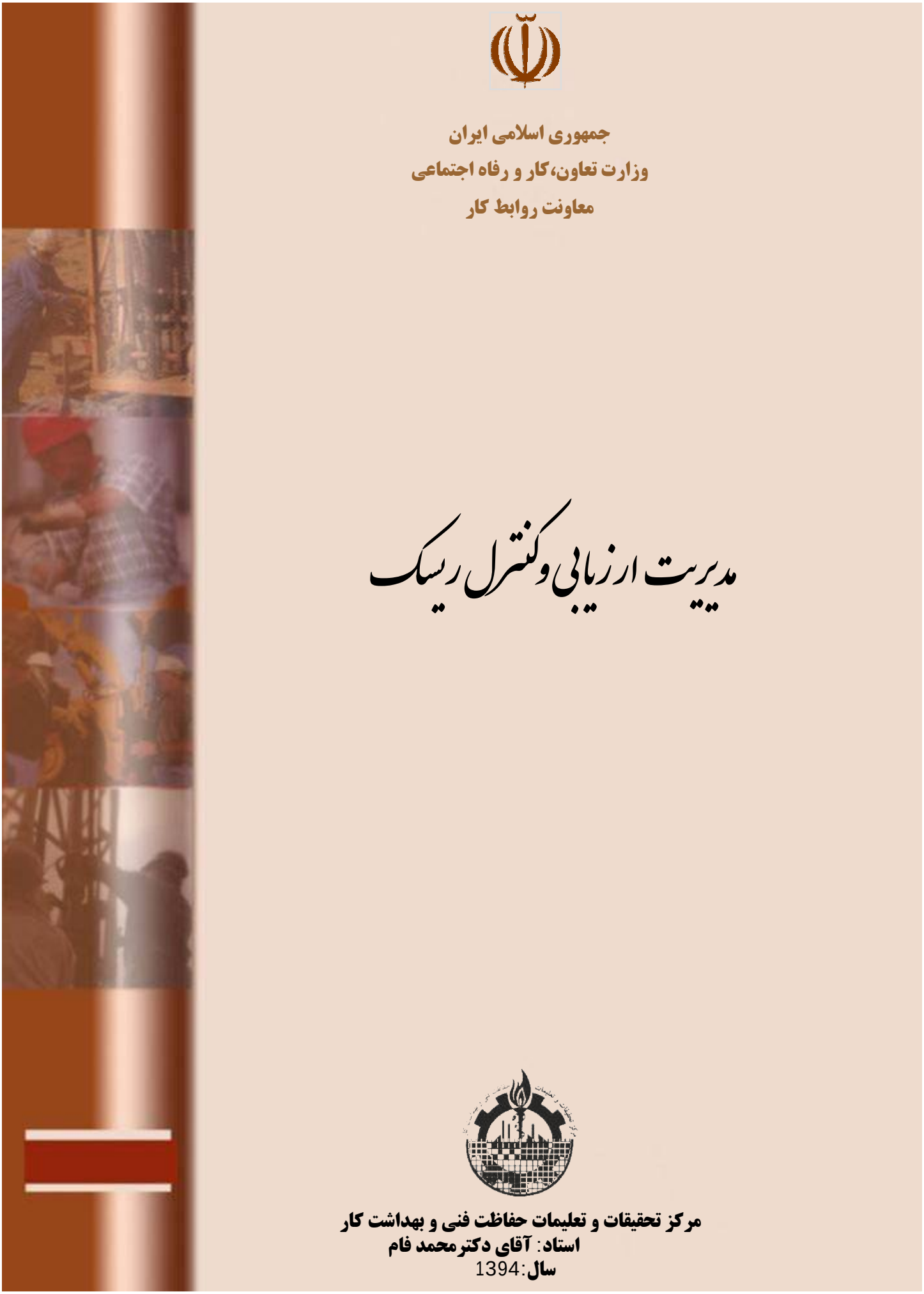


جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی
معاونت روابط کار

مدیریت ارزیابی و کنترل ریسک

مرکز تحقیقات و تعلیمات حفاظت فنی و بهداشت کار
استاد: آقای دکترمحمد فام
سال:1394

بنام خدا

ارزیابی و مدیریت ریسک

مؤلف: دکتر ایرج محمدفام

فهرست مطالب

مقدمه:

داشتن زندگی عاری از خطر آرزو و هدف همه مردم در همه اعصار بوده است زیرا میل به ایمنی و امنیت بخش تفکیک ناپذیری از ماهیت همه انسانها می باشد. از طرفی دیگر بشر همواره در تلاش برای بهبود زندگی و راحتی بیشتر بوده و در این راه سعی کرده است با ایجاد تغییر در طبیعت، متغیرهای آن را بخدمت خود درآورد که در این راه همراه با دستیابی به مواد، تجهیزات، دستگاهها و بعبارتی ساده تر بخدمت گرفتن فن آوری نوین و غیره با خطرات بیشتر و همچنین جدیدتری نیز مواجه گردیده است.

