ISIRI-IEC
60300-3-9
1st. Edition

جمهوری اسلامی ایران
Islamic Republic of Iran
مؤسسه استاندارد وتحقیقات صنعتی ایران
Institute of Standards and Industrial Research of Iran

استاندارد ایران–آی‌ای‌سی
۹-۳-۶۰۳۰۰
چاپ اول

مدیریت قابلیت اعتماد
قسمت۳: راهنمای کاربرد
بخش ۹: تحلیل ریسک سیستم‌های تکنولوژیکی

Dependability management – Part3:Application guide- Section 9: Risk analysis of technological systems

ICS:03.100.40 ; 03.120.01

به‌نام خدا

آشنایی با مؤسسهٔ استاندارد و تحقیقات صنعتی ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که تکلیف تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان مؤسسه* صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می‌شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی(رسمی) ایران چاپ و منتشر می‌شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذیصلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیتهٔ ملی طرح و ارزشیابی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود .بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که مؤسسه استاندارد تشکیل می‌دهد به تصویب رسیده باشد.

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین المللی بهره‌گیری می‌شود.

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران می‌تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشو ر و / یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. مؤسسه می‌تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سا زمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل اندازه گیری ، مؤسسهٔ استاندارد این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آنها نظارت می‌کند .ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل اندازه گیری، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این مؤسسه است.

---

* موسسهٔ استاندارد و تحقیقات صنعتی ایران

1- International organization for Standardization
2 - International Electro technical Commission
3- International Organization for Legal Metrology (Organization International de Metrology Legal)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« مدیریت قابلیت اعتماد، قسمت۳: راهنمای کاربرد، بخش ۹: تحلیل ریسک سیستم‌های تکنولوژیکی »

رئیس:	**سمت و/ یا نمایندگی**
سقایی، عباس (دکترای مهندسی صنایع)	هیئت علمی دانشگاه آزاد- نایب رئیس انجمن مدیریت کیفیت ایران
دبیر:	
ذرّه، مهدی (کارشناس ارشد مهندسی برق)	کارشناس استاندارد
اعضاء: (اسامی به ترتیب حروف الفبا)	
بستان دوست راد، احسان (کارشناس مهندسی صنایع)	مدیر عامل شرکت مهندسی سیستم‌های مدیریت قابلیت اعتماد توازن
ذرّه، هومن (کارشناسی ارشد ریاضی)	شرکت واصل الکتریک الوند
راعی، جلال (کارشناس ارشد مدیریت)	معاونت آماد و پشتیبانی دانشگاه هوایی- کارشناس استاندارد
سیدی نیاکی، کیوان (کارشناس ارشد مکانیک -تبدیل انرژی)	عضو هیئت علمی سازمان پژوهش های علمی و صنعتی ایران
طوماریان، سهیلا (کارشناس مهندسی الکترونیک)	کارشناس مسئول دفتر امور تدوین موسسه استاندارد و تحقیقات صنعتی ایران
عزیززاده، عین اله (کارشناس ارشد مهندسی معدن)	کارشناس ارشد، شرکت مهندسی سیستم‌های مدیریت قابلیت اعتماد توازن
فرحانی، فواد	عضو هیئت علمی سازمان پژوهش های علمی و

(دکترای مهندسی مکانیک) صنعتی ایران

فهرست مندرجات

پیش گفتار

استاندارد «مدیریت قابلیت اعتماد، قسمت۳: راهنمای کاربرد، بخش ۹: تحلیل ریسک سیستم‌های تکنولوژیکی » که پیش نویس آن درکمیسیون های مربوط توسط "شرکت مهندسی سیستم های مدیریت قابلیت اعتماد توازن" تهیه و تدوین شده و در هشتاد و ششمین اجلاس کمیتهٔ ملی استاندارد مدیریت کیفیت مورخ ۱۳۸۸/۰۶/۰۷ مورد تصویب قرار گرفته است ، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ ، به عنوان استاندارد ملی ایران منتشر می‌شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

منبع و ماخذی که برای تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

IEC 60300-3-9: 1995, First Edition, Dependability management –Part3:Application guide-Section 9: Risk analysis of technological systems

مقدمه

فرآیند مدیریت ریسک شامل عناصر متعددی از شناسایی اولیه و تحلیل ریسک، تا ارزشیابی قابلیت تحمل آن و شناسایی گزینه های بالقوه کاهش ریسک از طریق انتخاب، اجرا و پایش اقدامات مناسب کنترلی و کاهشی می باشد . این فرآیند در شکل ۱ شرح داده شده است .

تحلیل ریسک – که موضوع این استاندارد است – فرآیند ساختار یافته ای است که احتمال و گستره عواقب و عواقب منفی ناشی از فعالیت، وسیله یا سیستم معین را شناسایی می کند. عواقب زیانبار مورد توجه در مطالب این استاندارد شامل آسیب و ضایعات فیزیکی به افراد، دارایی ها و محیط زیست است.

تحلیل ریسک تلاش می کند تا به سه پرسش اساسی پاسخ دهد :

چه چیزی ممکن است نادرست شود (با شناسایی خطر) ؟

احتمال وقوع این حادثه چقدر است (با تحلیل فراوانی) ؟

عواقب چیست (با تحلیل عواقب) ؟

هدف این استاندارد انعکاس رویه‌های مناسب کنونی جهت انتخاب و کاربرد فنون تحلیل ریسک بوده و به مفاهیم جدید یا نوظهور که به سطح مناسبی از اجماع حرفه ای نرسیده اند رجوع نمی نماید.

این استاندارد ماهیتی عمومی داشته و لذا می‌تواند راهنمایی‌هایی در بسیاری از صنایع و انواع سیستم ها ارائه دهد. ممکن است استانداردهای خاص‌تری در صنایع مذکور وجود داشته باشد که روش شناسی‌های مطلوب و سطوح تحلیل مناسب در کاربردهای ویژه را تشریح نماید. اگر استانداردهای خاص دارای هماهنگی کامل با محتویات این استاندارد باشند، عموما استانداردهای مذکور کافی خواهند بود.

این استاندارد صرفا بخش تحلیل ریسک از فعالیت‌های گسترده‌تر ارزیابی و مدیریت ریسک را در بر می‌گیرد. مورد اخیر ممکن است در استانداردهای آتی مطرح شوند. این استاندارد تا حد امکان بر مبنای مفاهیم و واژگان ارائه شده در مدارک فهرست شده در بند ۲ و سایر استانداردها، بنا شده است. موارد متعدی را می‌توان ذکر نمود که مدارک مورد اشاره فاقد هماهنگی کامل بوده و یا عمدتا فقط برای یک صنعت قابل استفاده هستند. در این موارد، استاندارد حاضر می تواند یکی از رویکرد ها/ تعاریف را به کار برده و یا تعریف عمومی تری را ارائه نماید .

مدیریت قابلیت اعتماد- قسمت۳: راهنمای کاربرد، بخش ۹: تحلیل ریسک سیستم‌های تکنولوژیکی

۱ هدف و دامنه کاربرد

این استاندارد حاوی راهنمایی هایی برای انتخاب و اجرای روش‌های تحلیل ریسک اولیه برای ارزیابی ریسک سیستم‌های تکنولوژیکی است. هدف این استاندارد حصول اطمینان از کیفیت و سازگاری در طرح ریزی و اجرای تحلیل ریسک و ارائه نتایج و نتیجه گیری ها است.

این استاندارد حاوی راهنمایی هایی برای تحلیل ریسک به این شرح است: مفاهیم تحلیل ریسک، فرآیند تحلیل ریسک، روش‌های تحلیل ریسک.

این استاندارد به صورت زیر قابل کاربرد است:

- راهنمایی برای طرح‌ریزی، اجرا و مستندسازی تحلیل ریسک.
- مبنایی برای مشخص‌کردن الزامات کیفی تحلیل ریسک (این موضوع مخصوصاً زمانی که با مشاورین بیرونی سروکار داشته باشد، می‌تواند مهم باشد)
- مبنایی برای ارزیابی تحلیل ریسک بعد از انجام.

تحلیل ریسک انجام شده مطابق این استاندارد یک ورودی برای فعالیتهای مدیریت ریسک فراهم می آورد(به شکل۱ مراجعه شود)

یادآوری – این استاندارد معیارهای خاصی برای شناسایی نیاز تحلیل ریسک یا مشخص کردن نوع خاص روش تحلیل ریسک الزام شده برای یک وضعیت معین، ارائه نمی‌کند. همچنین فاقد راهنمایی های تفصیلی برای خطرات خاص یا منافع بیمه، آماری، قانونی و مالی است.

۲ مراجع الزامی

مراجع الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آنها ارجاع شده است. به این ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می شوند. در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آنها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه های بعدی آن مورد نظر می باشد.

استفاده از مراجع زیر برای این استاندارد الزامی است.

۲-۱ استاندارد ملی ایران، ۱۳۸۸: ۱۹۱-۱۰۴۲۵، واژگان الکتروتکنیک، فصل ۱۹۱، قابلیت اعتماد و کیفیت خدمت

۲-۲ استاندارد ملی ایران، ۲-۶۰۳۰۰، مدیریت قابلیت اعتماد-قسمت دوم: عناصر و تکالیف برنامه قابلیت اعتماد

2-3 IEC 60812: 1985, Analysis techniques sor system reliability – Procedure for failure mode and effects analysis (FMEA)
2-4 IEC 61025: 1990, Fault tree analysis (FTA)
2-5 IEC 61078: 1991, Analysis techniques for dependability – Reliability block diagram method

۳ اصطلاحات و تعاریف

در این استاندارد علاوه بر اصطلاحات و تعاریف استاندارد ملی ۱۹۱-۱۰۴۲۵، اصطلاحات و تعاریف زیر به کار می رود.

۳-۱

آسیب[1]

جراحت فیزیکی یا صدمه به سلامتی، دارایی‌ها یا محیط‌زیست.

۳-۲

خطر[2]

منبع آسیب بالقوه یا وضعیتی با استعداد برای آسیب.

۳-۳

رخداد خطرناک[3]

رخدادی که می‌تواند موجب آسیب شود.

۳-۴

شناسایی خطر[4]

فرآیند تشخیص وجود خطر و تعریف ویژگیهای آن.

۳-۵

ریسک[5]

ترکیب فراوانی، یا احتمال، وقوع و عواقب یک رخداد خطرناک خاص.

یادآوری- مفهوم ریسک همواره دو عنصر دارد: فراوانی یا احتمال وقوع یک رخداد خطرناک و عواقب آن رخداد خطرناک.

1 - Harm
2 - Hazard
3 - Hazardous event
4 -Hazard identification
5 - Risk

۶-۳

تحلیل ریسک[1]

کاربرد سیستماتیک اطلاعات موجود برای شناسایی خطرات و برآورد ریسک برای افراد یا جوامع، دارایی‌ها یا محیط‌زیست (به شکل۱ رجوع کنید).

یادآوری- تحلیل ریسک را گاهی اوقات تحلیل ایمنی احتمالی، تحلیل ریسک احتمالی، تحلیل ایمنی کمی و تحلیل ریسک کمی نیز می‌نامند.

۷-۳

ارزیابی ریسک[2]

فرآیند کلی تحلیل ریسک و ارزیابی ریسک (به شکل۱ رجوع کنید).

۸-۳

کنترل ریسک[3]

فرآیند تصمیم‌گیری برای مدیریت و/یا کاهش ریسک؛ پیاده‌سازی، اجرا کردن و ارزشیابی مجدد هرازچندگاهی آن با استفاده از نتایج ارزیابی ریسک به عنوان یک ورودی.

