدام لازم را انجام دهد (مانند شیر تخلیه فشار،

---

[۸] Consequence
[۹] Barrier
[۱۰] Human Barrier
[۱۱] Hardware Barrier
[۱۲] Active Barrier

اقدام بهره‌بردار، یا سیستم خاموش کردن خودکار[۱۳]). یک مانع فعالِ معتبر، باید اجزای زیر را داشته باشد تا موثر باشد:

- حسگر: برای تشخیص شرایطی که نیاز به عمل دارد.
- تحلیلگر منطقی[۱۴] : تصمیم می‌گیرد که چه اقداماتی باید انجام شود. و
- اقدام کننده[۱۵] یا عنصر نهایی[۱۶]: که برای رسیدگی به شرایط انتشار خطر، اقدام می‌کند.

موانع فعال می‌توانند سخت افزاری، انسانی و یا ترکیبی از هر دو باشد.

۱۱-۳- مانع غیرفعال[۱۷]: موانع غیرفعال معمولاً موانع سخت افزاری هستند که حضور مستمرشان باعث حفاظت می‌شوند مانند دایک اطراف یک مخزن که زمان خروج مواد از مخزن، از تشدید پیامد جلوگیری می‌کند.

۱۲-۳- اعتبار مانع[۱۸]: یک مانع معتبر در نمودار پاپیون باید دارای سه ویژگی باشد:

- **موثر**: توان کاهش احتمال وقوع رویداد اصلی را داشته باشد (در سمت چپ نمودار پاپیون) و یا بتواند از بروز پیامد جلوگیری کند یا پیامد را محدود کند (در سمت راست نمودار پاپیون).
- **مستقل**: باید از وقوع تهدید/ رویداد آغازین و همچنین از دیگر موانع در نظر گرفته‌شده برای همان شرایط، مستقل باشد.
- **قابل ممیزی**: باید از طریق بازرسی، تست، نگهداری سوابق و... ارزیابی شود و عملکرد صحیح آن در هنگام نیاز، تأیید شود.

۱۳-۳- فاکتور تخریب[۱۹]: عوامل، موقعیت‌ها یا شرایطی که کارایی مانع را کاهش می‌دهند، به آن آسیب می‌رسانند یا از آن عبور می‌کنند و ممکن است منجر به خرابی جزئی یا کامل مانع شوند. این عوامل می‌توانند بر روی موانع در سمت چپ یا راست پاپیون اثر بگذارند.

---

[۱۳] Automatic shutdown system
[۱۴] Logic Solver
[۱۵] Actuator
[۱۶] Final element
[۱۷] Passive Barrier
[۱۸] Barrier Validity
[۱۹] Degradation factor

۱۴-۳- کنترل تخریب[۲۰]: اقداماتی هستند که برای حفظ عملکرد مانع یا جلوگیری از خراب شدن عملکرد مانع توسط فاکتورهای تخریب، در نظر گرفته می‌شوند. به عبارت دیگر در طول عمر تاسیسات ممکن است موانع یا لایه‌های حفاظتی خراب شوند و در موقع نیاز عمل نکنند. برای جلوگیری از افزایش احتمال خرابی هر مانع یا لایه حفاظتی هنگام نیاز[۲۱] (PFD) باید اقدام اصلاحی تعریف شود تا جلوی تاثیر فاکتورهای تخریب بر مانع یا لایه حفاظتی را بگیرد. این اقدامات کنترلی در مسیر ارتباط بین فاکتور تخریب و مانع، قرار می‌گیرند.

لازم به ذکر است که کنترل تخریب می‌تواند شرایط لازم برای اعتبار مانع را نداشته باشد.

۱۵-۳- استاندارد عملکرد / استاندارد عملکرد یکپارچگی فنی[۲۲]: سندی که به صورت کمّی یا کیفی الزامات عملکرد یک سیستم یا یک تجهیز را تعیین می‌کند. این سند حاوی اطلاعات لازم برای تایید اثربخشی عملکرد آن تجهیز در طول چرخه عمر آن (از طراحی، ساخت، تست، راه اندازی، بهره‌برداری و از سرویس خارج کردن[۲۳]) است و به عنوان مبنایی برای مدیریت مؤثر موانع جهت جلوگیری از وقوع حادثه یا محدود کردن پیامد حادثه مهم به‌کار می‌رود.

۱۶-۳ - عناصر حیاتی ایمنی[۲۴]: هر تجهیز یا سیستم یا فرآیند مدیریتی است که در سناریوهای دارای ریسک ناحیه قرمز یا زرد، صحت عملکرد موانع سخت‌افزاری و انسانی را تضمین می‌کند.

۱۷-۳- فعالیت‌های حیاتی ایمنی[۲۵]: مجموعه وظایفی که برای توسعه، اجرا، بهره‌برداری یا نگهداری عناصر حیاتی ایمنی، تعریف می‌شوند.

۱۸-۳- سمت‌های حیاتی ایمنی[۲۶]: پست‌های سازمانی که برای مدیریت خطرات مهم مسئولیت طراحی، اجرا، بهره‌برداری یا حفظ موانع را بر عهده دارند.

۱۹-۳- سناریو[۲۷]: توالی رویدادها شامل وقوع تهدید یا رویداد آغازین و خرابی لایه‌های حفاظتی که درنهایت موجب بروز حادثه و پیامدهای خسارت‌بار می‌شود.

---

[۲۰] Degradation control
[۲۱] Probabability of Failure on Demand (PFD)
[۲۲] Performance Standard / Technical Integrity Performance Standard (TIPS)
[۲۳] Decommissioning
[۲۴] Safety Critical Element
[۲۵] Safety Critical Activities
[۲۶] Safety Critical Positions

۲۰-۳- رهبر مطالعه: رهبر مطالعه پاپیون فردی ذیصلاح است که توسط رئیس/ مدیر اداره HSE تعیین می‌شود و مسئولیت هدایت و موفقیت مطالعه پاپیون را بر عهده دارد. عملکرد او تأثیر مستقیمی بر موفقیت مطالعه و ارزش نتایج گزارش نهایی دارد. نقش کلیدی او شامل ایجاد انگیزه در تیم، زمینه‌سازی برای مشارکت اعضای تیم و بهره‌گیری از تکنیک‌هایی مانند طوفان فکری برای هدایت مؤثر تیم مطالعه است. این فرد باید دارای شرایط و صلاحیت‌های زیر باشد:

- داشتن مدرک دانشگاهی در رشته‌های مهندسی شیمی یا مکانیک.
- تسلط به روش انجام مطالعه پاپیون و سایر تکنیک‌های ارزیابی ریسک تیمی مانند HAZID، HAZOP، تجزیه و تحلیل پیامد، آنالیز لایه‌های حفاظتی و ارزیابی کمّی ریسک.
- داشتن مهارت فنی و درک عمیق از فرآیند یا عملیاتی که مورد مطالعه قرار می‌گیرد.
- داشتن مهارت‌های ارتباطی و مجری‌گری قوی.

۲۱-۳- دبیر مطالعه: شخصی مستقل از سازمان و مجرب در زمینه ارزیابی ریسک است که وظیفه اصلی، مستندسازی گفتگوهای فنی تیم و ترسیم نسخه اولیه نمودار پاپیون به عنوان خروجی تیم را بر عهده دارد. انتخاب دبیر بر عهده رهبر مطالعه است و این فرد باید دارای شرایط و صلاحیت‌های زیر باشد:

- داشتن مدرک دانشگاهی در رشته‌های مهندسی شیمی یا مکانیک.
- آشنایی با روش‌های شناسایی خطر و ارزیابی ریسک: تسلط بر روش انجام مطالعه پاپیون و آشنایی با سایر روش‌های شناسایی خطر و ارزیابی ریسک نظیر HAZID, HAZOP، تجزیه و تحلیل پیامد[۲۸]، آنالیز لایه‌های حفاظتی[۲۹] و ارزیابی کمّی ریسک.
- داشتن درک عمیق از فرایند یا عملیات خاصی که مورد مطالعه قرار می‌گیرد.
- توانایی کار با نرم‌افزارهای تخصصی مورد نیاز برای این مطالعات.

---

[۲۷] Scenario
[28] Consequence Analysis
[۲۹] LOPA

٤- مسئولیت‌ها

١-٤-مدیر عامل: کلیه شرکت‌های فرعی تابعه و شرکت‌های وابسته مسئولیت دارند براساس مفاد این دستورالعمل زیر ساخت‌های لازم جهت اجرایی شدن این دستورالعمل را فراهم نموده و از اجرای اثربخش آن در واحدهای عملیاتی/ فرایندی تحت نظارت خود اطمینان حاصل کنند.

٢-٤- رهبر مطالعه: رهبر مطالعه پاپیون مسئولیت‌های ذیل را بر عهده دارد:

- انتخاب و معرفی دبیر مطالعه
- تایید اعضای تیم جهت انجام مطالعه پاپیون و تعیین مسئولیت‌های آنها
- ارائه برنامه زمان بندی تشکیل جلسات
- تعیین فهرست اسناد مرجع مورد نیاز جهت انجام مطالعه
- برگزاری جلسات مطالعه، ایجاد انگیزه در اعضای تیم مطالعه و هدایت و رهبری آنها
- زمینه‌سازی برای مشارکت فعال تمام اعضای تیم در مطالعه.
- بهره‌گیری از تکنیک‌های گروهی مانند تکنیک طوفان فکری برای بهبود کار تیم
- هماهنگی با دبیر مطالعه و هدایت او در تهیه گزارش نهایی مطالعه
- تایید و ارائه گزارش نهایی مطالعه

٣-٤- دبیر مطالعه: دبیر مطالعه پاپیون مسئولیت‌های ذیل را بر عهده دارد:

- مستندسازی و ثبت دقیق تمامی مباحث، تصمیمات و استدلال‌های مطرح‌شده در جلسات فنی تیم مطالعه پاپیون به صورت ساختاریافته
- ترسیم و ارائه پیش‌نویس نمودارپاپیون بر اساس کار جمعی تیم
- پشتیبانی از رهبر مطالعه با مدیریت اسناد و گردش کار جلسه
- اطمینان از دقت فنی، صحّت و کامل بودن اطلاعات ثبت‌شده در گزارش نهایی با هماهنگی رهبر مطالعه

۵- مراحل اجرا:

۵-۱- شناسایی خطرات مهم

مطالعه پاپیون باید برای تحلیل خطرات فرایندی مهم و حوادث فرایندی مهم انجام شود. خطرات مهم با انجام سایر مطالعات شناسایی خطر، شناسایی شده و ریسک آنها در ماتریس ریسک در ردیف ریسک‌های ناحیه زرد و قرمز قرار گرفته است.

بنابراین شرکت‌ها باید نسبت به شناسایی خطرات فرایندی اقدام و پس از محاسبه و ارزش گذاری ریسک بر مبنای ماتریس ریسک شرکت مندرج در پیوست الف، لیست خطرات فرایندی دارای ریسک ناحیه زرد و قرمز را به عنوان خطرات فرایندی مهم تهیه نموده و جهت انجام مطالعه پاپیون اولویت بندی نمایند.

در صورت وقوع حوادث فرایندی مهم {مطابق تعریف دستورالعمل گزارش حوادث و رویدادها به شماره (۱)۲۱۷۰۰۵}، می‌بایست در فرایند تحلیل حادثه کلیه مراحل این دستورالعمل لحاظ شود.

۵-۲- آمادگی‌های لازم قبل از تشکیل تیم مطالعه

قبل از اقدام به ترسیم نمودار پاپیون می‌بایست موارد ذیل را مشخص نمود:

۵-۲-۱- تعیین رهبر مطالعه: برای انجام این مطالعه از یک رهبر ذیصلاح استفاده شود. رهبر باید مستقل از سازمان باشد یعنی توسط شخص / اشخاص ثالث (حقیقی /حقوقی) انجام گیرد.

تبصره: تنها در صورتی که مطالعه پاپیون برای تحلیل حادثه انجام می‌شود، شرکت می‌تواند از کارکنان ذیصلاح و آموزش دیده به عنوان رهبر جهت انجام مطالعه پاپیون استفاده کند.

۵-۲-۲- تعیین دبیر: انتخاب دبیر بر عهده رهبر مطالعه پاپیون است.

۵-۲-۳- تعیین اعضای تیم مطالعه: تیم اجرایی مطالعه پاپیون برحسب مسئولیت‌ها و تخصص‌ها به دو گروه تقسیم می‌گردد:

- گروه مجری شامل رهبر و دبیر مطالعه
- گروه همکاران شرکتی شامل یک نفر از کارشناسان خبره واحدهای بهره‌برداری، مهندسی، فرآیند، برق و ابزار دقیق، ایمنی فرآیند، تعمیرات و نگهداری می‌شوند که اطلاعات کاملی از موانع و کنترل‌های تخریب فرایند مورد مطالعه دارند.

تبصره: بر اساس نیاز و به تشخیص رهبر مطالعه، نمایندگان دیگر واحدها نیز می‌توانند در تیم مطالعه حضور یابند.

توصیه می‌شود رئیس واحد مورد مطالعه نیز به عنوان عضوتیم در جلسات مطالعه حضور یابد.

تعداد نفرات گروه همکاران شرکتی تیم مطالعه بین شش تا هشت نفر می‌باشد.

تمام اعضای تیم مطالعه باید آموزش تخصصی روش مطالعه پاپیون را گذرانده باشند.

اعضای تیم مطالعه پاپیون می‌بایست مشخص و قبل از آغاز مطالعه به صورت کتبی به تایید رهبر مطالعه پاپیون رسانده شود.

٤-٢-٥- تهیه اسناد مرجع: قبل از تشکیل جلسات مطالعه پاپیون، مدارک روزشده و منطبق بر شرایط فیزیکی واحد، باید توسط بهره‌بردار تاسیسات مورد مطالعه، جمع آوری شود تا به درخواست رهبر مطالعه جهت استفاده به عنوان مرجع در اختیار رهبر و اعضای تیم مطالعه قرارگیرد. این مدارک می‌تواند شامل موارد ذیل:

- نقشه‌های P&ID، نقشه جریان فرآیند[۳۰]، دیاگرام علت-اثر[۳۱]، نقشه‌های جانمایی، نقشه‌های طبقه بندی منطقه خطر و شرح فرایند
- گزارش مطالعات خطر فرایند نظیر HAZID، HAZOP، LOPA، Bow tie و مطالعه خطرات تغییر(در صورت ایجاد تغییر فرایندی)
- اسناد الزام آور بالادستی، قوانین، استانداردهای ملی، دستورالعمل مدیریت ریسک، ابلاغیه‌ها و...
- دستورالعمل‌ها، روش‌های اجرایی مورد نیاز و ماتریس ریسک مصوب شرکت
- اطلاعات در مورد رویدادهای فرایندی و خرابی‌های[۳۲] قبل
- گزارش حوادث فرایندی، حوادث و شبه حوادث آن تاسیسات و تاسیسات مشابه
- مطالعات مربوط به عوامل انسانی یا گزارش خطاهای انسانی

در صورت به روز نبودن نقشه‌های P&ID و عدم انطباق آن با شرایط فیزیکی واحد، شرکت باید قبل از شروع مطالعات، نقشه‌ها را به روز کند.

---

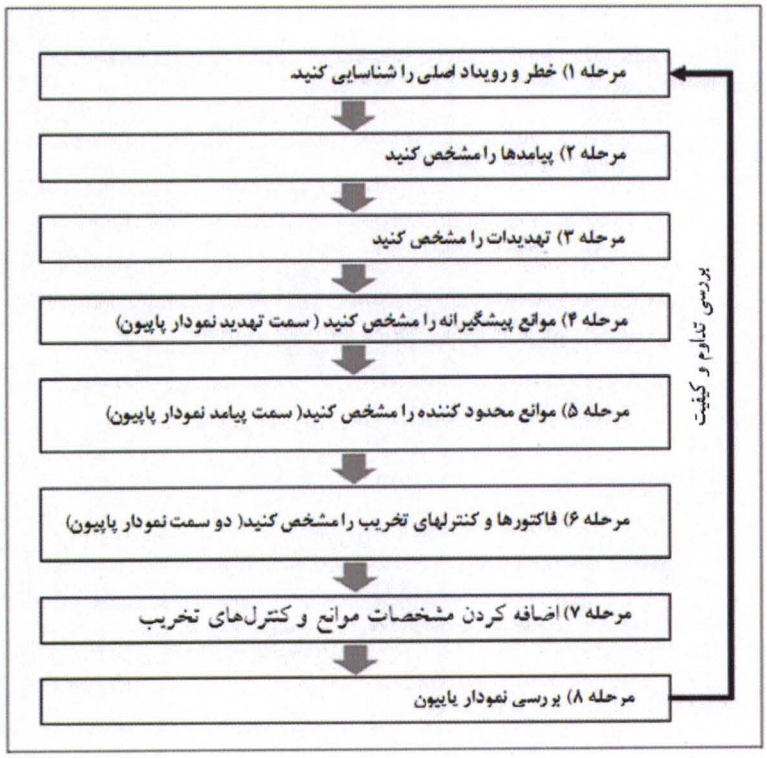
[۳۰] PFD
[۳۱] Cause effects diagram
[۳۲] Failures

۳-۵- تشکیل تیم و نحوه ترسیم نمودار پاپیون

قبل از تشکیل جلسات تیم مطالعه پاپیون، می‌بایست اعضای جلسه، رهبر و دبیر، مسئولیت‌های هر عضو، برنامه زمان‌بندی تشکیل جلسات اسناد مرجع مورد نیاز، لیست توزیع اسناد، ذی‌نفعان و دریافت‌کنندگان نهایی نمودار پاپیون مشخص و تایید شود.