۹-۳

برآورد ریسک[4]

فرآیند مورد استفاده برای تعیین مقیاس سطح ریسکهای مورد تحلیل. برآورد ریسک شامل این گام‌ها است: تحلیل فراوانی، تحلیل عواقب و انسجام آنها.

۱۰-۳

ارزشیابی ریسک[5]

فرآیند کارشناسی دربارهٔ قابلیت تحمل ریسک بر مبنای تحلیل ریسک و در نظر گرفتن عواملی مثل جنبه‌های اجتماعی – اقتصادی و زیست محیطی.

۱۱-۳

مدیریت ریسک[6]

کاربرد سیستماتیک خط مشی ها، روش های اجرایی و رویه های مدیریت برای تکالیف تحلیل، ارزشیابی و کنترل ریسک (به شکل ۱ رجوع شود).

---

1 - Risk analysis
2- Risk assessment
3 - Risk control
4 - Risk estimation
5- Risk evaluation
6- Risk management

۱۲-۳

سیستم[1]

مقوله ای مرکب، با هر سطحی از پیچیدگی، از کارکنان، روش های اجرایی، مواد، ابزار، تجهیزات، تسهیلات و نرم‌افزارها. عناصر این مقوله ی مرکب در کنار هم و در محیط عملیاتی یا پشتیبانی مورد نظر برای انجام یک وظیفه خاص یا رسیدن به یک هدف مشخص بکار گرفته می‌شوند.

۴ مفاهیم تحلیل ریسک

۱-۴ مفاهیم پایه و هدف‌تحلیل ریسک

ریسک در همهٔ فعالیت های انسان وجود دارد و می‌تواند مربوط به سلامت و ایمنی(به طور مثال شامل هر دو تاثیرات فوری و بلند مدت سلامتی در مواجهه با سموم شیمیایی)، اقتصاد(به طور مثال پیامد خرابی تجهیزات و ضایع شدن محصولات بر اثر آتش، انفجار یا تصادفات دیگر) یا اثر بر محیط زیست باشد. هدف مدیریت ریسک، کنترل، جلوگیری و یا کاهش تلفات انسانی، بیماری، آسیب و یا خسارات وارده به دارایی‌ها و خسارت های متعاقب و اثرات زیست‌محیطی است.

قبل از آنکه ریسک بتواند به نحو اثر بخشی مدیریت شود، بایستی تحلیل شود. تحلیل ریسک ابزار مفیدی است برای:

الف) شناسایی ریسک و رویکرد های حل آن ها

ب) تأمین اطلاعات عینی برای تصمیم‌گیری

پ) برآوردن الزامات قانونی

نتایج یک تحلیل ریسک را می‌تواند برای کمک به کارشناسی دربارهٔ قابلیت تحمل ریسک و کمک در انتخاب بین کاهش ریسک بالقوه یا مقیاس اجتناب از ریسک توسط تصمیم‌گیر بکار برده شود.

برخی از مزایای اصلی تحلیل ریسک از دیدگاه تصمیم‌گیران عبارتست از:

الف) شناسایی سیستماتیک خطرات بالقوه

ب) شناسایی سیستماتیک انواع وقوع خرابی بالقوه

پ) بیانیه ها یا رتبه‌بندی کمی ریسک

ت) ارزشیابی تعدیلات ممکن برای کاهش ریسک یا دست یابی به سطوح بهتری از قابلیت اعتماد

ث) شناسایی مؤلفه‌های مهم ریسک و پیوندهای ضعیف در یک سیستم

ج) درک بهتر سیستم و نصب آن

چ) مقایسهٔ ریسک با ریسک سیستم‌ها یا فناوریهای جایگزین

ح) شناسایی و تبادل ریسک‌ها و عدم قطعیت ها

خ) کمک به استقرار اولویت‌ها در بهبود سلامت و ایمنی

د) مبنایی برای نگهداری پیشگیرانه و بازرسی که باید منطقی باشد

1- System

ذ) تحقیق پس از رخداد و پیشگیری
ر) انتخاب میان گزینه‌ها مثل اقدامات و فناوری‌های مختلف کاهش ریسک.
همهٔ موارد فوق نقش مهمی در مدیریت اثر بخش ریسک دارند و تفاوتی نمی‌کند که هدف اصلی بهبود شرایط مرتبط با سلامت و ایمنی است یا جلوگیری از زیان اقتصادی و یا انطباق با مقررات دولتی.
تحلیل ریسک غالباً یک رویکرد چند رشته ای را الزام می‌کند زیرا می‌تواند حوزه‌ها و تخصص‌های زیر را پوشش دهد:
الف) تحلیل سیستم‌ها
ب) احتمالات و آمار
پ) مهندسی شیمی، مکانیک، برق، سازه یا هسته‌ای
ت)علوم فیزیک، شیمی یا زیست شناسی
ث) علوم سلامتی شامل سم‌شناسی و همه‌گیر شناسی
ج) علوم اجتماعی شامل اقتصاد، روانشناسی و جامعه‌شناسی
چ) عوامل انسانی، ارگونومی و علوم مدیریت.

۲-۴ مدیریت ریسک و رده بندی ریسک

تحلیل ریسک بخشی از فرآیند ارزیابی و مدیریت ریسک مطابق شکل ۱ است و شامل تعریف دامنه کاربرد، شناسایی خطر و برآورد ریسک می‌باشد.
خطرات در چهار رده کلی گروه‌بندی می‌شود، به نام های :
الف) خطرات طبیعی (سیل، زلزله، طوفان، صاعقه)
ب) خطرات تکنولوژیکی (تأسیسات صنعتی،سازه‌ها، سیستم‌های حمل‌ونقل، محصولات مصرفی، آفت‌کش‌ها، علف‌کش‌ها، داروها)
پ) خطرات اجتماعی (شورش، جنگ، خرابکاری، بیماری‌های واگیر)
ت) خطرات سبک زندگی (مصرف مواد مخدر،الکل، دخانیات)
بدیهی است که این گروه ها ممکن است هم‌زمان رخ دهند و هنگام تحلیل خطرات فنی غالباً لازمست تأثیر عوامل سایر رده ها (به ویژه خطرات طبیعی) و سایر سیستم‌ها را نیز به عنوان بخشی از تحلیل ریسک در نظر گرفت.
ریسک را هم‌چنین می‌توان بر اساس ماهیت عواقبی که مورد تحقیق قرار می گیرند، رده بندی کرد. مثلاً:
الف) فردی (اثر بر تک تک اعضاء جامعه)
ب) شغلی (اثر بر کارگران)
پ) اجتماعی(اثر کلی بر جامعه)
ت) خسارت به دارایی‌ها و زیان اقتصادی(وقفه تجاری، جرائم و...)
ث) زیست‌محیطی (اثر بر زمین، هوا، آب، گیاهان، جانوران و میراث فرهنگی).

هدف کلی تحلیل ریسک ارائه مبنای عقلانی برای تصمیمات مربوط به ریسک است. این تصمیمات به عنوان بخشی از فرآیند مدیریت ریسک بزرگ تر، از طریق مقایسه نتایج ریسک با معیارهای قابلیت تحمل ریسک، اتخاذ خواهند شد. در مواقع زیادی لازمست که ارزیابی منافع برای گرفتن یک تصمیم متعادل، بر یک پایه ی مورد–به–مورد انجام شود. موضوع کلی معیارهای تحمل پذیری ریسک بسیار پیچیده بوده، شامل ملاحظات اجتماعی،اقتصادی و سیاسی هستند و لذا خارج از دامنه کاربرد این استاندارد قرار می‌گیرند.

۳-۴ کاربرد تحلیل ریسک طی فازهای چرخهٔ عمر

برخی اهداف خاص تحلیل ریسک وابسته به فاز ها مختلف چرخهٔ عمر (به استاندارد ملی ۲-۶۰۳۰۰ مراجعه شود) سیستم‌ها، تأسیسات یا محصولات خطرناک به این صورت است:

الف) فازهای مفهوم و تعریف/ طراحی و تکوین:

۱) شناسایی مولفه‌های عمده ریسک و عوامل مهم دخیل
۲) تأمین ورودی به فرآیند طراحی و ارزیابی کفایت کل طراحی
۳) شناسایی و ارزشیابی مقیاس های ممکن ایمنی در طراحی
۴) فراهم کردن ورودی برای ارزیابی قابلیت پذیرش تأسیسات، فعالیتها یا سیستم های خطرناک پیشنهادی
۵) تأمین اطلاعات لازم برای یاری به روش های اجرایی تکوین در شرایط عادی و اضطراری
۶) ارزشیابی ریسک در رابطه با قوانین و سایر الزامات
۷) ارزشیابی مفاهیم طراحی جایگزین

ب) مراحل ساخت، نصب، بهره‌برداری و نگهداری:

۱) پایش و ارزشیابی تجربه ها برای مقایسهٔ عملکرد واقعی با الزامات مربوط
۲) فراهم کردن ورودی در بهینه‌سازی عملکرد عادی و روش‌های اجرایی اضطراری نگهداری/بازرسی
۳) به روز رسانی اطلاعات مربوط به مؤلفه‌های اصلی ریسک و عوامل موثر
۴) تأمین اطلاعات مربوط به اهمیت ریسک برای تصمیم‌گیری مربوط به بهره‌برداری
۵) ارزشیابی اثرات تغییر در ساختار سازمانی، رویه ها و روش‌های اجرایی بهره‌برداری و اجزای سیستم
۶) تمرکز بر فعالیتهای آموزشی

پ) فاز وارهایی: توقف کاربرد:

۱) ارزشیابی ریسک مربوط به فعالیت‌های وارهایی سیستم و حصول اطمینان از برآورده شدن الزامات
۲) تأمین ورودی در روش های اجرایی وارهایی

۵ فرآیند تحلیل ریسک

۵-۱ مرور کلی

برای ارتقاء کیفی اثر بخشی و عینیت تحلیل ریسک و سهولت قیاس با سایر تحلیل‌های ریسک، بایستی سری قوانین کلی را رعایت نمود. فرآیند تحلیل ریسک بایستی مطابق توالی گام های تعیین شده زیر انجام شود:

الف) تعریف دامنه ی کاربرد؛

ب) شناسایی خطر و ارزشیابی عواقب اولیه؛

پ) برآورد ریسک؛

ت) تصدیق؛

ث) مستندسازی؛

ج) روزآمدی تحلیل.

این فرآیند در شکل ۲ نشان داده شده است. برآورد ریسک شامل تحلیل فراوانی و پیامد است. اگر چه مستندسازی به صورت قلم جداگانه‌ای ارائه شده ولی در همهٔ مراحل فرآیند تکوین می‌شود. بسته به حوزهٔ کاربرد، ممکن است نیاز باشد فقط برخی عناصر فرآیند نشان داده شده در نظر گرفته شود. برای مثال در برخی موارد فراتر رفتن ازتحلیل اولیه خطر و عواقب نیازی نیست.

دانش کامل از سیستم و روش‌های تحلیل مورد استفاده الزام شده است. در صورتی که تحلیل ریسک برای سیستم مشابه موجود باشد می‌توان به‌عنوان مرجع از آن استفاده کرد. هر چند که این فرآیند ها مشابه اند یا تغییرات ایجاد شده تغییرات چشمگیری را در نتایج ایجاد نخواهد کرد، بایستی اثبات شود. اینکار بایستی بر مبنای ارزشیابی سیستماتیک تغییرات و راه هایی که آن ها می توانند بر خطرات مختلف موجود تاثیر بگذارند، باشد.

۵-۱-۱ کارکنان تحلیل ریسک

تحلیل‌گران ریسک بایستی برای پذیرفتن تکالیف شایسته باشند. بسیاری سیستم‌ها برای فهم کامل توسط یک فرد بیش از حد پیچیده‌اند و گروهی از تحلیل گران برای انجام دادن کار مورد نیازند. فرد یا گروه کاری بایستی با روش های استفاده شده برای تحلیل ریسک آشنا باشند و دانش کاملی از موضوع تحت بررسی داشته باشند. دانش اختصاصی ضروری دیگر بایستی مطابق نیاز فراهم شود و در تحلیل ادغام شود. تخصص گروه کاری باید مشخص و ثبت گردد.

۵-۲ تعریف دامنه کاربرد

دامنه کاربرد تحلیل ریسک باید تعریف و مستند شود تا طرح تحلیل ریسک در ابتدای پروژه ایجاد شود (به استاندارد ملی ۲-۶۰۳۰۰ مراجعه کنید). تعریف دامنه کاربرد تحلیل ریسک بایستی شامل گام‌های ذیل باشد:

الف) علل و/یا مشکلات که منجر به تحلیل ریسک شده را شرح دهید. این کار شامل مراحل زیر می‌شود:

۱) فرمول بندی اهداف تحلیل ریسک بر اساس دغدغه‌های اصلی شناسایی شده؛

۲) تعریف معیارهای موفقیت/ وقوع خرابی سیستم. دغدغه اصلی ممکن است نتیجه‌ای نامطلوب (مثل وقوع خرابی سیستم، رهایی مواد سمی) یا شرایط بالقوه زیان‌آور باشد.

ب) سیستم مورد تحلیل را تعریف کنید. تعریف باید شامل موارد زیر باشد:

۱) توصیف کلی سیستم؛

۲) تعریف مرزها و واسط[1]ها با سیستمهای مرتبط فیزیکی و وظیفه‌ای؛

۳) تعریف محیط؛

۴) تعریف انرژی، مواد و اطلاعات جاری در مرزها؛

۵) تعریف شرایط بهره‌برداری که به‌وسیله تحلیل ریسک و محدودیت‌های مرتبط در بر گرفته می‌شوند.

پ)شناسایی منابع ارائه دهنده جزئیات فنی، محیطی،قانونی، سازمانی و وضعیت انسانی مرتبط با فعالیت و مشکل مورد تحلیل. بویژه هر نوع اوضاع احوال مرتبط با ایمنی نیز بایستی توصیف شود؛

ت) مفروضات و قید و بندهای حاکم بر تحلیل را بیان کنید؛

ث) تصمیماتی که باید گرفته شود، خروجی الزام شده از بررسی و تصمیم‌گیران را شناسایی کنید.

تکلیف تعریف دامنه کاربرد تحلیل همچنین بایستی شامل آشناسازی کامل با سیستم تحلیل شده به عنوان فعالیت طرح ریزی شده باشد. یکی از اهداف آشناسازی، تعیین این است که کجا و چگونه می‌توان به دانش تخصصی دسترسی یافت و آنها را در تحلیل یکپارچه کرد.

۳-۵ شناسایی خطر و ارزشیابی اولیه عواقب

خطراتی را که در سیستم ریسک ایجاد می‌کنند بایستی به همراه راه‌هایی که در آن خطرات می‌توانند تحقق یابد، شناسایی شوند. خطرات شناخته شده (شاید در حوادث قبلی تحقق یافته باشد) باید به روشنی بیان شود. برای شناسایی خطراتی که قبلاً شناسایی نشده‌اند، روش‌های قراردادی دربرگیرنده وضعیت خاص بایستی بکار برده شوند(به ۷-۳-۱ مراجعه فرمایید).

ارزشیابی اولیه از اهمیت خطرات مشخص شده بایستی بر مبنای تحلیل عواقب به همراه آزمایش علل ریشه‌ای انجام شود. این موضوع باید یکی از مراحل کاری ذیل را تعیین کند:

الف) اقدامات اصلاحی در این نقطه به قصد حذف یا کاهش خطرات اتخاذ کنید؛

ب) به تحلیل در این جا خاتمه دهید زیرا خطرات یا عواقبشان ناچیزند.

پ) برآورد ریسک را ادامه دهید.

مفروضات اولیه و نتایج باید مستند شوند (به ۵-۶ مراجعه فرمایید)

۴-۵ برآورد ریسک

برآورد ریسک بایستی رخدادها یا اوضاع احوال آغازگر – ترتیب رخدادهای مورد نگرانی- خصیصه های کاهش دهنده و ماهیت و فراوانی عواقب مخرب امکان پذیر خطرات شناسایی شده را جهت فراهم آوردن مقیاسی از سطح ریسک های مورد تحلیل را آزمایش کند. این مقیاس های ریسک انسان، می‌تواند به دارایی

1 -Interface

یا محیط را بپردازند و بایستی شامل نشان‌دهی عدم قطعیت مرتبط به برآوردها باشند. این فرآیند در ۵-۴-۱، ۵-۴-۲و ۵-۴-۳ به صورت اجمالی تهیه شده است. روش‌های تحلیل ریسک در جدول ۱ توصیف شده‌اند.
روش‌های استفاده شده در برآورد ریسک اغلب کمی‌اند، اگرچه درجه جزئیات الزام شده در آماده‌سازی برآوردها به کاربردهای خاص وابسته خواهند بود(به شکل ۷-۲ مراجعه فرمایید). در هر حال تحلیل‌های کاملاً کمی به دلیل ناکافی بودن اطلاعات درباره سیستم یا فعالیت مورد تحلیل، کمبود داده‌های وقوع خرابی، تاثیر عوامل انسانی و غیره، همیشه ممکن نخواهند بود. در چنین وضعیتی رتبه بندی قیاسی کمی یا کیفی ریسک‌ها توسط متخصصان مطلع در حوزه مربوطه آن‌ها هنوز ممکن است مؤثر باشد. در مواردی که رتبه‌بندی کیفی است، بایستی توصیف روشنی از همهٔ اصطلاحات به‌کار گرفته شده و مبنای رده‌بندی همه فراوانی‌ها و عواقب ثبت شود جایی که تحلیل کاملاً کمی انجام می‌شود نیاز است به این مسئله توجه شود که مقادیر محاسبه شده ریسک برآورد شده‌اند و بایستی دقت به‌عمل آید اطمینان حاصل شود که آن‌ها به‌سطحی از درستی و دقت ناسازگار با درستی داده‌ها و روش‌های تحلیلی به‌کار گرفته شده، منسوب نشده‌اند.
عناصر فرآیند برآورد ریسک برای همه خطرات، مشترک هستند. نخست علل ممکن خطر جهت تعیین فراوانی وقوع، مدت و ماهیت آن (کمیت، ترکیب ، خصوصیات رهایی[1]/ کاربرد و غیره) تحلیل می‌شنود. در صورت تحلیل کردن امکانات صنعتی، این تحلیل فراوانی، ممکن است فعالیتی عمده باشد. در صورت تحلیل کردن یک زنجیره ی شیمایی غذایی- به عنوان مثال- تحلیل خیلی کمتری ضروری است. دوم، عواقب رهایی خطر تحلیل می‌شوند. این تحلیل عواقب شامل برآورد شدت عواقب مرتبط با خطر است. این تحلیل همچنین می‌تواند برآورد احتمال منجر شدن خطر به عواقب را، الزام کند و بنابراین می‌تواند تحلیل توالی رخدادها را که توسط ان خطر می‌تواند منجر به عواقب (ها) شود را، شامل شود.

۵-۴-۱ تحلیل فراوانی

از تحلیل فراوانی برای برآورد احتمال هر یک از رخدادهای نامطلوب شناسایی شده در مرحله شناسایی خطر استفاده می‌شود. معمولاً سه رویکرد برای برآورد فراوانی رخداد به‌کار برده می‌شود (به ۷-۳-۲-۱ مراجعه فرمایید)، که عبارتند از:
الف)استفاده از داده های پیشین مربوط؛
ب) استنتاج کردن فراوانی‌های رخداد به کمک فنون تحلیلی یا شبیه‌سازی؛
پ)استفاده کردن از کارشناسی متخصصین.
تمامی فنون فوق ممکن است به تنهایی یا همراه هم بکار برده شوند. دو رویکرد اول مکمل هستند، هر کدام در جایی که دیگری ضعف هایی دارد، دارای قوت هایی هستند. در صورت امکان بایستی هر دو را به کار برد. بدین‌ترتیب آنها می توانند به عنوان وارسی های مستقل از یکدیگر استفاده شوند و این ممکن است در افزایش اطمینان نتایج بکار رود. هنگامی که ازآن ها نمی توان استفاده کرد یا کافی نیستند، ممکن است ضروری باشد که تا حدی به درجات از کارشناسی متخصصین تکیه شود.

---

1 -Release

۵-۴-۲ تحلیل عواقب

تحلیل عواقب برای برآورد پیامدهای احتمالی که ممکن است در اثر رخدادهای نامطلوب رخ دهند، استفاده می‌شود.

تحلیل عواقب بایستی:

الف) بر مبنای رخدادهای نامطلوب انتخاب شده باشد؛

ب) همه عواقب ناشی از رخدادها نامطلوب را شرح دهد؛

پ) مقیاس‌های موجود برای کاهش عواقب به همراه همه شرایط مربوطه که تأثیری بر عواقب دارند، را در نظر بگیرد.

ت) معیارهای مورد استفاده در تکمیل شناسایی عواقب را ارائه دهد.

عواقب بلافصل و آن هایی که ممکن است بعد از گذشت زمان مشخصی رخ دهند را اگر با دامنه کاربرد بررسی سازگارند، در نظر بگیرد.

ج) عواقب ثانویه مثل آن عواقبی که به تجهیزات و سیستم‌های مجاور مرتبطند را در نظر بگیرد.

۵-۴-۳ محاسبات ریسک

ریسک بایستی با مناسب‌ترین عبارات بیان شود. برخی از خروجی‌های مورد استفاده مشترک عبارتند از:

الف) پیش‌بینی فراوانی مرگ و میر یا شیوع بیماری یک فرد (ریسک فردی)؛

ب) نمودارهای فراوانی در برابر عواقب (معروف به منحنی‌های F-N که F بیان کننده فراوانی و N عدد تجمعی افرادی که از سطح صدمه مشخصی رنج می‌برند یا هزینهٔ تجمعی آسیب است) برای ریسک اجتماعی؛

پ) نرخ مورد انتظار زیان آماری بر اساس مصدومین، هزینهٔ اقتصادی یا آسیب های محیطی؛

ت) توزیع ریسک سطحی آسیب مشخص که به‌صورت نمودار تراز نمایش داده می‌شود که سطوح آسیب یکسان را نمایش می‌دهد.

بایستی بیان شود که آیا برآورد ریسک، سطح کلی ریسک را منعکس می‌کند یا فقط بخشی از کل ریسک را شامل می‌شود.

در محاسبه سطوح ریسک نیاز است طول مدت رخداد نامطلوب و احتمال این‌که مردم در معرض آن قرار خواهند گرفت، به حساب آیند.

داده های مورد استفاده در محاسبه ی سطح ریسک بایستی متناسب با کاربرد ویژه باشند. در صورت امکان چنین اطلاعاتی بایستی بر مبنای اوضاع احوال خاص تحت تحلیل، باشد. جایی که آن ها موجود نباشند داده های معرف ماهیت تمام موقعیت باید بکارفته شوند، یا کارشناسی متخصصین طلب شود.

داده ها باید به شکلی جمع‌آوری و سازماندهی شوند که بازیابی راحت اطلاعات برای ورودی تحلیل ریسک و قابلیت پیگیری را تسهیل کنند. داده هایی که دیگر با موقعیت کنونی مرتبط نیستند بایستی شناسایی شوند و استفاده ی آن ها در تحلیل کنا گذاشته شوند.