در آغاز اولین جلسه، رهبر مطالعه باید خلاصه‌ای از روش تهیه نمودار پاپیون و اصطلاحات و قواعد کلیدی آن را توضیح دهد.

این ارائه با هدف یادآوری مفاهیم به اعضای آموزش‌دیده تیم انجام می‌شود. سپس رهبر مطالعه، باید جلسات مطالعه را مطابق مراحل مندرج در «فلوچارت ترسیم نمودار پاپیون» (شکل۱) هدایت کند:



شکل ۱: فلوچارت ترسیم نمودار پاپیون

۱-۳-۵- شناسایی خطر و رویداد اصلی

خطرات فرایندی که باید با روش پاپیون تحلیل شوند، از طریق مطالعات شناسایی خطر مانند HAZID، HAZOP یا سایر روش‌های شناسایی خطرات فرایندی تعیین می‌شوند. همان‌طور که در بخش ۵-۱ اشاره شد، خطرات فرایندی مهم (دارای ریسک در محدوده زرد و قرمز) باید به‌ترتیب اولویت در برنامه انجام مطالعه پاپیون قرار گیرند.

نخستین رویدادی که بلافاصله پس از رهاشدن خطر رخ می‌دهد (مانند انتشار هیدروکربن‌ها، مواد سمی یا انرژی)، به‌عنوان «رویداد اصلی» مرتبط با آن خطر، در نظر گرفته می‌شود. این رویدادها معمولاً به صورت نوعی ازدست‌دادن مهار یا کنترل خطر ظاهر می‌شوند.

محدوده رویداد اصلی (شامل حالت‌های عملیاتی، تأسیسات یا واحدهای فرایندی مرتبط) باید به‌طور دقیق تعریف و مستند شود.

۲-۳-۵- تعیین پیامدها از طریق طوفان فکری

پیامد، اثر فیزیکی ناشی از انتشار خطر بر افراد، دارایی‌ها، محیط‌زیست یا اعتبار سازمان است. به عبارت دیگر، خودِ نشت مواد از تجهیزات عملیاتی به‌عنوان پیامد محسوب نمی‌شود، بلکه آسیب فیزیکی حاصل از آن نظیر صدمات جانی، خسارات مالی یا آلودگی محیط‌زیست به‌عنوان پیامد اولیه و مواردی نظیر توقف تولید، کاهش فروش، کاهش کیفیت محصول، نقض الزامات قانونی، از دست دادن اعتبار (در نظر عموم، مشتری‌ها، سهامداران شرکت و قانون‌گذار) به عنوان پیامد ثانویه در نظر گرفته می‌شود.

محدوده مطالعه باید حتما شامل پیامدهای اولیه باشد؛ لیکن بسته به ریسک سناریوی مورد مطالعه توصیه می‌شود محدوده مطالعه تا بررسی پیامدهای ثانویه گسترش یابد.

یک رویداد اصلی ممکن است چندین پیامد معتبر[۳۳] داشته باشد. بنابراین، برای شناسایی دقیق موانعِ محدودکننده، لازم است تمام پیامدهای محتمل در نمودار پاپیون لحاظ شوند.

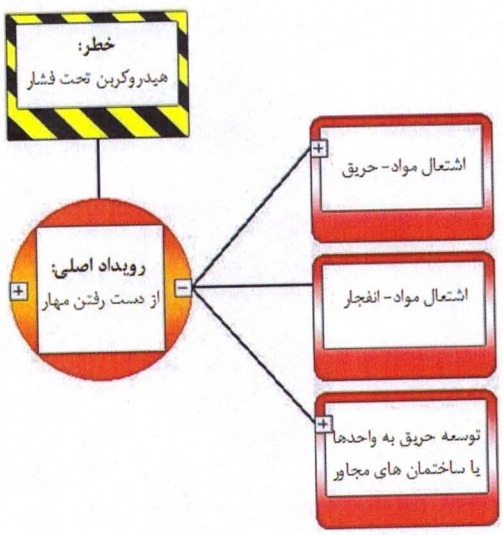
---

[۳۳] Credible Consequence

شناسایی پیامدها پیش از تهدیدها به تیم کمک می‌کند تا درک بهتری از ابعاد رویداد اصلی پیدا کند و از پرداختن به تهدیدهایی که تنها منجر به رویدادها یا پیامدهای کم‌اهمیت می‌شوند، جلوگیری شود.

در نمودار پاپیون، برای هر پیامد باید خط جداگانه‌ای بین رویداد اصلی و پیامد ترسیم شود. در صورتی که موانع محدودکننده برای چند پیامد یکسان باشند، می‌توان آن‌ها را ادغام کرد. برای مثال، اگر موانع مربوط به «آتش فورانی»[۳۴] و «آتش لحظه‌ای»[۳۵] مشترک باشند، می‌توان هر دو را در یک خط پیامد با عنوان کلی «آتش‌سوزی» نمایش داد.

ممکن است برخی پیامدها (مانند آتش‌سوزی یا انفجار) محدود به یک منطقه نباشند و با تأثیر برمحیط اطراف، باعث آسیب‌های ثانویه شوند. در صورت معتبر بودن این نوع سناریوها، باید آن‌ها را نیز تحلیل کرد و به نمودار پاپیون افزود؛ به شکل ۲ مراجعه کنید.



شکل ۲: ترسیم پیامد در نمودار پاپیون

[۳۴] Jet Fire
[۳۵] Flash Fire

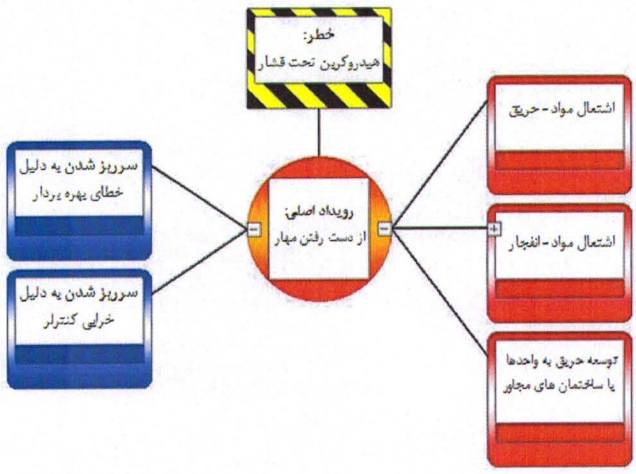
۳-۳-۵- شناسایی تهدیدها

برای هر خطر باید کلیه تهدیدها شناسایی شوند. هر تهدید باید با یک خط جداگانه به رویداد اصلی متصل شود و حداقل یکی از پیامدهای تعریف شده با آن مرتبط باشد.

اگر آنالیز پاپیون نشان دهد که تهدیدهای متعدد، موانع یکسان دارند، می‌توان این تهدیدها را با هم ادغام کرد.

باید توجه داشت که پاپیون کلیه تهدیدها را به طور هم‌سطح نمایش می‌دهد و بین احتمال وقوع تهدیدهای مختلف (مستقل یا همزمان)، تفاوتی قائل نمی‌شود.

تهدیدها باید واضح و مستقل باشند [یعنی به صورت مجزا درک شوند]. به عنوان مثال، خوردگی، به عنوان یک تهدید داخلی و خارجی برای لوله‌های فرایندی مطرح است، اما رنگ آمیزی بخش خارجی لوله تنها می‌تواند کنترلی برای مدیریت خوردگی خارجی باشد. بنابراین تهدید باید به خوردگی خارجی و داخلی تفکیک شود تا کنترل مربوطه بتواند مستقیماً تهدید را مورد هدف قرار دهد.