۵-۴-۴ عدم قطعیت ها

عدم قطعیت های زیادی در رابطه با برآورد ریسک وجود دارند. فهم عدم قطعیت ها و علل آنها برای تفسیر اثر بخش مقادیر ریسک الزامی است. تحلیل عدم قطعیت ها مرتبط با داده‌ها، روش‌ها و مدل‌های مورد استفاده در شناسایی و برآورد ریسک دخیل، نقش مهمی در کاربرد آنها ایفا می‌کند. تحلیل عدم قطعیت شامل تعیین واریانس و عدم دقت در نتایج مدل است که ناشی از واریانس تجمعی پارامترها و مفروضات مورد استفاده در تعریف مدل می‌باشد. حوزه‌ای که ارتباط نزدیکی با تحلیل عدم قطعیت‌ها دارد تحلیل حساسیت است. تحلیل حساسیت شامل تعیین تغییر در پاسخ مدل به تغییرات در هر یک از پارامترهای مدل است.

برآورد عدم قطعیت عبارت است از ترجمه عدم قطعیت در پارامترهای مدل بحرانی به عدم قطعیت در خروجی های مدل ریسک. تکمیل و درستی برآورد ریسک بایستی تا بیشترین حد امکان بیان شود. در صورت امکان بایستی منابع عدم قطعیت را شناسایی نمود. این موضوع باید به عدم قعطیت داده‌ها و مدل اشاره کند. پارامترهایی که تحلیل نسبت به آنها حساس است بایستی بیان گردند.

۵-۵ تصدیق تحلیل

برای تأیید یکپارچگی تحلیل می بایست یک فرآیند بازنگری رسمی توسط افرادی که در کار دخیل نیستند انجام شود. بازنگری ها مجاز است به‌صورت داخلی هدایت شود یا با استفاده از سازمان‌هایی خارج از آن‌هایی که تحلیل را انجام داده‌اند.

تصدیق بایستی شامل گام های ذیل باشد:

الف) این‌که دامنه کاربرد برای اهداف بیان شده مناسب است، را وارسی کنید؛

ب) همهٔ مفروضات اصلی و اطمینان از معتبر بودن آنها بر اساس اطلاعات موجود را بازنگری کنید؛

پ) از این‌که تحلیل‌گر از روش‌ها، مدل‌ها و داده‌های مناسب استفاده کرده است، اطمینان حاصل کنید؛

ت) این‌که تحلیل توسط کارکنان دیگر جز تحلیل‌گر(ها) اصلی نیز قابل تکرار است را وارسی کنید؛

ث) عدم حساسیت نتایج تحلیل به روش قالب بندی داده‌های و نتایج را وارسی کنید.

در صورت وجود تجربهٔ میدانی کافی، تصدیق می‌تواند با مقایسه نتایج تحلیل با مشاهدات مستقیم تحلیل گر انجام شود.

۵-۶ مستندسازی

گزارش تحلیل ریسک، فرآیند تحلیل ریسک را مستند می‌کند و بایستی طرح تحلیل ریسک و نتایج ارزشیابی اولیه خطر را شامل باشد یا به آنها اشاره کند. ارائه اطلاعات فنی در مستند سازی بخش حیاتی از فرآیند تحلیل ریسک است. برآوردهای ریسک بایستی با عبارات قابل فهم بیان شود، نقاط قوت و محدودیتهای مقیاس های مختلف ریسک استفاده شده بایستی توضیح داده شود و عدم قطعیت حول و حوش برآورد ریسک بایستی با زبان مناسب مخاطب منظور شود.

وسعت گزارش به اهداف و دامنه کاربرد تحلیل بستگی دارد. غیر از تحلیل‌های بسیار ساده، مستندسازی به طور مشترک بایستی به موارد ذیل بپردازد:

الف) خلاصه
ب) نتیجه گیری ها
پ) اهداف و دامنه کاربرد؛
ت) محدودیت‌ها، مفروضات و توجیه فرضیه‌ها؛
ث) شرح بخش‌های مرتبط سیستم؛
ج) روش‌شناسی تحلیل؛
چ) نتایج شناسایی خطرات؛
ح) مدل‌های مورد استفاده، شامل فرض ها و معتبر سازی؛
خ) داده‌ها و منابع آنها؛
د) نتایج برآورد ریسک؛
ذ) تحلیل حساسیت و عدم قطعیت؛
ر) بحث درباره نتایج (شامل بحث دربارهٔ دشواری‌های تحلیلی)؛
ز) مراجع.

۷-۵ به روز رسانی تحلیل

اگر تحلیل ریسک ملزم به پشتیبانی فرآیند مستمر مدیریت ریسک باشد بایستی به نحوی اجرا و مستندسازی شود که در طول عمر چرخه سیستم، تسهیلات یا فعالیت بتواند نگهداری شود. به‌محض این‌که که اطلاعات معنادار جدید آماده و مطابق با نیازهای فرآیند مدیریت باشند، تحلیل بایستی به روزرسانی شود.

۶ ممیزی ها

درصورت الزام بایستی ممیزی فرآیند تحلیل ریسک توسط افرادی که مستقیماً در اجرای تحلیل ریسک نقش نداشته‌اند، انجام گیرد تا از اثر بخشی و تبعیت آن از این استاندارد تضمین شود. بایستی از فرآیندها و روش‌های اجرایی تضمین کیفیت مرتبط استفاده شود.

۷ روش‌های تحلیل ریسک

۷-۱ کلیات

این بند به شرح برخی روش‌های رایج برای تحلیل سیستم‌های تکنولوژیکی می‌پردازد که برای شناسایی خطر و برآورد ریسک، به همراه معیارها برای انتخابشان، قابل استفاده اند.

۷-۲ انتخاب روش ها

به بیان کلی، روش مناسب باید ویژگی های زیر را نشان دهد:
الف) بایستی از نظر علمی قابل دفاع بوده و برای سیستم تحت بررسی مناسب باشد.
ب) بایستی نتایج را به نحوی ارائه کند که درک بهتر از ماهیت ریسک و چگونگی کنترل آن را ارتقاء بخشد.
پ) بایستی بتوانند برای استفاده ی انواع انجام دهندگان به شیوه‌ای که قابل پیگیری، قابل تکرار و قابل تصدیق باشد مناسب باشد.

علل انتخاب روش‌ها بایستی با توجه به ارتباط و مناسبت آن ها، بیان شوند. در صورت تردید پیرامون ارتباط یا مناسبت، بایستی روش‌های جایگزین بکار برده شوند و نتایج مقایسه شوند. هنگام تلفیق نتایج بررسی ها مختلف بایستی روش‌شناسی ها و خروجی های سازگار باشند.

به محض اخذ تصمیم برای اجرای تحلیل ریسک و تعریف اهداف و دامنه ی کاربرد، روش یا روش ها بایستی بر مبنای عوامل قابل کاربرد انتخاب شوند –به شکل ۳ مراجعه نمایید- برای مثال:

الف) فاز تکوین سیستم. در مراحل تکوین اولیه می‌توان از روش‌های کلی‌تر استفاده کرد. وقتی اطلاعات بیشتر موجود باشند، بایستی آنها را تصحیح نمود؛

ب) اهداف بررسی. اهداف تحلیل تأثیر مستقیمی روی روش های مورد استفاده دارند. برای مثال، اگر یک بررسی ی مقایسه ای بین گزینه های مختلف بعهده گرفته شود، می‌تواند برای استفاده ی مدل هایی با عواقب نسبتاً نا مطلوب برای قسمت‌هایی از سیستم که از تفاوت ها تاثیر نمی پذیرند، قابل قبول باشد؛

پ) نوع سیستم و خطر مورد تحلیل؛

ت) سطح بالقوه ی شدت. تصمیم‌گیری در مورد عمق تحلیل باید دیدگاه اولیه در خصوص عواقب را منعکس کند(اگرچه ممکن است این موضوع به محض این‌که ارزشیابی اولیه تکمیل شد تغییر داده شود)؛

ث) نیروی انسانی، درجه تخصص و منابع الزام. تا زمانی که اهداف و دامنه ی کاربرد تحلیل را براورده کند، روش ساده‌ای که به خوبی اجرا شود می‌تواند نتایج بهتری نسبت به روش اجرایی پیچیده‌ای که ضعیف اجرا شده باشند ارائه کند. به‌طور مشترک میزان تلاش انجام شده در تحلیل بایستی هم سان با سطح بالقوه ی ریسک مورد تحلیل باشد؛

ج) موجود بودن اطلاعات و داده‌ها. برخی روش‌ها به اطلاعات و داده‌های بیشتری از بقیه نیاز دارند؛

چ) نیاز به تعدیل/ به روز رسانی تحلیل. ممکن است تحلیل نیاز داشته باشد که در آینده تعدیل/ به روز رسانی شود و برخی مدل‌ها از این نظر قابل اصلاح تراند؛

ح) کلیه ی الزامات نظارتی و قراردادی؛

۳-۷ روش‌های تحلیل

برخی از متداول‌ترین روش‌های مورد استفاده در جدول ۱ ارائه و همچنین در زیر شرح داده شده‌اند. البته فهرست جدول ۱ به هیچ‌وجه جامع نمی‌باشد. توضیح مختصری از برخی روش‌های مورد استفاده نیز در پیوست الف ارائه شده‌اند. گاهی اوقات لازم است بیش از یک روش تحلیل را به کار ببریم.

۱-۳-۷ شناسایی خطر

شناسایی خطر به بازنگری سیستماتیک سیستم مورد بررسی برای شناسایی نوع خطرات ذاتی موجود به همراه راه هایی که می توانند تحقق یابند، می‌پردازد. سوابق حادثه ی تاریخی و تجربه ی تحلیل‌های ریسک قبلی می‌توانند ورودی سودمندی برای فرآیند شناسایی خطر باشند. باید قبول کنیم که یک عنصر ذهنیت در کارشناسی در مورد خطرات وجود دارد و خطرات شناسایی شده ممکن است همواره تنها خطرهایی که می توانند تهدیدی برای سیستم ایجاد کنند، نباشند. مهم است که خطرات شناسایی شده بر حسب هر نوع داده ی جدید مرتبط بازنگری می‌شوند. روش‌های شناسایی خطر به طور کلی در ۳ رده قرار می‌گیرند:

الف) روش‌های مقایسه‌ای، که مثال‌هایی از آن‌ها فهرست وارسی، شاخص‌های خطر و بازنگری داده های تاریخی می باشند؛
ب) روش‌های بنیادی که ساختار آن ها متضمن برانگیختن گروهی از افراد برای بکارگیری آینده نگری در ارتباط با دانششان برای تکلیف شناسایی خطرات از طریق طرح سری پرسش های " اگر ... شد، چه؟" است. بررسی خطر و قابلیت بهره‌برداری[1](HAZOP) و تحلیل انواع و آثار خرابی [2](FMEA) مثالهایی از این نوع روش‌شناسی هستند؛
پ) فنون استدلال استقرایی مثل نمودارهای منطق درخت رخداد.
برای مشکلات خاص می‌توان سایر فنون را جهت بهبود شناسایی خطر بکار برد(و توانمندی های برآورد ریسک). برخی مثال ها شامل موارد ذیل می باشند: تحلیل پنهانی، روش‌شناسی دلفی و تحلیل قابلیت اطمینان انسان.
صرف نظر از فنون عملی به‌کار برده شده، مهم است که در فرآیندهای کلی شناسایی خطر شناخت کافی به این حقیقت که خطاهای انسانی و سازمانی عواملی مهمی در خیلی اتفاقات هستند، داده شود. به این دلیل که سناریوی اتفاقی بایستی شامل خطای انسانی و سازمانی باشد، فرآیند شناسایی خطر نبایستی منحصراً به جنبه های "سخت افزاری" اشاره کند.