شکل ۳: ترسیم تهدید در نمودار پاپیون

٤-٣-٥- شناسایی موانع پیشگیرانه

موانع واقع در سمت چپ پاپیون از انتشار یک خطر به وسیله تهدید جلوگیری می‌کنند که به آنها موانع پیشگیرانه (یا اقدامات کنترلی) گفته می‌شود. تمام موانع پیشگیرانه موجود برای هر تهدید باید به طور سیستماتیک مستند شوند. نمونه‌هایی از موانع پیشگیرانه شامل موارد ذیل می‌شود:

- سیستم‌های اصلی کنترل فرایند[٣٦]
- آلارم‌های هشداردهنده مهم و اقدام بهره‌بردار در کنترل شرایط فرایندی (در صورت رعایت معیارهای کفایت مانع)
- سیستم‌های ابزاردقیقی ایمنی[٣٧]

٥-٣-٥- شناسایی موانع محدودکننده

به موانع واقع در سمت راست پاپیون که پیامدها را محدود می‌کنند یا آنها را کاهش می‌دهند، موانع محدود کننده (یا اقدامات بازیابی) گفته می‌شود. تمام موانع محدود کننده موجود، باید به طور سیستماتیک مستند و ثبت شوند. نمونه‌هایی از موانع محدود کننده شامل موارد ذیل می‌شود:

- تجهیزات جلوگیری از گسترش پیامد (مانند موج انفجار یا نشر مواد) در سطح واحدها نظیر دیوارهای محافظ[٣٨] و دیوارهای حائل[٣٩].
- تجهیزات اطفاء حریق، نظیر تشخیص گاز و پاشش اتوماتیک فوم یا سیستم اتوماتیک پاشش آب بر روی دستگاه‌های عملیاتی[٤٠]

نکته: تنها موانع معتبر باید در دو سمت نمودار پاپیون درج شوند. الزامات مربوط به اعتبار موانع در بخش ٥-٤ تبیین شده است.

تجهیزات دستی آتش نشانی، سیستم‌های دستی پاشش آب بر روی دستگاه‌های عملیاتی (دیلاج)، روش‌های تخلیه و فرار کارکنان از تأسیسات و موارد مشابه را نمی‌توان به عنوان مانع یا لایه حفاظتی مستقل در نظر گرفت، زیرا متغیرهای متعددی (مانند تأخیر زمانی) بر اثربخشی آنها در

---

[٣٦] Basic Process Control System (BPCS)
[٣٧] Safety Instumented System(SIS)
[٣٨] Blast wall
[٣٩] Dikes
[٤٠] Deluge Systems

محدود کردن پیامدهای یک سناریو تأثیر گذار است. نمونه‌هایی از مواردی که نباید به عنوان مانع یا لایه حفاظتی مستقل در نظر گرفته شود، در پیوست «د» ارائه شده است.

٦-٣-٥- شناسایی فاکتورهای تخریب و کنترل‌های آن

برای تمام موانع (پیشگیرانه یا محدود کننده) باید تمام عوامل یا فاکتورهایی که می‌توانند باعث خرابی مانع یا کاهش کارایی آن شوند را شناسایی کرد و در نمودار پاپیون آنها را در جایگاه فاکتور تخریب به مانع مربوطه متصل نمود.

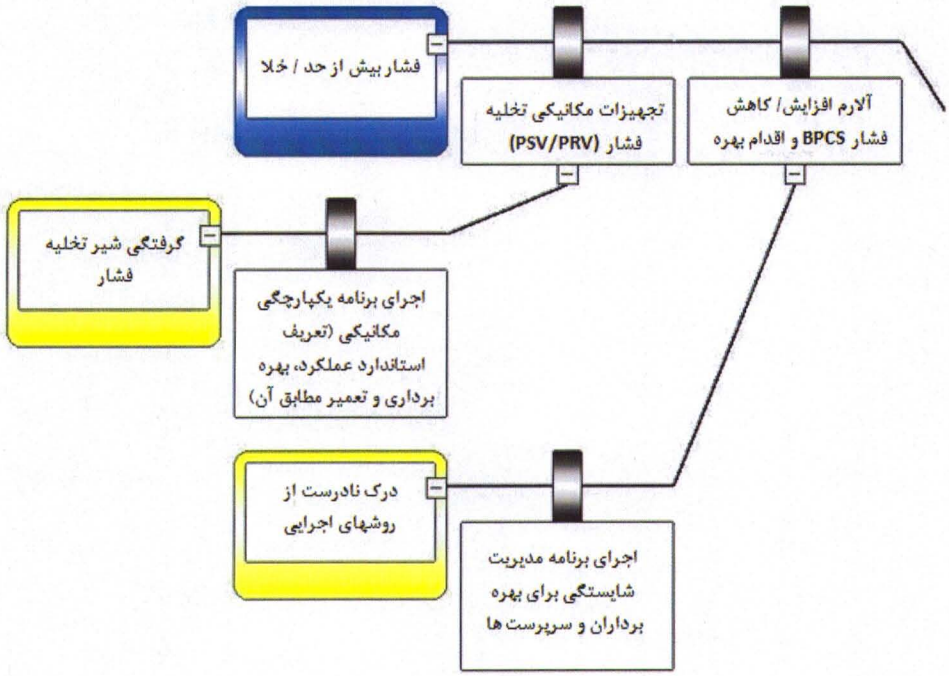
سپس برای هر فاکتور تخریب، باید کنترل‌های تخریب، شناسایی شوند تا از وقوع فاکتورهای تخریب جلوگیری شود، یا از شرایط مانع و صحت عملکرد موانع آنها اطمینان حاصل شود. این کنترل‌ها به طور مستقیم نه از وقوع رویداد اصلی جلوگیری می‌کنند و نه پیامد را کاهش می‌دهند. کنترل تخریب اغلب معیارهای اعتبار مانع (مندرج در بخش ٥-٤) را برآورده نمی‌کند؛ اگرچه در صورت برآورده شدن، بسیار قوی‌تر خواهند بود. کنترل‌های تخریب غالباً عوامل انسانی و سازمانی‌اند که برای مدیریت ریسک به کار می‌روند.

نمونه‌هایی از کنترل‌های تخریب عبارتند از: استانداردهای مهندسی، مدیریت پیمانکار، مدیریت تغییر، آموزش و.... اما درج فاکتورهای تخریبی که به طور مکرر رخ می‌دهند می‌توانند کارایی پاپیون به عنوان یک ابزار ارتباط بصری را کاهش دهد؛ لذا در تهیه نمودار پاپیون باید فاکتورهای تخریب خاص لحاظ شوند. به شکل٤ و ٥ مراجعه کنید.

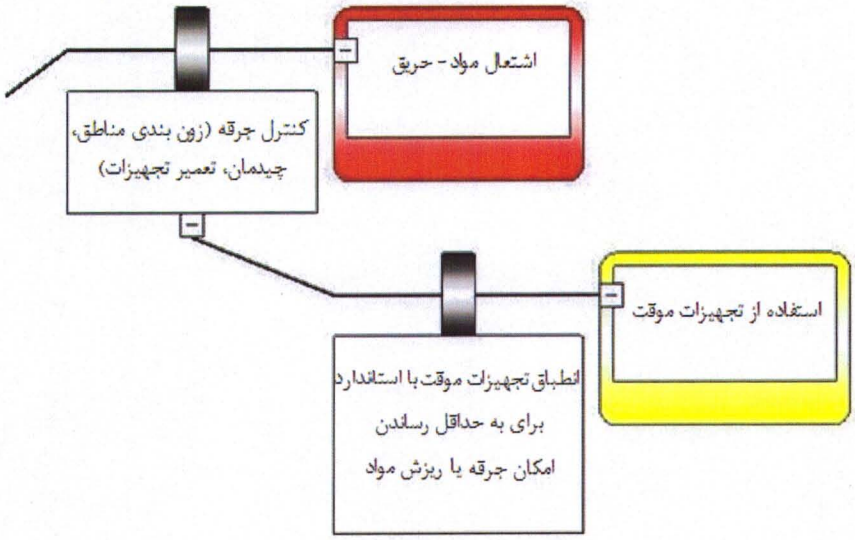
فاکتورهای تخریب رایج که معیارهای عملکردِ موانع سخت‌افزاری را بیان می‌کنند (نظیر استانداردهای طراحی یا عملیات)، باید از پاپیون حذف شوند.

فرض بر این است که فرآیندها و رویه‌ها رعایت می‌شوند و آموزش‌های لازم اجرا می‌شوند، بنابراین عبارت‌های کلی مانند «خطای انسانی» و «ضعف در اجرای یک دستورالعمل» نباید به عنوان فاکتور تخریب در نظر گرفته شوند.