۲-۳-۷ برآورد ریسک

در عمل، شناسایی خطر سیستم ویژه، تسهیلات یا فعالیت ممکن است به سناریوهای بسیار متعدد حوادث بالقوه منجر شود و ممکن است همواره تحلیل عواقب و فراوانی کمی تفصیلی امکان پذیر نباشد. در این شرایط رتبه‌بندی سناریوهای حوادث به‌صورت کیفی و قرار دادن آنها در یک ماتریس ریسک، حاوی سطوح مختلف ریسک می‌تواند منطقی باشد. سپس کمی سازی بر سناریو های ارزیابی شده منجر به سطوح بالاتر ریسک متمرکز می‌شود. شکل ۴ مثالی از یک ماتریس ریسک را نشان می دهد. کاربرد ماتریس ریسک می‌تواند منجر شود که سناریو های بررسی شده با ریسک کم یا جزئی از بررسی های بعدی تا زمانی که آن‌ها مجتمعاً نتوانند به سطوح معنادار ریسک ارتقا یابند حذف شوند. ماتریس‌های ریسک متعددی وجود دارند؛ مناسب‌ترین آنها برای یک تحلیل معلوم به کاربرد ویژه بستگی دارد. ضروری است که شکل هر ماتریس استفاده شده به همراه موقعیت برآورد شده ی تمام سناریوهای حادثه در نظر گرفته شده و بدون توجه به این‌که آن ها متعاقباً تحت تحلیل کمی تفصیلی قرار می گیرند، ثبت شوند.
تحلیل کمی ریسک معمولاً برآورد فراوانی (یا احتمال) رخداد نامطلوب و عواقب همبسته (یا شدت) برای فراهم ساختن مقیاس ریسک را الزام می‌کند. به هر حال در برخی موارد – مثلاً وقتی محاسبات نشان می‌دهد که عواقب معنادار نباشند یا فراوانی بسیار اندک است- ممکن است برآورد تک پارامتری کافی باشد.

1 -Hazard and Operability
2 -Fault Modes and Efects Analysis

۷-۳-۲-۱ تحلیل فراوانی

مقصود از تحلیل فراوانی، تعیین فراوانی هر رخداد نامطلوب یا سناریوهای حادثه ی شناسایی شده در مرحله شناسایی خطر است. معمولاً سه رویکرد اساسی اتخاذ می‌شوند:

الف) استفاده از داده‌های پیشین برای تعیین فراوانی که با آن این رخدادها در گذشته اتفاق افتاده‌اند و سپس کارشناسی‌هایی در مورد فراوانی وقوع آنها در آینده. داده‌های مورد استفاده بایستی متناسب با نوع سیستم، تسهیلات یا فعالیت مورد بررسی و همچنین مرتبط با استانداردهای بهره‌برداری سازمان دخیل، باشند؛

ب) پیش‌بینی فراوانی رخداد با استفاده از فنونی مثل تحلیل درخت خرابی و تحلیل درخت رخداد. در صورت فقدان یا ناکافی بودن داده‌های تاریخی ضروری است که فراوانی رخداد را با تحلیل سیستم و انواع خرابی‌های مربوط آن بدست آورید. داده‌های عددی مربوط به تمام رخدادهای مرتبط، شامل وقوع خرابی تجهیزات و خطای انسانی حاصل از تجربیات بهره‌برداری یا منابع داده منتشر شده، برای تولید برآوردی از فراوانی رخداد نامطلوب تلفیق می‌شوند. هنگام استفاده از فنون پیش‌بینی لازم است اطمینان حاصل کنیم که هزینه کافی در تحلیل امکان‌پذیری وقوع خرابی‌های نوع مشترک شامل وقوع خرابی همزمان تعدادی از قسمت‌های مختلف یا اجزاء در داخل سیستم داده شده است. فنون شبیه سازی ممکن است برای تولید فراوانی های وقوع خرابی تجهیزات و ساختاری به علت پیری و دیگر فرآیندهای تنزل با محاسبه تاثیرات عدم قطعیت ها، لازم باشد.

پ) استفاده از کارشناسی متخصصین. تعدادی روش‌های رسمی برای استنباط کارشناسی متخصصین وجود دارد که کاربرد کارشناسی ها را عینی و صریح می‌کند و کمکی برای پرسیدن سوالات مناسب فراهم می‌کند. کارشناسی متخصصین بایستی بر مبنای همه اطلاعات موجود مرتبط شامل اطلاعات تاریخچه‌ای، خاص-سیستم، تجربی، طراحی انجام شود. روش‌های موجود شامل رویکرد دلفی، مقایسه ی جفتی، مقادیر اسمی رده و کارشناسی مطلق بر احتمال می‌باشد.

تحلیل درخت خرابی و تحلیل درخت رخداد در پیوست الف این استاندارد شرح داده شده‌اند. IEC 61025 به تفضیل تحلیل درخت خرابی می‌پردازد.

۷-۳-۲-۲ تحلیل عواقب

تحلیل عواقب وقتی رخداد نامطلوب رخ دهد، شامل برآورد اثر بر افراد، دارایی‌ها یا محیط می‌باشد. به‌طور مشترک برای محاسبه ریسک مرتبط با ایمنی(برای جامعه یا کارکنان)، در وقوع رخداد نامطلوب این تحلیل شامل برآورد تعداد افراد مستقر در محیط‌های مختلف، در فواصل مختلف از منبع رخداد که ممکن است کشته شده،آسیب ببینند یا شدیداً تاثیر پذیرند، می‌شود.

رخدادهای نامطلوب معمولاً شامل شرایطی مثل رها شدن مواد سمی، آتش‌سوزی، انفجار،جسم پرتاب شده را تجهیزات از هم پاشیده و غیره می‌باشد. مدل‌های عواقب برای پیش‌بینی میزان مصدومین و اثرات دیگر مورد نیازند. دانش مکانیسم رهایی و عواقب مواد رها شده (یا انرژی) امکان انجام پیش‌بینی اثرات رهایی در فواصل مختلف از منبع در زمان‌های گوناگون را مقدور می‌کند.

روش‌های زیادی برای برآورد این اثرات از رویکرد تحلیلی ساده تا مدل‌های رایانه‌ای بسیار پیچیده وجود دارد. باید دقت شود تا اطمینان حاصل شود روش‌های انتخابی برای مشکل مورد نظر مناسب هستند

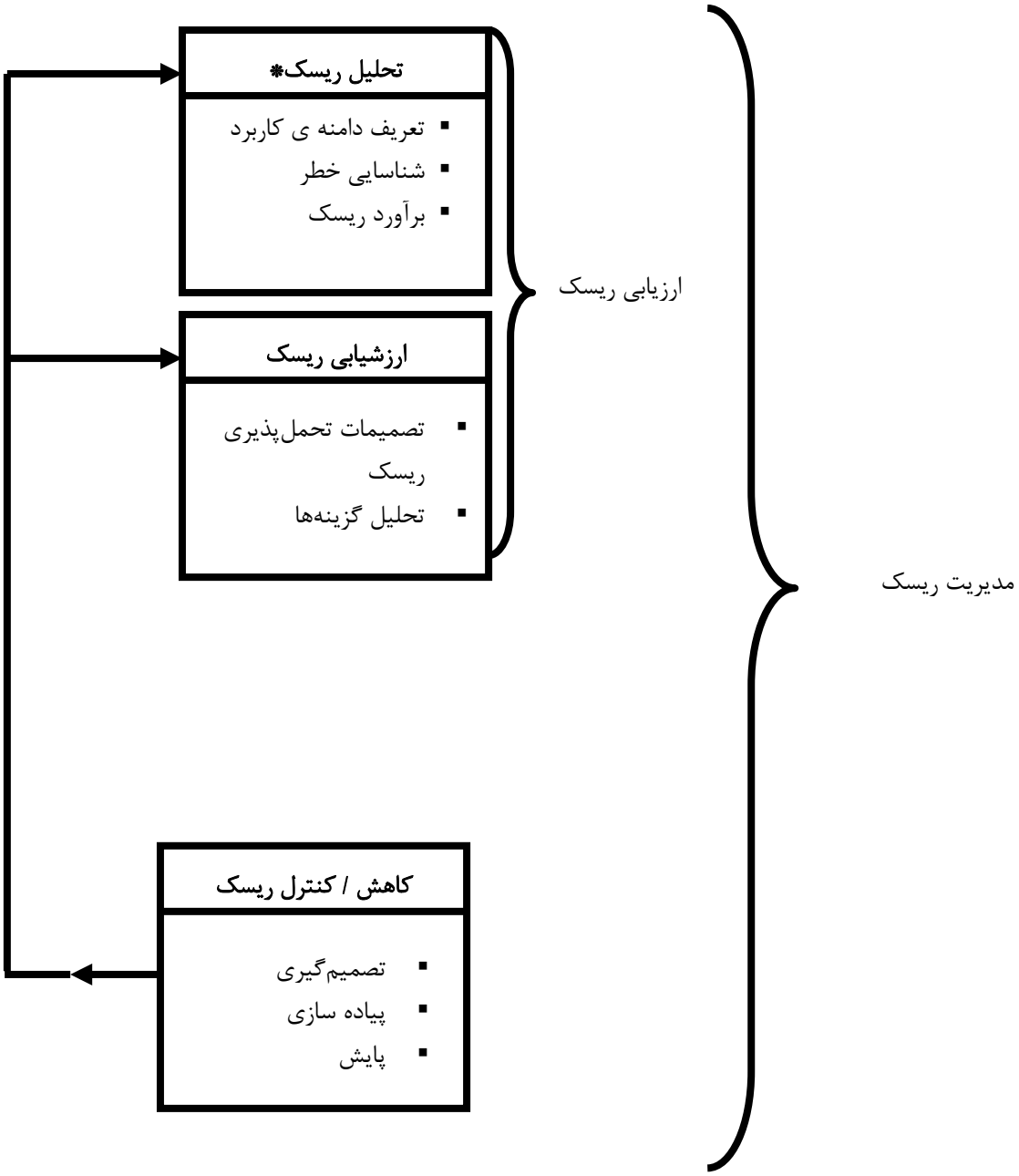
جدول ۱- روش‌های مورد استفاده در تحلیل ریسک

الف)متداول‌ترین روش‌ها

روش	شرح و کاربرد	منبع
تحلیل درخت رخداد	فن شناسایی خطرات و تحلیل فراوانی که از استدلال استقرایی برای تبدیل وقایع اولیه مختلف به نتایج ممکن استفاده می‌کند.	الف-۴
تحلیل انواع و آثارخرابی و تحلیل انواع، آثار و خطیر بودن خرابی	فن بنیادی تحلیل شناسایی خطرات و فراوانی، فنون تحلیل که همه انواع خرابی یک قلم تجهیزات برای آثارشان بر روی دیگر اجزاء و سیستم ها دیگر را تحلیل می‌کند.	IEC 60812 الف-۲
تحلیل درخت خرابی	فن شناسایی خطر و تحلیل فراوانی که با رخداد نامطلوب آغاز می‌شود و همه ی راه های وقوع آن را تعیین می‌کند. آنها به صورت گرافیکی نمایش داده می‌شوند.	IEC 61025 الف-۳
مطالعه خطر و قابلیت بهره‌برداری	فن بنیادی شناسایی خطر که هر بخش سیستم را به‌طور سیستماتیک ارزشیابی می‌کند تا ببیند انحراف از قصد طراحی چگونه می‌تواند رخ دهد و آیا می توانند منجر به مشکلات شوند.	الف-۱
تحلیل قابلیت اطمینان انسانی	فن تحلیل فراوانی که با اثر افراد روی کارآیی سیستم سر و کار دارد و تأثیر خطاهای انسانی بر قابلیت اطمینان را ارزشیابی می‌کند.	الف-۶
تحلیل مقدماتی خطر	فن شناسایی خطر و تحلیل فراوانی که می‌تواند در مراحل اولیه طراحی برای شناسایی خطرات و ارزیابی وخامت آنها به کار رود.	الف-۵
نمودار بلوکی قابلیت اطمینان	فن تحلیل فراوانی که مدلی از سیستم و زواید آن برای ارزشیابی قابلیت اطمینان کل سیستم ایجاد می‌کند.	IEC 61087

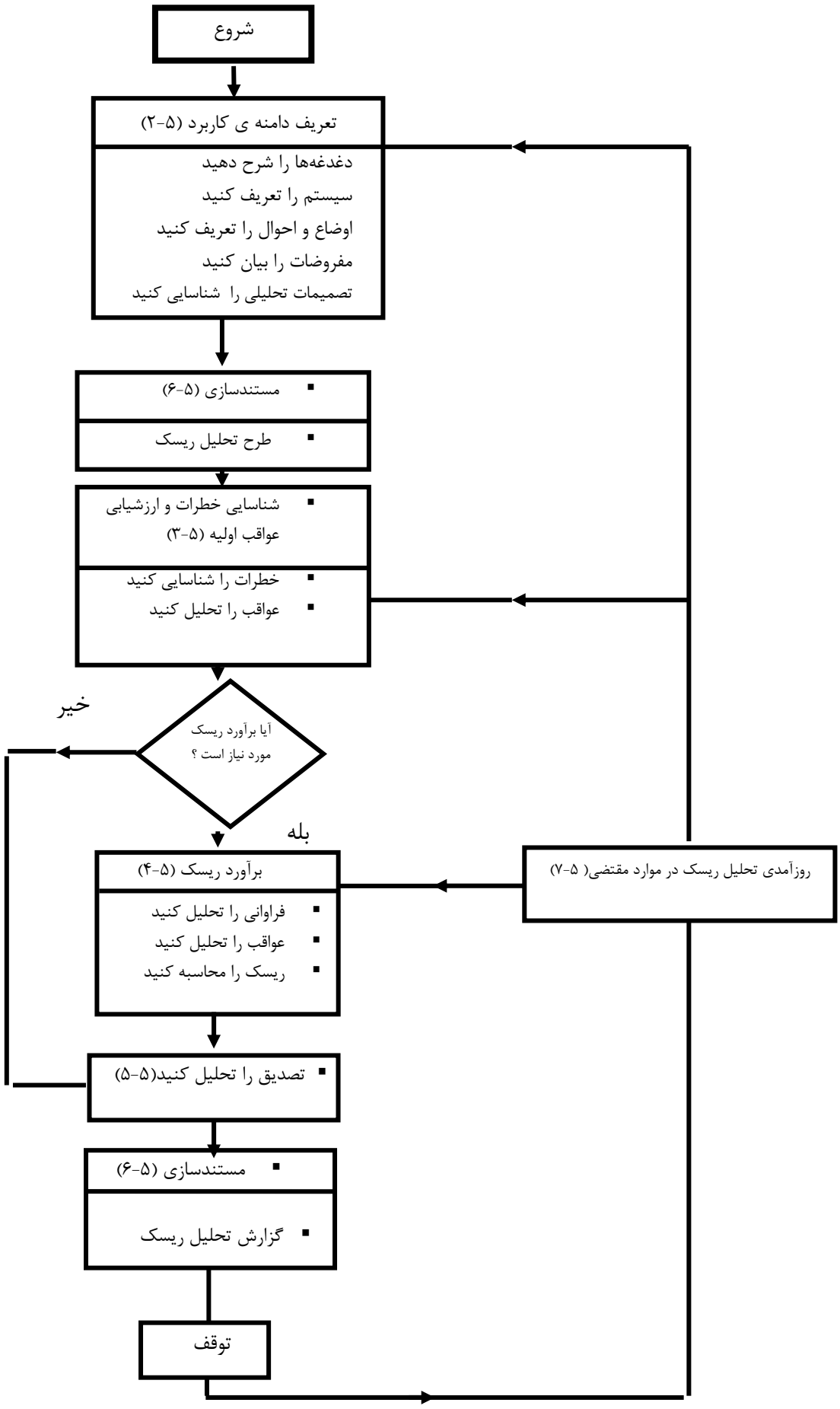
ب) روش های تکمیلی

روش	شرح و کاربرد
مقادر اسمی رده	روشی برای تعیین مقادیر اسمی ریسک ها بوسیله ی رده هایی که این ریسک ها در آن ها قرار می گیرند، که گروه ریسک هایی با اولویت را مشخص می‌کنند
فهرست وارسی	فن شناسایی خطر که فهرستی از مواد خطرناک معمول و/ یا منابع بالقوه حوادث که نیاز است در نظر گرفته شوند را ، ارائه می‌کند که می‌تواند انطباق با دستورعمل ها و استانداردها را ارزشیابی.
تحلیل نوع مشترک وقوع خرابی	روشی برای ارزیابی این‌که آیا وقوع خرابی همزمان چند قسمت یا جزء مختلف یک سیستم ممکن است و تاثر کلی محتمل آن
مدل‌های عواقب	برآورد اثر رخداد روی افراد، داراییها یا محیط. هر دو رویکرد تحلیلی ساده و مدل‌های رایانه‌ای پیچیده موجود است
فن دلفی	روشی برای ترکیب دیدگاه‌های تخصصی که می‌تواند تحلیل فراوانی، مدلسازی عواقب و/ یا برآورد ریسک را پشتیبانی کند
شاخص‌های خطر	فن شناسایی/ ارزشیابی خطر که می‌تواند برای رتبه‌بندی گزینه‌های مختلف و شناسایی کم خطرترین گزینه‌ها استفاده شود
شبیه‌سازی مونت-کارلو و سایر فنون شبیه‌سازی	فن تحلیل فراوانی که از مدل سیستم برای ارزشیابی تغییرات در شرایط و مفروضات ورودی استفاده می‌کند
مقایسه جفتی	روشی برای برآورد و رتبه‌بندی مجموعه ای از ریسک‌ها با نظر به یک جفت ریسک و ارزشیابی فقط یک جفت در هر زمان
بازنگری داده های تاریخی	یک فن شناسایی خطرات که می‌تواند برای شناسایی حیطه ی مشکلات بالقوه استفاده شود و همچنین برای تحلیل فراوانی، ورودی بر مبنای داده های سانحه و قابلیت اعتماد و دیگر، فراهم می‌کند
تحلیل پنهانی	روش شناسایی مسیرهای پنهان که می‌توانند موجب وقوع رخداد پیش‌بینی نشده شوند



* موضوع این استاندارد

شکل ۱- رابطهٔ ساده شده میان تحلیل ریسک و سایر فعالیتهای مدیریت ریسک



شکل ۲- فرآیند تحلیل ریسک (بند۵)

شکل ۳- ملاحظات نمونه در انتخاب نوع تحلیل و عمق بررسی

فراوانی رخداد	فراوانی اخباری (در هر سال)	شدت عواقب			
مکرر	$1<$	H	H	H	I
متحمل	$1\text{-}10^{-1}$	H	H	I	L
گاه به گاه	$10^{-1}\text{-}10^{-2}$	H	H	L	L
بعید	$10^{-2}\text{-}10^{-4}$	H	H	L	L
غیر متحمل	$10^{-4}\text{-}10^{-6}$	H	I	L	T
باورنکردنی	$10^{-6}>$	I	I	T	T
یادآوری – تعاریف و مقادیر این رده بکاربرده شده در این ماتریس تنها برای توضیح می‌باشد.					

که در آن طبقات ریسک

H= ریسک بالا

I= ریسک متوسط

L= ریسک پایین

T= ریسک ناچیز

برای این مثال، شدت عواقب رده ها به این صورت تعریف شده است:

فاجعه آمیز اتلاف کامل کارخانه یا سیستم در عمل. قربانیان زیاد

عمده صدمات وسیع به کارخانه یا سیستم. قربانیان کم

شدید جراحات شدید، بیماری‌های شغلی شدید، صدمات چشمگیر به کارخانه یا سیستم

جزئی جراحات جزئی، بیماری‌های شغلی جزئی یا صدمات جزئی به سیستم

شکل ۴- ماتریس ریسک

پیوست الف

(اطلاعاتی)

روش‌های تحلیل

الف-۱ مطالعه خطرات و قابلیت بهره‌برداری (HAZOP)

مطالعه HAZOP نوعی تحلیل انواع و آثار خرابی (FMEA) است. مطالعات HAZOP در آغاز در صنعت شیمیایی تکوین شد. مطالعه HAZOP فن سیستماتیک برای شناسایی خطرات و مشکلات بهره‌برداری سراسر یک تسهیلات کامل می‌باشد. این روش بخصوص در شناسایی خطرات پیش‌بینی نشده مفید می‌باشد که به علت کمبود اطلاعات، در تسهیلات طراحی شده یا به علت تغییر شرایط فرآیند یا روش اجرایی بهره‌برداری در تسهیلات موجود طراحی شده. اهداف اساسی این فنون عبارتند از:

الف) حصول یک توصیف کامل تسهیلات یا فرآیند شامل شرایط طراحی مورد نظر؛

ب) بازنگری سیستماتیک همه بخش‌های تسهیلات یا فرآیند به منظور کشف این‌که چگونه انحراف نسبت به قصد طراحی می‌تواند رخ دهد؛

پ) و تصمیم گرفتن در مورد این‌که آیا این انحرافات می‌تواند به خطر یا مشکلات بهره‌برداری منجر شود؛

اصول مطالعات HAZOP می‌تواند در کارخانه های فرآیندی در حال بهره‌برداری یا مراحل طراحی گوناگون به‌کار گرفته شود. مطالعه HAZOP انجام شده در طول فاز اولیه طراحی می‌تواند مکرراً راهنمایی برای طراحی تفصیلی ایمن تر فراهم کند.

متداول‌ترین شکل مطالعه HAZOP در فازهای تفصیلی طراحی انجام شده و آن را مطالعه HAZOPII می‌نامند.

مطالعه HAZOP II شامل مراحل زیر است:

۱) تعریف اهداف و دامنه کاربرد مطالعه، به عنوان مثال خطراتی که بر محل کار یا خارج از محل کار اثر می‌گذارند و نواحی از کارخانه که باید در نظر گرفته شوند و غیره؛

۲) جمع آوری تیم مطالعه HAZOP. این تیم بایستی متشکل از کارکنان طراحی و بهره‌برداری دارای تخصص فنی جهت ارزشیابی اثرات انحراف از عملیات مورد نظر باشد.

۳) جمع‌آوری اسناد، نمودارها و شرح فرآیندهای مورد نیاز. این موضوع شامل نمودار جریان فرآیند، نقشه ی لوله کشی و ابزار، تجهیزات، مشخصات لوله کشی و ابزار، ترسیم جانمایی کنترل فرآیند، نقشه‌های طرح کلی، روش‌های اجرایی بهره‌برداری و نگهداری، روش‌های پاسخگویی اضطراری و غیره می‌باشد.

۴) تحلیل هر قلم مهم از تجهیزات و تمام تجهیزات، لوله کشی، کاربرد ابزار پشتیبان، با استفاده از مستندات جمع‌آوری شده در گام ۳. قصد فرآیند طراحی در ابتدا تعریف شده سپس واژگان راهنما (به جدول الف-۱ مراجعه فرمایید) برای هر خط و قلم تجهیزات به منظور متغیرهای فرآیندی از قبیل دما، فشار، جریان، سطح و ترکیب شیمیایی اعمال می‌شود. (این واژگان راهنما تفکر فردی را برمی انگیزند و بحث گروهی ایجاد می‌کنند.)