به جای استفاده از فاکتورهای تخریب کلی، باید اقدامات مشخصی برای رفع شکاف‌های شناسایی‌شده تعیین گردد.



شکل ٤: بیان نادرست فاکتورهای تخریب



شکل۵: بیان فاکتورهای تخریب برای نشان دادن شکاف‌های خاص

۷-۳-۵- ثبت مشخصات موانع و کنترل‌های تخریب

در این مرحله با استفاده از دانش تیم، مشخصات موانع و کنترل‌های تخریب شامل نوع مانع و توضیحات مربوطه، صاحب مانع، اثربخشی، استاندارد عملکرد، درجه اهمیت مانع، وضعیت، معیار پذیرش و... را درج کنید.[۴۱]

پس از تکمیل، رهبر باید نمودار پاپیون را از نظر کامل بودن، رعایت الزامات اعتبار موانع (بند۵-٤)، کفایت موانع (بند۵-۵) و انطباق با شرایط مرجع بررسی و تایید نموده و گزارش نهایی آن را ارائه دهد.

در گزارش نهایی علاوه بر ترسیم نمودار پاپیون موارد ذیل باید برای هر رویداد اصلی ارائه شود:

- موانع موجود مرتبط با هر تهدید به ترتیب سطح اهمیت موانع
- موانع مورد نیاز جهت انطباق با الزامات/ مدیریت ریسک
- استاندارد و شاخص‌های ارزیابی عملکرد موانع

٤-۵- اعتبار موانع

تمام تهدیدها و پیامدها باید موانع معتبر، شناسایی شوند. موانع پیشگیرانه موجود در سمت چپ پاپیون باید به تنهایی توانایی جلوگیری از تهدید را داشته باشند تا تهدید منجر به رویداد اصلی نشوند یعنی در صورتی معتبر تلقی می‌شوند که (به خودی خود) از یک تهدید موجود جلوگیری کنند. اگر مانع محدود کننده است و در سمت راست پاپیون قرار دارد، باید بتواند موجب کاهش یا حذف پیامد شود. تمام موانع برای اینکه معتبر باشند باید الزامات اعتبار مانع شامل مؤثر، مستقل و قابل ممیزی بودن را برآورده کنند. در صورت رعایت الزامات اعتبار مانع، به آن مانع، لایه حفاظتی مستقل[۴۲] (IPL) هم گفته می‌شود.

---

[۴۱] برای کسب اطلاعات بیشتر به بخش ۵-۳-۳ کتاب نمودارهای پاپیون در مدیریت ریسک (CCPS:Bow ties in risk management) مراجعه کنید.

[۴۲] Indipendent Protection Layer

۱-٤-۵ موثر بودن مانع:

برای اینکه مانع موثر باشد و در پاپیون لحاظ شود، باید به اندازه کافی بزرگ، به اندازه کافی قوی و به اندازه کافی سریع واکنش نشان دهد تا بتواند تهدیدی که منجر به رویداد اصلی می‌شود را متوقف کند یا با عمل (مطابق طراحی)، موجب کاهش یا حذف پیامد شود. به عبارت دیگر مانع باید ویژگی‌های ذیل را داشته باشد تا بتوان آن را موثر تلقی کرد:

• باید همیشه بتواند تمام وضعیت‌های نیازمند اقدام را تشخیص دهد و اگر نتواند شرایط را شناسایی کند و اقدام هدف خود را انجام دهد، یک مانع یا IPL نیست.

• باید بتواند شرایط را به موقع تشخیص دهد و در زمان لازم اقدام اصلاحی انجام دهد و از پیامد نامطلوب جلوگیری کند. زمان مورد نیاز باید حداقل شامل موارد ذیل شود:

- زمان لازم برای تشخیص وضعیت،
- زمان لازم برای پردازش اطلاعات و تصمیم گیری،
- زمان لازم برای انجام اقدامات و
- زمان اثرگذاری اقدام

• باید ظرفیت کافی برای انجام اقدامات لازم در زمان موجود را داشته باشد. اگر سایز خاصی از تجهیزات (مانند سایز دهانه شیر تخلیه، حجم دایک و غیره) نیاز است، آیا مانع موجود الزامات مربوط به سایز را برآورده می‌کند؟ به عبارت دیگر آیا قدرت مانع (IPL) برای اقدام مورد نیاز کافی است؟ قدرت یک مانع (IPL) ممکن است شامل قدرت فیزیکی مانع (مثل دیوار انفجاری یا دایک) باشد یا به توان نیروی انسانی مرتبط باشد (به عنوان مثال، آیا وظیفه مورد نیاز در حد توانایی‌های فیزیکی همه بهره‌بردارها است؟).

بیان اثربخشی یک مانع، نوعی رتبه بندی کیفی است. اثربخشی هر مانع را باید برای کنترل‌های سخت‌افزاری و همچنین کنترل‌هایی که به مداخله انسان نیاز دارند، ارزیابی کرد. این ارزیابی موارد زیر را در نظر می‌گیرد:

- کامل بودن و توانایی مانع در انجام کار خود
- استقلال از عامل انسانی
- قابلیت اعتماد

موانع سمت راست پاپیون تنها زمانی می‌توانند موثر در نظر گرفته شوند که عملکرد آن توسط سناریوی مورد بررسی آسیب نبیند.

نکته: مانع باید در برابر پیامدهای انتشار خطرات دیگر محافظت شود و اگر تحت تاثیر تهدید دیگری قرار گرفت بتواند مطابق آنچه در نظر گرفته شده عمل کند. به عنوان مثال، شیر جداسازی موجود در مرز واحد به واسطه محل قرارگیری آن باید توسط یک محفظه حفاظتی در برابر آتش سوزی و انفجار محافظت شود.

۲-٤-۵ مستقل بودن مانع:

موانع باید از تهدیدها و موانع دیگر مستقل باشد. برای اینکه مانع مستقل باشد باید:

- مستقل از تهدید؛
- مستقل از سایر موانع موجود در آن مسیر؛ (مثلاً اگر سیستم دیلاج و تشخیص گاز، یک کنترلگر منطقی مشترک داشته باشند، مستقل نخواهند بود).
- نداشتن حالت خرابی مشترک با سایر موانع (در صورت وجود علت خرابی مشترک[۴۳] بین دو یا چند مانع، نمی‌توان آن موانع را مستقل در نظر گرفت.)
- عملکرد مؤثر یک مانع نباید به عملکرد موفقیت آمیز مانع دیگری وابسته باشد.

نکته: خرابی مانع نباید باعث از دست رفتن مهار یا کنترل خطر و شروع تهدید شود. همچنین اگر تعدادی از موانع سخت افزاری و اقدام انسان، اجزاء یک برنامه واحد هستند (مثل یک سیستم مدیریت خوردگی که شامل تزریق مواد شیمیایی، بازرسی و موارد دیگر است) باید به عنوان یک مانع منفرد یا یک برنامه نشان داده شوند، زیرا واقعاً مستقل نیستند.

۳-٤-۵ قابل ممیزی بودن مانع:

موانع باید قابلیت ممیزی داشته باشند تا از کارکردن درست آنها هنگام تقاضا اطمینان حاصل شود. قابل ممیزی بودن موانع ایمنی، وجود دنباله‌ای از اقدامات ایمنی را تضمین می‌کند که نشان دهنده توانایی شرکت در انجام موارد زیر است:

- ایجاد و حفظ روش‌های اجرایی بازرسی
- ثبت و نگهداری نتایج ارزیابی‌های اعتبار سنجی قبلی و سایر اطلاعات مرتبط
- حصول اطمینان از انجام تست، نگهداری و بهره‌برداری مطابق با انتظارات در جهت برآوردن هدف طراحی ایمنی تاسیسات

---

[۴۳] Common cause failure

تمام مانع باید از طریق یک سیستم رسمی (مانند تست و بازرسی یا ممیزی معیارهای عملکرد سخت افزاری و وظایف حیاتی ایمنی مورد نیاز برای حفظ مؤثر بودن مانع) مورد ارزیابی قرارگیرند تا توان عملکرد صحیح آنها هنگام نیاز، تأیید شود.

نکته: شایستگی و توانمندی کارکنانی که در ایجاد، بهره‌برداری و یا حفظ یک مانع (یا بخشی از آن) نقش دارند باید طی یک سند رسمی تعریف و اجرایی شود. بنابراین، قابلیت ممیزی موانع معتبر، به بررسی آموزش و تضمین شایستگی پرسنلی که وظایف و یا فعالیت‌های حیاتی ایمنی را انجام می‌دهند، نیز توسعه می‌یابد.

در بسیاری از موارد، موانع فقط تا حدی معتبر[44] هستند یا به عبارت دیگر فقط بخشی از یک مانع هستند. چراکه برای کنترل کامل تهدید یا پیامد، به کمک یا حمایت یک مانع دیگر نیاز دارند. این نوع موانع را باید با مانع دیگری (که آن هم تا حدی معتبراست) ترکیب کرد تا مجموعا بتوانند به عنوان یک مانع معتبر لحاظ شوند.

باید در نظر داشت که مداخله بهره‌بردار تنها زمانی یک مانع انسانی معتبر است که زمان کافی برای پاسخگویی و جلوگیری از رویداد وجود داشته باشد. تعیین مقدار زمان لازم در این ارتباط می‌بایست در الزامات هر شرکت تعیین شود.

به طور کلی، اگر یک بهره‌بردار موجب فعال شدن تهدید شود، برای مداخله این بهره‌بردار نمی‌توان هیچ اعتباری در نظر گرفت. اگر یک بهره‌بردار به عنوان بخشی از دو مانع در نظر گرفته شود، موارد زیر باید لحاظ شود تا بتوان آن موانع را مستقل در نظر گرفت:

- پاسخ بهره‌بردار باید در دوره‌های زمانی مختلف انجام شود، و
- بهره‌بردار باید زمان کافی برای پاسخ مطلوب داشته باشد.

تبصره: سخت افزارها و موانع انسانی که در پاپیون درج می‌شوند باید آنهایی باشند که بتوانیم از اعتبار آنها اطمینان یابیم یا اعتبار آنها را تایید کنیم. حصول اطمینان از قابل ممیزی بودن یک مانع، برای مدیریت موفقیت آمیز خطرات مهم[45] حیاتی است. موانع سخت افزاری باید توسط افراد دارای وظایف حیاتی، بررسی و نگهداری شوند. مانع انسانی هم به مداخلات انسانی (از طریق فعالیت / وظایف حیاتی) نیاز دارد.

---

[44] Partially Valid (PV)
[45] Major Hazards

نمونه‌هایی از دسته بندی موانع سخت افزاری و موانع انسانی در پیوست ج داده شده است.

۵-۵- کفایت موانع

برای تعیین کفایت مانع (لایه حفاظتی مستقل) و حصول اطمینان از تبدیل نشدن تهدیدها به رویداد اصلی و کاهش یا حذف پیامدها می‌بایست فرکانس وقوع رویداد اصلی/ پیامد با روش آنالیز لایه‌های حفاظتی[۴۶] محاسبه و نتیجه با فرکانس معیار مندرج در پیوست ب (که به عنوان الگوی حداقل الزامات برای واحدهای عملیاتی که کمتر از ۶۰ سال قدمت دارند، ارائه شده است) مقایسه شود. فرکانس وقوع رویداد اصلی/ پیامد می‌بایست کوچکتر/مساوی معیار ارائه شده باشد. اگر فرکانس محاسبه‌شده بیشتر از معیار باشد، باید لایه حفاظتی جدید طراحی و اجرا گردد.

در مواردی که به دلیل قدمت بالای تأسیسات یا محدودیت‌های سیستم‌های ابزار دقیق، امکان رعایت معیار مندرج در پیوست ب وجود ندارد، شرکت‌ها موظفند معیار تصمیم‌گیری مختص خود را تدوین و تصویب کنند. به‌عنوان یک راهنمای کلی، به این شرکت‌ها پیشنهاد می‌شود حداقل ۳ مانع مستقل در سمت چپ (مسیر منتهی به تهدید) و ۲ مانع مستقل در سمت راست (مسیر منتهی به پیامد) نمودار پاپیون را به عنوان معیار کفایت در نظر بگیرند. مجددا تأکید می‌شود در تعیین تعداد موانع مورد نیاز، تنها باید موانع معتبر لحاظ گردند.

۶-۵- تدوین و اجرای برنامه مدیریت موانع

پس از آغاز بهره‌برداری، به‌دلیل تأثیر فاکتورهای تخریب، کارایی موانع از حالت طراحی خارج می‌شود. بنابراین اجرای یک فرآیند مستمر برای مدیریت موانع ضروری است. برنامه مدیریت موانع باید به‌عنوان بخشی از برنامه جامع ایمنی فرایند مبتنی بر ریسک، بر وضعیت موانع نظارت کرده و بازگشت آن‌ها به شرایط استاندارد را تضمین کند.

برنامه مدیریت موانع حداقل شامل موارد ذیل است:

۱-۶-۵ شناسایی موانع:

شرکت‌ها باید لیست موانعی را که باید تحت پوشش برنامه مدیریت موانع قرار گیرند را مستقیماً از نمودارهای پاپیون، استخراج نمایند.

---

[۴۶] LOPA

۲-۶-۵ شناسایی عناصر حیاتی ایمنی

با توجه به تفاوت در سطح اهمیت موانع[۴۷]، لازم است عناصر حیاتی ایمنی شناسایی شود تا امکان اجرای استراتژی حفظ، نگهداری و تعمیرات آنها به صورت کارآمدتر فراهم شود. به همین دلیل شرکت‌ها باید فهرست عناصر حیاتی ایمنی را تهیه کنند. این عناصر شامل تجهیزات، سیستم‌ها و فرآیندهای مدیریتی هستند که صحت عملکرد موانع سخت‌افزاری و انسانی را تضمین می‌کنند (نمونه در پیوست ج).

۳-۶-۵ تعیین استاندارد عملکرد و شاخص‌های ارزیابی

پس از شناسایی عناصر حیاتی باید برای هریک استاندارد عملکردی تهیه شود که در آن سطح عملکرد مورد انتظار[۴۸]، در دسترس بودن[۴۹]، قابلیت اطمینان[۵۰]، بقا[۵۱] و وابستگی متقابل[۵۲] مشخص شود. ضمنا اطلاعات لازم برای تأیید اثربخشی عنصر حیاتی ایمنی در طول طراحی، ساخت و بهره‌برداری از سیستم را داشته باشد به نحوی که بتوان تضمین کرد با گذشت زمان موانع حیاتی در جای خود باقی می‌مانند و به طور مؤثر خطر را مدیریت می‌کنند.

اگر عناصرحیاتی ایمنی، شامل مجموعه‌ای از اجزاء باشد بهتر است آن را به اجزاء تشکیل دهنده تقسیم نمود تا بتوان شاخص‌های مناسب برای تایید عملکرد آن را تعریف و با سهولت بیشتر آن را مدیریت نمود. به عنوان مثال، سیستم حفاظت در برابر حریق را می‌توان به عنوان یک عنصر حیاتی ایمنی در نظر گرفت یا آن را به تجهیزات و اجزایی مانند پمپ ها، شیرها، شبکه آب، سیستم‌های لوله کشی و انشعاب‌های مرتبط، و نازل‌ها تقسیم کرد. شاخص عملکرد برای آب آتش نشانی، مقدار آب مورد نیاز آتش نشانی در بدترین سناریو برای یک مدت زمان مشخص است در حالی که شاخص عملکرد پمپ آتش نشانی، اندازه گیری مقدار فشار و جریان در سمت تخلیه پمپ است. بدین ترتیب با تقسیم عناصرحیاتی ایمنی به اجزاء آن، مدیریت آنها ساده‌تر می‌شود.

طراحان و متخصصان ریسک باید عملکرد و سطح عملکرد مورد نیاز عناصرحیاتی ایمنی را در مرحله طراحی ارائه کنند. شرکت‌های بهره‌بردار نیز باید برای حفظ یکپارچگی این تجهیزات

---

[۴۷] مبنای تعیین سطح اهمیت موانع باید توسط هر شرکت تعیین شود؛ برای کسب اطلاعات بیشتر در این زمینه به بخش ۱/۵/۵کتاب نمودارهای پاپیون در مدیریت ریسک مراجعه نمایید.

[۴۸] Functionality
[۴۹] Avaliability
[۵۰] Reliability
[۵۱] Survivability
[۵۲] Interdependency

فعالیت‌های لازم (مانند تعمیر و نگهداری، بازرسی و تست) را انجام دهند تا پیوند شفافی بین خطرات/ ریسک‌های مهم، عناصرحیاتی ایمنی و استانداردهای عملکرد وجود داشته باشد.