۵) مستندسازی عواقب هر انحراف از نوع عادی و برجسته کردن انحرافاتی که خطرناک و معتبر شناخته شده‌اند. به علاوه روش برای کشف و/یا اجتناب از انحراف شناسایی می‌شود. این مستندسازی معمولاً در کربرگ های HAZOP صورت می‌گیرد. نمونه‌ای از چنین کاربرگی را برای واژه ی راهنمای «خیر، هیچ» مورد استفاده در «جریان» را در جدول الف-۲ نشان داده شده است.

یک مطالعه HAZOP ممکن است انحرافات خاص را که برای اقدامات کاهش دهنده لازم است تکوین شود را برجسته نماید. برای مواردی که مقیاس های کاهش دهنده واضح نیستند یا بالقوه خیلی پرهزینه اند، نتایج مطالعه HAZOP رخدادهای اولیه ضروری برای تحلیل ریسک بعدی را شناسایی خواهد کرد.

جدول الف-۱ واژگان راهنمای HAZOP II

واژگان	تعاریف
خیر یا هیچ	هیچ بخشی از نتیجه مورد نظر حاصل نشده است (مثلاً جریان وجود ندارد)
بیشتر	افزایش کمی (مثلاً فشار زیاد)
کمتر	کاهش کمی (مثلا فشار کم)
به اندازه	افزایش کیفی (مثلا مواد اضافه)
بخشی از	کاهش کیفی (مثلاً فقط یک یا دو مولفه در یک مخلوط کن)
بر عکس	معکوس (مثلا جریان برگشتی)
غیراز	هیچ بخشی از قصد به دست نیامده، واقعه‌ای کاملاً متفاوت رخ داده است (مثلاً جریان ماده اشتباه)

جدول الف-۲- نمونه کاربرگ HAZOP II برای واژهٔ راهنمای «خیر، هیچ»

واژه راهنما	انحراف	علل احتمالی	عواقب	اقدام لازم
خیر، هیچ	فاقد جریان	۱) ماده تغذیه کننده وجود ندارد	خروجی پلی مر کاهش یافته تشکیل خواهد شد	الف) از ارتباط خوب با اپراتور اطمینان حاصل کنید ب)اخطارکاهش سطح فراهم شده در مخزن تنظیم
		۲) پمپ خراب شده (علل مختلف)	مطابق ۱)	مطابق ب)
		۳) مسدود شدن خط یا دریچه در اثر خطا بسته شده یا کنترل دریچه خراب شده	مطابق الف-۱ پمپ بیش گرمایش پیدا می‌کند	نصب خط باز-گردش برای هر پمپ

الف-۲ تحلیل انواع خرابی و آثار آن (FMEA)

FMEA فن -اصولاً کیفی است که البته می‌تواند کمی شود- که به وسیله آن اثرات یا عواقب انواع خرابی جزء منفرد به‌طور سیستماتیک شناسایی می‌شوند. این فن، فنی استقرایی مبتنی بر پرسش «چه اتفاقی می‌افتد اگر... ؟» است. خصیصه ی اساسی در هر FMEA مطالعه هر قسمت/جزء عمده ی سیستم، چگونه

خراب می‌شوند(نوع خرابی) و اثر نوع خرابی روی سیستم چه خواهد بود(اثر نوع خرابی) است.معمولاً تحلیل توصیفی بوده و با ایجاد جدول یا کاربرگ برای اطلاعات سازمان دهی می‌شود.
به‌همین صورت FMEA به وضوح با انواع خرابی جزء، عوامل سببی و اثرات بر سیستم مرتبط است و آنها را در یک قالب خوانا ارائه می دهد.
FMEA رویکرد «پایین به بالا» بوده و در هر وهله عواقب یکی از انواع خرابی را بررسی می‌کند. به‌همین صورت این روش قبل از آنکه اجرای آن مشکل شود مستلزم مقدار کمی ردوندانسی است. همچنین نتایج می‌توانند به‌سهولت توسط فرد دیگر آشنا به سیستم تصدیق شود.
معایب عمده این فن شامل دشواری پرداختن به ردوندانسی و گنجاندن اقدامات تعمیر همچنین تمرکز روی وقوع خرابی جزء منفرد می‌باشد.
FMEA می‌تواند برای اجرای آنچه تحلیل انواع خرابی، اثرات و میزان بحرانیت (FMECA)[1] نامیده می‌شود، گسترش یابد. در FMECA هر نوع خرابی شناخته شده مطابق اثر ترکیبی احتمال وقوع و شدت عواقب آن رتبه‌بندی می‌شود. FMEA و FMECA ورودی برای تحلیل‌ها مثل تحلیل درخت خرابی را تأمین می‌کند. همچنین با پرداختن به اجزاء سیستم، می توانند به خطای انسانی نیز بپردازند. در شناسایی خطرات و برآورد احتمالات نیز می توانند به کار روند (اگر فقط سطح محدودی از ردوندانسی در سیستم حاضر باشد). جزییات بیشتری درباره FMEA و FMECA در IEC 60812 ارائه شده است.

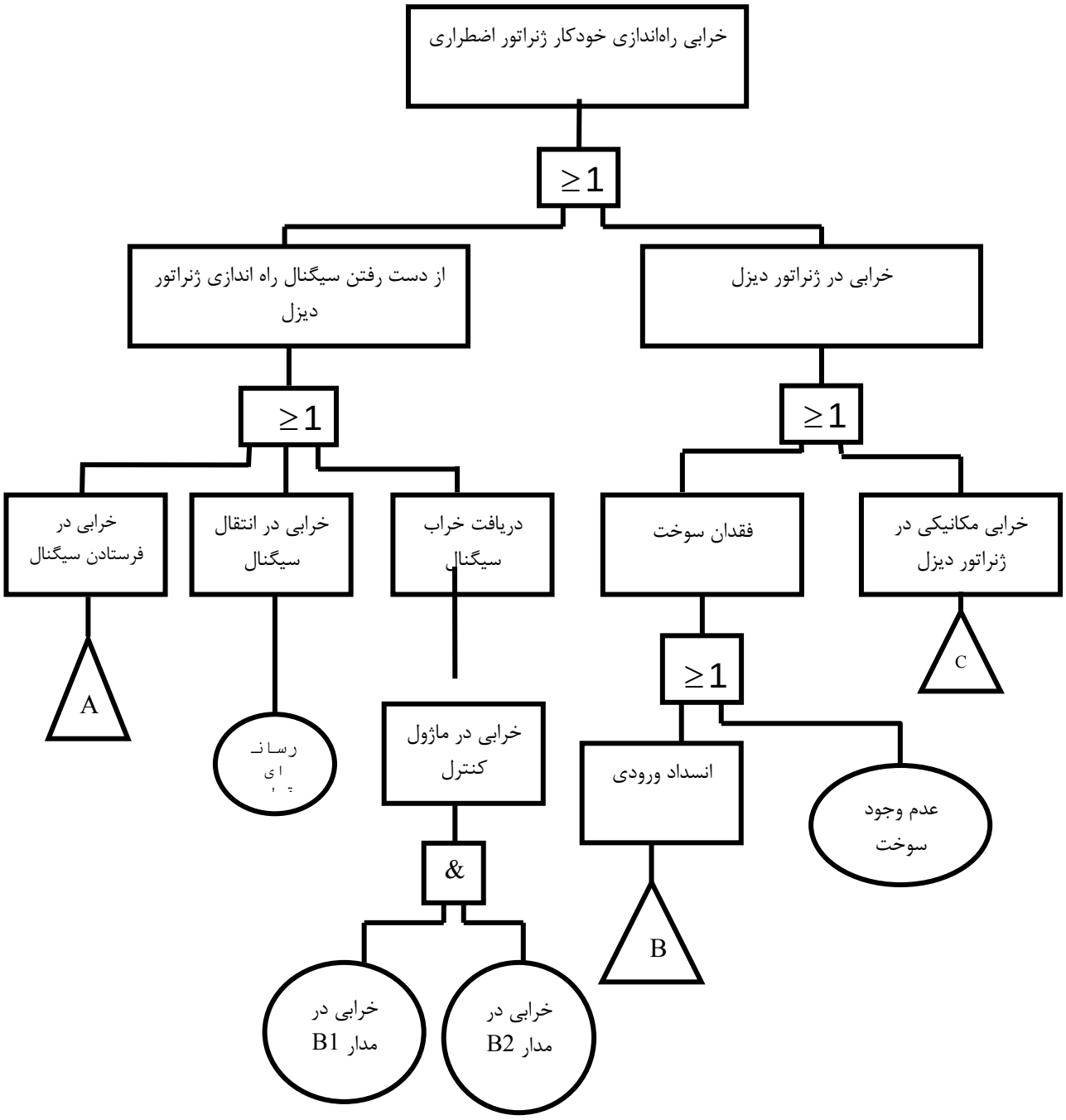
الف-۳ تحلیل درخت خرابی (FTA[2])

FTA فنی است که می‌تواند کیفی یا کمی‌باشد، که بوسیله ی آن شرایط و عواملی که می توانند در یک رخداد نامطلوب مشخص سهیم باشند (رخداد بالایی خوانده می‌شوند) به طور استقرایی شناسایی شده ، به‌طور منطقی سازماندهی شده و به‌صورت تصویری ارائه می‌شوند. خرابی شناسایی شده در درخت می‌تواند رخدادهایی باشد که با وقوع خرابی های جزء سخت افزاری، خطاهای انسان و یا هر رخداد وابسته که منجر به رخداد نامطلوب مرتبط باشند. با شروع رخداد بالایی، علل احتمالی یا انواع خرابی سطح پایین‌تر بعدی سیستم وظیفه‌ای شناسایی می‌شود. پیروی از شناسایی گام گام بهره‌برداری نامطلوب سیستم تا سطوح پایین سیستم متوالیاً به سطح مطلوب سیستم منجر خواهد شد، که معمولاً نوع خرابی جزء است. مثالی از درخت خرابی برای ژنراتور اضطراری در شکل الف-۱ ارائه شده است. جدولی از متداول‌ترین نمادهای درخت خرابی در شکل الف-۲ ارائه شده است.
FTA رویکردی منضبط را که کاملاً سیستماتیک است، حاصل می‌کند ولی در عین حال انعطاف‌پذیری کافی برای تحلیل انواع عوامل شامل تعاملات انسانی و پدیده‌های فیزیکی را دارد. کاربرد رویکرد «بالا به پایین» که در این فن نهفته است توجه را روی آن دسته از اثرات وقوع خرابی که مستقیماً با رخدادهای بالایی مرتبط هستند متمرکز می‌کند. این مزیت متمایزی است اگرچه ممکن است منجر به از دست رفتن اثراتی شود که در جای دیگری اهمیت دارد. FTA مخصوصاً در تحلیل سیستم‌هایی که واسط ها و تعاملات

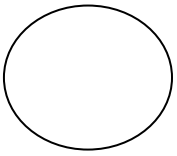
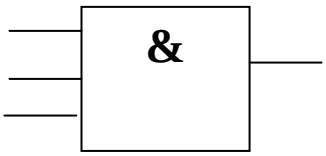
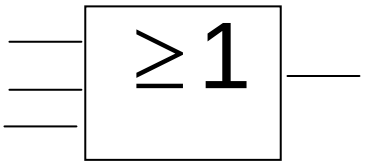
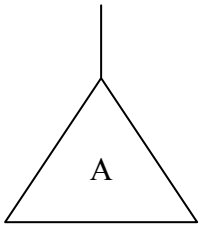
1 -Fault Mode, Effects and Criticality Analysis
2 -Fault Tree Analysis

متعددی دارند، مفید است. نمایش تصویری موجب درک ساده رفتار سیستم و عوامل درگیر می‌شود، اما از آن جا که درخت‌ها اغلب بزرگ اند، پردازش درخت‌های خرابی ممکن است نیازمند سیستم‌های رایانه‌ای باشد. همین خصیصه می‌تواند تصدیق درخت خرابی را مشکل سازد.