شاخص‌های عملکرد تجهیزات حیاتی ایمنی معمولاً برای تمام مراحل چرخه عمر تأسیسات تغییر نمی‌کنند، اما چگونگی تأیید تجهیزات حیاتی ایمنی ثابت نیستند و با تغییر مرحله چرخه عمر تأسیسات تغییر می‌کنند، مانند:

- طراحی: محاسبات مهندسی و تحلیل.
- اجرای پروژه (تامین تجهیزات[۵۳]، تولید اجزا[۵۴]، ساخت[۵۵] و تحویل برای راه اندازی[۵۶]): تست نوع تجهیزات و تست عملکرد؛
- بهره‌برداری: بازرسی، تعمیرات/نگهداری و تست.

بنابراین، ممکن است استانداردهای عملکرد اولیه با مواردی که به صورت مداوم برای ارزیابی تناسب تجهیزات حیاتی ایمنی استفاده می‌شود متفاوت باشد و از این رو برای تناسب اولیه و تداوم بهره‌برداری متناسب با شرایط برای هر مانع/ تجهیز حیاتی ایمنی باید استانداردهای عملکرد جداگانه ایجاد شوند.

استانداردهای عملکرد باید از برآورده شدن شاخص‌های تعریف شده برای تجهیزات حیاتی ایمنی در سراسر چرخه عمر تاسیسات اطمینان یابند.

٤-٦-٥ تهیه و اجرای برنامه پایش

شرکت باید برای حصول اطمینان از صحت عملکرد عناصر حیاتی ایمنی، برنامه مکتوبی برای پایش مستمر وضعیت آنها در نظر بگیرد و از اعمال اولویت بالاتر برای انجام بازرسی، تست، تعمیر/ نگهداری، تأمین قطعات یدک و دیگر اقدامات مورد نیاز برای عناصر حیاتی ایمنی اطمینان حاصل نماید. این برنامه مکتوب می‌تواند شامل موارد ذیل باشد:

- تعیین ابزارهای تست عملکرد
- تعیین بازه زمانی پایش و مسئولیت‌های مرتبط
- تعیین میزان تخریب مانع و اقدامات مورد نیاز برای بازگشت آن به وضعیت اولیه
- اولویت بندی و اجرای اقدامات مورد نیاز و حصول اطمینان از اجرای آنها

این برنامه باید به‌طور مستمر به‌روزرسانی و اثربخشی آن تضمین شود.

---

[۵۳] Procurement
[۵۴] Fabrication
[۵۵] Construction
[۵۶] Commitionning

٦- تاریخ تصویب و اجرا

این دستورالعمل توسط مدیریت بهداشت، ایمنی و محیط زیست تهیه و توسط مدیریت مهندسی ساختار در شش بند تنظیم و تدوین یافته و در تاریخ ۱۴۰۵/۲/۱۶ به تصویب معاون وزیر و مدیرعامل شرکت ملی پالایش و پخش فرآورده‌های نفتی ایران رسید.

بهنام لازمی	**سرلک**	**صادق عظیمی‌فر**
مدیر بهداشت، ایمنی، محیط زیست بحران و پدافند غیرعامل	مدیر مهندسی ساختار	معاون وزیر و مدیر عامل

۷- منابع ومراجع

۱. راهنمای استقرار سیستم مدیریت ایمنی فرایند در صنعت نفت به شماره MOP-HSE-GL-۲۳۰ (۱)

۲. نمودارهای پاپیون در مدیریت ریسک، کتاب مفهومی ایمنی فرایند، انتشارات دانش بنیاد، ۱٤۰۰

۳. Center for Chemical Process Safety (CCPS) - Guidelines for Risk Based Process Safety-Wiley-AIChE (۲۰۰۷)

٤. Center for Chemical Process Safety (CCPS) - Bow Ties in Risk Management: A Concept Book for Process Safety-Wiley-Energy Institute (۲۰۱۸)

٥. Center for Chemical Process Safety, ۲۰۰۷: Risk Based Process Safety Overview (۲۰۱٤)

٦. Guidelines for Risk based Process Safety, CCPS Publication.

۷. Center for Chemical Process Safety, ۲۰۰٥. Business Case for Process Safety.

پیوست الف: ماتریس تحمل ریسک شرکت

ماتریس تحمل ریسک شرکت

رده بندی شدت پیامد						
	S۵ فاجعه بار	S_5L_1	S_5L_2	S_5L_3	S_5L_4	S_5L_5
	S۴ مهم	S_4L_1	S_4L_2	S_4L_3	S_4L_4	S_4L_5
	S۳ بزرگ	S_3L_1	S_3L_2	S_3L_3	S_3L_4	S_3L_5
	S۲ جزئی	S_2L_1	S_2L_2	S_2L_3	S_2L_4	S_2L_5
	S۱ ناچیز	S_1L_1	S_1L_2	S_1L_3	S_1L_4	S_1L_5
		L۱ بعید	L۲ بسیارکم	L۳ محتمل	L۴ زیاد	L۵ بسیار زیاد

رده بندی فرکانس وقوع رویداد اصلی

رده بندی حدود تحمل ریسک	
ریسک قابل قبول	S_1L_1 , S_1L_2 , S_1L_3 , S_1L_4 , S_2L_1 , S_2L_2 , S_3L_1
ریسک قابل پذیرش (ALARP)	S_1L_5 , S_2L_3 , S_2L_4 , S_2L_5 ,S_3L_2 , S_3L_3 , S_3L_4 , S_4L_1 , S_4L_2 , S_5L_1 , S_5L_2
ریسک غیرقابل قبول	S_3L_5 , S_4L_3 , S_4L_4 , S_4L_5 , S_5L_3 ,S_5L_4 , S_5L_5

رده بندی فرکانس وقوع رویداد اصلی					
	بعید L_1	بسیارکم L_2	محتمل L_3	زیاد L_4	بسیار زیاد L_0
احتمال وقوع	کوچکتر از 10^{-4}	بین 10^{-3} – 10^{-4}	10^{-2} – 10^{-3}	10^{-1} – 10^{-2}	10^{-1} – ۱
فرکانس وقوع	بیش از ۱ بار در ۱۰ سال ۱۰۰۰۰۰	بیش از ۱ بار در ۱۰۰۰۰ سال	بیش از ۱ بار در ۱۰۰۰ سال	بیش از ۱ بار در ۱۰۰ سال	بیش از ۱ بار در ۱۰ سال

رده بندی شدت پیامد					
نوع پیامد	ناچیز S_1	جزئی S_2	بزرگ S_3	مهم S_4	فاجعه بار S_0
آسیب به انسان در اثر حادثه	آسیب قابل ثبت (کمک های اولیه)	آسیب‌ناتوان کننده قابل برگشت یک نفر	نقص عضو یک نفر یا آسیب‌ناتوان کننده قابل برگشت چند نفر	فوت یک نفر یا نقص عضو چند نفر	فوت بیش از یک نفر
اثر بر سلامت	استشمام بو یا مواجهه کارکنان با مواد، کمتر از حد مجاز	مواجهه کارکنان با مواد، بیشتر از حد مجاز	ایجاد عوارض کوتاه مدت، بی حالی، سرگیجه	بستری شدن یک یا چند نفر در بیمارستان با عوارض برگشت پذیر	فوت یا عوارض دائمی برای کارکنان یا بستری افرادی از همسایگان مجاور
خسارت مالی به تجهیزات	کمتر از ۱۰ هزار دلار	بین ۱۰ تا ۱۰۰ هزار دلار	بین ۱۰۰ هزار تا ۱ میلیون دلار	بین ۱ تا ۱۰ میلیون دلار	بزرگتر و مساوی ۱۰ میلیون دلار
توقف تولید	وقفه روزانه در واحدهایی که در تولید بنزین نقش ندارند. نظیر حذف گوگرد از نفت سفید/ نفت گاز	وقفه روزانه در واحدهایی که در تولید بنزین نقش دارند. نظیر هیدروژن، GTG، گاز مایع، ایزومر یا آیزوماکس شود.	وقفه یک روز واحدهای یوتیلیتی یا کاهش ۵۰٪ محصولات به دلیل وقفه در واحدهای تولیدی نظیر تقطیر اتمسفریک و تقطیر در خلاء	شات دان کامل از ۲۴ ساعت تا کمتر از سه روز برای تمام واحدهای عملیاتی	شات دان کامل به مدت ۳ روز یا بیشتر برای تمام واحدهای عملیاتی
اثرات زیست محیطی	آلودگی ناچیز در اثر انتشار مواد در محل وقوع	آلودگی کم در اثر انتشار مواد در محدوده واحد مرتبط که سریع از بین می‌رود	آلودگی متوسط در محدوده شرکت با اثرات موضعی و کوتاه مدت که نیاز به پاک سازی دارد	آلودگی مهم در محدوده شرکت با اثرات بلند مدت نیاز به پاک سازی و پرداخت جریمه دارد	شیوع گسترده آلودگی خارج از محدوده شرکت با اثرات بلند مدت و آسیب به اکولوژی منطقه همراه است.
اثرات اجتماعی بر اعتبار شرکت	انعکاس خبری در سطح شرکت	انعکاس خبری در سطح شهر	انعکاس خبری در سطح استان	انعکاس خبری در سطح کشور	انعکاس خبری در سطح بین المللی