از FTA می‌توان برای شناسایی خطر نیز استفاده کرد البته آن در درجه اول در ارزیابی ریسک به‌عنوان ابزاری برای حصول برآورد احتمالات یا فراوانی های وقوع خرابی بکاررفته است . در IEC 61025 جزئیات بیشتری درباره FTA ارائه می‌شود.



شکل الف-۱ مثالی از درخت خرابی

نماد	وظیفه	توضیح
	بلوک توصیف رخداد	نام یا توصیف رخداد و کد رخداد احتمال وقوع (مطابق الزام) باید درون نماد قرار گیرد
	رخداد پایه	رخدادی که قابل تقسیم نیست
	دروازه ی AND	رخداد فقط در صورتی اتفاق می‌افتد که تمام ورودیها همزمان رخ بدهند.
	دروازه ی OR	رخداد در صورتی اتفاق می افتد که هر یک از رخداد های ورودی تنها یا در هر ترکیبی رخ دهد.
	انتقال	رخداد جای دیگری در درخت خطا تعریف شده است.

یادآوری – برگرفته از IEC 61025 و مورد استفاده در شکل الف-۱. البته قراردادهای مختلفی نیز برای نمادهای درخت خرابی وجود دارد.

شکل الف-۲ . نمادهای درخت خرابی

الف-۴ تحلیل درخت رخداد(ETA) [1]

ETA فنی - کیفی یا کمی - است که برای شناسایی نتایج احتمالی و در صورت لزوم -احتمال های آنها- با فرض وقوع یک رخداد آغازگر، بکار می‌رود. ETA به طور گسترده‌ای برای تسهیلات خصوصیات کاهشی حادثه مهندسی شده برای شناسایی توالی رخداد هایی که منجر به وقوع عواقب خاص، مجهز هستند در پی وقوع رخدادهای آغازگر، استفاده می‌شوند. به‌طور کلی فرض می‌شود که هر رخداد در توالی، موفقیت یا وقوع خرابی است. درخت رخداد ساده برای انفجار گرد و غبار با شمول احتمالات در شکل الف-۳ نشان داده شده است. توجه کنید که احتمالات موجود در درخت رخداد، احتمالات شرطی هستند، مثلاً احتمال انجام وظیفه

1 -Event Tree Analysis

کردن سیستم اطفاء حریق از آزمون ها در شرایط عادی احتمالاً بدست نمی‌آید بلکه احتمال انجام وظیفه کردن سیستم در شرایط آتش‌سوزی ناشی از انفجار به‌دست می آید.

ETA نوعی استقرایی تحلیل است که در آن به این پرسش اساسی پرداخت می‌شود که «چه اتفاقی می‌افتد اگر ...؟». این روش نوعی ارتباط میان انجام وظیفه یا وقوع خرابی سیستم‌های کاهشی مختلف و در نهایت رخدادهای خطرناک در پی وقوع رخداد آغازگر منفرد، به طریقی روشن فراهم می‌آورد. ETA در شناسایی رخدادهایی که نیازمند تحلیل بیشتر با استفاده از FTA می باشند بسیار مفید است (یعنی رخداد های بالایی از درخت های خرابی). برای آنکه بتوان ارزیابی جامع ریسک انجام داد، نیاز است تمامی رخدادهای آغازگر بالقوه شناسایی شوند. اگرچه همواره امکان از قلم افتادن برخی رخدادهای آغازگر مهم در این فن وجود دارد. به علاوه درخت رخداد فقط به دو نوع موفقیت و خرابی یک سیستم پرداخته می‌شود و گنجاندن موفقیت های تأخیری یا رخداد های بازیابی دشوار است.

می‌توان از ETA برای شناسایی خطرات و برآورد احتمال توالی رخدادهای منجر به شرایط خطرناک استفاده کرد.

رخداد آغازگر	شروع آتش	سیستم اطفاء حریق کار می‌کند	هشدار آتش فعال شده است	نتیجه	فراوانی (در هر سال)
انفجار ۱۰$^{-۲}$ در هر سال	بله ۰/۸	بله ۰/۹۹	بله ۰/۹۹۹	آتش کنترل شده با هشدار	۷/۹×۱۰$^{-۳}$
			بله ۰/۰۰۱	آتش کنترل شده بدون هشدار	۷/۹×۱۰$^{-۶}$
		خیر ۰/۰۱	بله ۰/۹۹۹	آتش کنترل نشده با هشدار	۸/۰×۱۰$^{-۵}$
			خیر ۰/۰۰۱	آتش کنترل نشده بدون هشدار	۸/۰×۱۰$^{-۸}$
	خیر ۰/۲			آتش وجود ندارد	۲/۰×۱۰$^{-۳}$

شکل الف-۳ نمونه‌ای از یک درخت رخداد برای انفجار غباری

الف-۵ تحلیل مقدماتی خطر (PHA) [1]

PHA روش تحلیل استقرایی است که هدف آن شناسایی خطرات، شرایط خطرناک و رخداد هایی است که می توانند منجر به آسیب به فعالیت معلوم، تسهیلات یا سیستم معلوم شوند. متداول‌ترین کاربرد آن در مراحل اولیه تکوین یک پروژه است زمانی که اطلاعات کمی دربارهٔ جزئیات طراحی و روش‌های اجرایی بهره‌برداری وجود دارد و اغلب می‌تواند مقدمه‌ای برای بررسی های بیشتر باشد. همچنین می‌تواند در تحلیل سیستم‌های موجود یا الویت‌بندی خطرات جایی که اوضاع و احوال استفاده از روش‌های گسترده‌تر را مانع می‌شود، مفید باشد.

PHA فهرستی از خطرات و شرایط خطرناک عام توسط ویژگی‌های مورد بررسی بیان می‌کند. مثل:

الف) مواد مورد استفاده یا تولید شده و واکنش پذیری آن‌ها

ب) تجهیزات مورد استفاده

پ)محیط بهره‌برداری

ت) چیدمان

ث) واسطهای بین اجزاء سیستم و غیره.

این روش با شناسایی احتمال وقوع حادثه، ارزشیابی کیفی وسعت آسیب ها یا زیان های احتمالی به سلامتی که می توانند حاصل شوند و شناسایی مقیاس های جبرانی ممکن، تکمیل می‌شود. PHA بایستی در فازهای طراحی، ساخت و آزمون برای آشکارسازی خطرات به روز شده و در صورت لزوم اصلاحات اجرا شود. نتایج بدست آمده می‌تواند به روش‌های مختلف مثل جداول و درخت ها نمایش داده شوند.

الف-۶ ارزیابی قابلیت اطمینان انسان (HRA) [2]

کلیات

ارزیابی قابلیت اطمینان انسان (HRA) به اثر اپراتورها و نگهدارندگان انسانی روی عملکرد سیستم پرداخته و می توانند برای ارزشیابی اثرات خطای انسانی روی ایمنی و بهره‌وری استفاده شوند.

بسیاری از فرآیندها حاوی استعداد خطای انسانی هستند به ویژه زمانی که زمان موجود برای اپراتور برای تصمیم گیری کوتاه است. احتمال این‌که مشکلاتی که به کفایت توسعه یابند، به مشکلات جدی تبدیل شوندمعمولاً کم است. اگرچه گاهی اوقات اقدام انسانی تنها دفاع برای جلوگیری از پیشرفت خرابی آغازگر به سمت حادثه است.

HRA انواع مختلف اقدامات حاوی خطا را که می توانند رخ دهند، شامل موارد ذیل، شناسایی می‌کند:

الف)خطای حذف، وقوع خرابی در اجرای اقدام لازم ؛

ب) خطای راه اندازی که می‌تواند شامل موارد ذیل باشد:

۱) وقوع خرابی در اجرای با کفایت یک عمل لازم؛

۲) اقدامی که با نیروی خیلی زیاد یا خیلی کم یا بدون درستی لازم انجام شود.

---

1 -Perliminay Hazard Analysis

2 -Human Reliability Assessment

۳) اقدام اجرا شده در زمان اشتباه

۴) اقدام (یا اقدامات) اجرا شده با توالی اشتباه

پ) اقدام نامربوط، اقدام غیرلازم به جای یا علاوه بر اقدام لازم.

HRA فرصت‌های بازیابی خطا یعنی اقداماتی که می توانند خطاهای قبلی را بازیابی کنند، را نیز شناسایی می‌کند.

HRA رشته‌ای مرکب با محققان و متخصصانی که عموماً از مهندسی قابلیت اطمینان یا روان‌شناسی و عوامل انسانی آمده اند، می‌باشد.

اهمیت HRA در حوادث گوناگون که خطاهای انسانی بحرانی موجب توالی رخدادهای فاجعه آمیز شده‌اند، شرح داده شده است. این حوادث هشداری علیه ارزیابی ریسک هایی اند که صرفاً به سخت‌افزار و نرم‌افزار سیستم متمرکز است. این حوادث، خطرات چشم پوشی از احتمال سهم خطای انسانی را نشان می‌دهد. به علاوه HRAها در برجسته کردن خطرات مانع برای بهره‌وری و روش‌های آشکارسازی این خطاها و وقوع خرابی‌های دیگر (سخت افزار یا نرم افزار) که می‌توانند توسط اپراتورهای انسانی یا کارکنان نگهدارنده بازیابی شوند، مفید ند.

HRA ممکن است شامل گام های ذیل باشد:

۱) تحلیل تکالیف

۲) شناسایی خطای انسانی

۳)کمی سازی قابلیت اطمینان انسانی

هر مرحله در ادامه توضیح داده و روش‌های تحلیل ذکر شده‌اند.

تحلیل تکالیف و شناسایی خطرات انسانی معمولاً بایستی در طول فاز مفهوم و تعریف یا در اوایل فاز طراحی و تکوین آغاز می‌شود و باید در مراحل بعدی سیستم روزآمد و تصحیح شود.

تحلیل تکالیف(TA) [1]

هدف TA در فرآیند HRA، توضیح و تعیین ویژگی‌های تکلیف مورد تحلیل با جزئیات کافی برای انجام شناسایی خطای انسانی و/یا کمی سازی قابلیت اطمینان انسانی است. تحلیل تکالیف را می‌توان برای مقصودهای دیگر از قبیل ارزشیابی واسط انسان ماشین یا طراحی روش اجرایی به کار برد.

شناسایی خطای انسانی (HEI) [2]

این گام اقدامات ممکن خطادار در اجرای یک تکلیف را شناسایی می‌کند و توضیح می دهد. شناسایی خطای انسانی می‌تواند شامل شناسایی عواقب احتمالی و علل اقدامات خطا و پیشنهاد مقیاس هایی برای کاهش احتمال خطای انسانی، بهبود فرصت‌های بازیابی و/یا کاهش عواقب اقدامات خطا باشد. نتایج HET، ورودی ارزشمندی برای مدیریت ریسک ارائه می دهد حتی اگر هیچ کمی‌سازی انجام نشده باشد.

1 -Task Analysis
2 -Human Error Identification

کمی سازی قابلیت اطمینان انسانی (HRQ) [1]

هدف HRQ برآورد احتمال عملکرد صحیح تکلیف یا احتمال اقدامات خطا است. برخی فنون HRA همچنین می توانند شامل گام‌هایی برای برآورد احتمال یا فراوانی توالی‌های رخداد نامطلوب مشخص شده یا خروجی‌های نامطلوب باشند.

جزئیات بیشتری درباره HRA در IEC 60300-3-8 ارائه شده است.

الف-۷ مدرک ارجاع

IEC 60300-3-8: Dependability management – part 3 : Application guide – Section 8: Human reliability

1-Human Reliability Quantification