پیوست ب: معیار تصمیم گیری حدود قابل تحمل فرکانس وقوع رویداد اصلی

معیار تصمیم گیری حدود قابل تحمل فرکانس وقوع رویداد اصلی

طبقه بندی / شدت پیامد	خسارت به دارایی Asset	ایمنی کارکنان personnel Safety	ایمنی جامعه public Safety	محیط زیست Environment
ناچیز (S۱)	$۱۰^{-۱}$	$۱۰^{-۲}$	$۱۰^{-۳}$	$۱۰^{-۲}$
جزئی (S۲)	$۱۰^{-۲}$	$۱۰^{-۳}$	$۱۰^{-۴}$	$۱۰^{-۳}$
بزرگ (S۳)	$۱۰^{-۳}$	$۱۰^{-۴}$	$۱۰^{-۵}$	$۱۰^{-۴}$
مهم (S٤)	$۱۰^{-۴}$	$۱۰^{-۵}$	$۱۰^{-۶}$	$۱۰^{-۵}$
فاجعه بار (S۰)	$۱۰^{-۵}$	$۱۰^{-۶}$	$۱۰^{-۷}$	$۱۰^{-۶}$

پیوست ج: نمونه موانع سخت افزاری، انسانی و فرایندهای حیاتی

TABLE 6.3
Examples of Passive IPLs

IPL	Comments *Assuming an adequate design basis and adequate inspection and maintenance procedures*	PFD from Literature and Industry	PFD Used in This Book (For screening)
Dike	Will reduce the frequency of large consequences (widespread spill) of a tank overfill/rupture/spill/ etc.	$1 \times 10^{-2} - 1 \times 10^{-3}$	1×10^{-2}
Underground Drainage System	Will reduce the frequency of large consequences (widespread spill) of a tank overfill/rupture/spill/ etc.	$1 \times 10^{-2} - 1 \times 10^{-3}$	1×10^{-2}
Open Vent (no valve)	Will prevent over pressure	$1 \times 10^{-2} - 1 \times 10^{-3}$	1×10^{-2}
Fireproofing	Will reduce rate of heat input and provide additional time for depressurizing/firefighting/etc.	$1 \times 10^{-2} - 1 \times 10^{-3}$	1×10^{-2}
Blast-wall/ Bunker	Will reduce the frequency of large consequences of an explosion by confining blast and protecting equipment/buildings/etc.	$1 \times 10^{-2} - 1 \times 10^{-3}$	1×10^{-3}
"Inherently Safe" Design	If properly implemented can significantly reduce the frequency of consequences associated with a scenario. Note: the LOPA rules for some companies allow inherently safe design features to eliminate certain scenarios (e.g., vessel design pressure exceeds all possible high pressure challenges).	$1 \times 10^{-1} - 1 \times 10^{-6}$	1×10^{-2}
Flame/ Detonation Arrestors	If properly designed, installed and maintained these should eliminate the potential for flashback through a piping system or into a vessel or tank.	$1 \times 10^{-1} - 1 \times 10^{-3}$	1×10^{-2}

TABLE 6.4
Examples of Active IPLs

IPL	Comments *Assuming an adequate design basis and inspection/maintenance procedures*	PFD from Literature and Industry	PFD Used in This Book (For screening)
Relief valve	Prevents system exceeding specified overpressure. Effectiveness of this device is sensitive to service and experience.	$1 \times 10^{-1} - 1 \times 10^{-5}$	1×10^{-2}
Rupture disc	Prevents system exceeding specified overpressure. Effectiveness can be very sensitive to service and experience	$1 \times 10^{-1} - 1 \times 10^{-5}$	1×10^{-2}
Basic Process Control System	Can be credited as an IPL if not associated with the initiating event being considered (see also Chapter 11). (See IEC 61508 (IEC, 1998) and IEC 61511 (IEC, 2001) for additional discussion.)	$1 \times 10^{-1} - 1 \times 10^{-2}$ ($>1 \times 10^{-1}$ allowed by IEC)	1×10^{-1}
Safety Instrumented Functions (Interlocks)	See IEC 61508 (IEC, 1998) and IEC 61511 (IEC, 2001) for life cycle requirements and additional discussion		
SIL 1	Typically consists of: Single sensor (redundant for fault tolerance) Single logic processor (redundant for fault tolerance) Single final element (redundant for fault tolerance)	$\geq 1 \times 10^{-2} - < 1 \times 10^{-1}$	This book does not specify a specific SIL level. Continuing examples calculate a required PFD for a SIF
SIL 2	Typically consists of: "Multiple" sensors (for fault tolerance) "Multiple" channel logic processor (for fault tolerance) "Multiple" final elements (for fault tolerance)	$\geq 1 \times 10^{-3} - < 1 \times 10^{-2}$	
SIL 3	Typically consists of: Multiple sensors Multiple channel logic processor Multiple final elements	$\geq 1 \times 10^{-4} - < 1 \times 10^{-3}$	

Note: Multiple includes 1 out of 2 (1oo2) and 2 out of 3 (2oo3) voting schemes

"Multiple" indicates that multiple components may or may not be required depending upon the architecture of the system, the components selected and the degree of fault tolerance required to achieve the required overall PFD and to minimize unnecessary trips caused by failure of individual components (see IEC 61511 (IEC, 2001) for guidance and requirements).

TABLE 6.5
Examples of Human Action IPLs*

IPL	Comments *Assuming adequate documentation, training and testing procedures*	PFD from Literature and Industry	PFD Used in This Book (For screening)
Human action with 10 minutes response time.	Simple well-documented action with clear and reliable indications that the action is required	$1.0 - 1 \times 10^{-1}$	1×10^{-1}
Human response to BPCS indication or alarm with 40 minutes response time	Simple well-documented action with clear and reliable indications that the action is required. (The PFD is limited by IEC 61511; IEC 2001.)	1×10^{-1} ($>1 \times 10^{-1}$ allowed by IEC)	1×10^{-1}
Human action with 40 minutes response time	Simple well-documented action with clear and reliable indications that the action is required	$1 \times 10^{-1} - 1 \times 10^{-2}$	1×10^{-1}

* Based on *Inherently Safer Chemical Processes: A Life Cycle Approach* (CCPS 1996b), *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications* (Swain 1983).

پیوست د: نمونه‌هایی از مواردی که مانع یا لایه حفاظتی مستقل نیستند.

TABLE 6.1
Examples of Safeguards Not Usually Considered IPLs

Safeguards not Usually Considered IPLs	Comments
Training and Certification	These factors may be considered in assessing the PFD for operator action, but are not—of themselves—IPLs.
Procedures	These factors may be considered in assessing the PFD for operator action, but are not—of themselves—IPLs.
Normal Testing and Inspection	These activities are assumed to be in place for all hazard evaluations and form the basis for judgment to determine PFD. Normal testing and inspection affects the PFD of certain IPLs. Lengthening the testing and inspection intervals may increase the PFD of an IPL.
Maintenance	This activity is assumed to be in place for all hazard evaluations and forms the basis for judgment to determine PFD. Maintenance affects the PFD of certain IPLs.
Communications	It is a basic assumption that adequate communications exist in a facility. Poor communications affects the PFD of certain IPLs.
Signs	Signs by themselves are not IPLs. Signs may be unclear, obscured, ignored, etc. Signs may affect the PFD of certain IPLs.
Fire Protection	Active fire protection is often not considered as an IPL as it is post event for most scenarios and its availability and effectiveness may be affected by the fire/explosion which it is intended to contain. However, if a company can demonstrate that it meets the requirements of an IPL for a given scenario it may be used (e.g., if an activating system such as plastic piping or frangible switches are used). *Note:* Fire protection is a mitigation IPL as it attempts to prevent a larger consequence subsequent to an event that has already occurred. Fireproof insulation can be used as an IPL for some scenarios provided that it meets the requirements of API and corporate standards.
Requirement that Information is Available and Understood	This is a basic requirement.

Note: Poor performance in the areas discussed in this table may affect the process safety of the whole plant and thus may affect many assumptions made in the LOPA process.

پیوست ه: نمای کلی یک نمودار پاپیون