در گذشته برنامه های ایمنی معمولاً بر اساس یک فلسفه بعد از واقعه به بررسی وکنترل حوادث می پرداختند بدین معنی که مهندسی ایمنی بعد از وقوع یک حادثه وارد عمل شده و سعی می کرد که با انجام تحقیقات لازم علل بروز حادثه را مشخص و از نتایج حاصله بعنوان پایه ای برای پیشگیری از وقوع حوادث مشابه استفاده کند. این نوع فعالیتهای ایمنی منفعل دو عیب عمده داشت؛ اول اینکه بایستی حادثه ای رخ می داد تا مهندسی ایمنی بتواند وارد عمل شود که این امر باعث تحمیل هزینه های زیادی می شد و عیب دیگر آن ناتوانی در شناسایی حوادث قابل قبول و قابل پیشگیری بود، بعنوان مثال در طول جنگ جهانی اول حوادث منجر به سقوط هواپیماها که بدلیل نقص ساختاری یا نقص در موتور هواپیما بوقوع می پیوست غیر قابل پیشگیری تلقی می شدند.

با توسعه سیستم های حساس و پیچیده بویژه ساخت و انبار کلاهکهای اتمی این ایده قوت گرفت که برای بررسی وضعیت ایمنی سیستمها دیگر نمی توان به حوادث اجازه وقوع داد لذا سعی گردید که روشهایی برای آنالیز حوادث ابداع شود که بتوانند پتانسیل وقوع خطر را قبل از عملیات یک سیستم شناسایی کنند و نتیجه این تلاشها باعث شد که امروزه ایمنی سیستم بر اساس یک برنامه طرح ریزی شده، دارای نظم، سازماندهی شده و در قالب یک فرایند قبل از ـ واقعه در آید که بر پایه روش آنالیز ـ کنترل قرار دارد در فلسفه امروزی ایمنی سیستم تأکید بر روی سطح قابل قبول از ایمنی در فاز طراحی و قبل از تولید و ارزیابی خطرات سیستم قبل از تحمیل خسارات می باشد.

قلب ایمنی سیستم، آنالیز خطر است؛ یک فرایند مؤثر آنالیز خطر در طول عمر سیستم ستون و چهارچوبی خواهد بود که کل اجزاءِ بدنه برنامه ایمنی سیستم بر روی آن استوار خواهد شد. البته بایستی در نظر داشت که ایمنی سیستم تنها آنالیز نقص نیست زیرا خطر یک اصطلاح جامع تر از نقص است که شامل ریسک خسارات و جراحات نیز می شود،

لازم بذکر است که کاربرد درست ایمنی سیستم نیازمند بکارگیری دقیق روشهای مهندسی به همراه کنترلهای مدیریتی لازم جهت اطمینان از کاربرد دقیق و اقتصادی آنهاست لذا فعالیتهای ایمنی سیستم را می توان در دو دسته کلی فعالیتهای مهندسی و فعالیتهای مدیریتی تقسیم بندی کرد که در این جزوه ضمن تشریح فعالیتهای مهندسی ایمنی در قالب مدیریت ریسک تعدادی از تکنیکهای معمول مورد استفاده در آن نیز بتفصیل مورد بحث قرار خواهند گرفت.

ایرج محمدفام – تابستان ۱۳۸۶

فصل اول:
شناسایی خطر

اهداف آموزشی:

۱. آشنا ساختن شرکت کنندگان با مفاهیم و اصول پایه ای ایمنی

۲. تشریح تاریخچه ایمنی
۳. بیان فرایند ایمنی سیستم
٤. آشنا ساختن شرکت کنندگان با ریسک و نحوه محاسبه آن
۵. تشریح اولویتهای کنترلی در رویکرد ایمنی مدرن

مفاهیم:

به منظور درک صحیح ایمنی که در این جزوه از آن صحبت می شود در ابتدا مفاهیم و اصول اساسی ایمنی تعریف می شود:

ایمنی: در فرهنگ لغات اصطلاح ایمنی به معنی امنیت، آسایش، سلامتی و... آمده است و از نظر تعریف عبارتست از میزان یا درجه فرار از خطر. ایمنی کامل یعنی مصونیت در برابر هر نوع آسیب، جراحت و نابودی که با توجه به تغیرپذیری ذاتی انسان و غیرقابل پیش بینی بودن کامل اعمال و رفتار او و همچنین علل دیگر بنظر می رسد که هیچگاه ایمنی صددرصد حتی برای یک دوره کوتاه مدت نیز وجود نداشته باشد به همین علت کارشناسان امر معمولاٌ بجای کلمه ایمنی از اصطلاحاتی نظیر پیشرفت ایمنی، ارتقاءِایمنی و ایمن تر و غیره استفاده می کنند.

سیستم: عبارتست از مجموعه افراد، تجهیزات، قوانین، روشها و دستورالعملها که به منطور اجرای یک فعالیت معین در یک محیط خاص کنار یکدیگر قرار می گیرند.

خطر: به شرایطی اطلاق می شود که دارای پتانسیل رساندن آسیب و صدمه به کارکنان، خسارات به وسایل، تجهیزات، ساختمانها و از بین بردن مواد یا کاهش قدرت کارآئی در اجرای یک عمل از قبل تعیین شده باشد.

شدت خطر: عبارتست از یک توصیف طبقه بندی شده از سطح خطرات بر اساس پتانسیل واقعی یا مشاهده شده آنها در ایجاد جراحت، صدمه و یا آسیب.

احتمال خطر: عبارتست ازامکان بروز شرایط خاص در یک وضعیت معین یا محیط کاری.

حادثه: واقعه برنامه ریزی نشده و بعضاٌ صدمه آفرین یا خسارت رسان که انجام، پیشرفت یا ادامه طبیعی یک فعالیت یا کار را مختل می سازد و همواره در اثر یک عمل یا کار ناایمن یا شرایط ناایمن و یا ترکیبی از آن دو به وقوع می پیوندد.

حوادث به خیر گذشته یا شبه حادثه: رویدادهای هستند که هرچند می توانند باعث صدمه و یا جراحت شوند ولی به موارد فوق منجر نمی شوند.

ریسک: عبارتست از بزرگی خطر بر حسب احتمال وقوع و شدت آن.

شکست یا نقص: عدم توانایی یک جزء، وسیله یا سیستم در اجرای عملکرد مورد انتظار و یا انجام یک عمل یا فعل ناخواسته توسط آن را نقص یا شکست گویند به عنوان مثال بصدا در نیامدن زنگ اعلام آتش سوزی در موقع حریق و یا بصدا در آمدن آن در مواقع غیر ضروری هر دو نقص محسوب می شوند.

قابلیت اعتماد: عبارت از حد اطمینانی است که یک محصول یا سیستم می تواند کارکرد معین خود را تحت شرایط عملیاتی و محیطی از پیش تعریف شده برای یک مدت معین انجام دهد.

تاریخچه ایمنی:

سیر تحول علوم انسانی از عصر شکار به عصر انقلاب صنعتی هر چند که به بهره وری روزافزون انسان از منابع خدادادی منتهی شد ولی از بعد دیگر او را با معضلات جدیدتری نیز مواجه ساخت زیرا انسانها با روند رو به رشد خود برای تأمین نیازهای خود شروع به کشف و اختراع وسایل جدید و بکارگیری تکنولوژیهای جدیدتری نمودند که مجموع این تلاشها به افزایش سریع و روزافزون آنها در ایجاد و سرعت بخشیدن به تغییرات دلخواه انجامید ولی این پیشرفتها به همان نسبت اثرات مثبت، به تأثیرات منفی نیز منجر گردید. زیرا همین تغییرات خود، عوامل پیش بینی نشده ای را بدنبال داشتند که باعث بروز آسیب، صدمه و خسارات مختلف گردیدند. در جدول شماره ۱ نمونه ها از پیشرفتهای تکنولوژیکی به همراه پاره ای از پیامدهای منفی آنها ارائه شده است.

جدول شماره ۱: پیامدهای سوء ناشی از پیشرفتهای تکنولوژی

پیشرفت	پیامد منفی
آتش	سوختگی ها، آتش سوزیهای ویرانگر
ابزارهای برنده	بریدگیها و صدمات ناخواسته
سوختهای فسیلی	آلودگی هوا
سیستم حمل و نقل سریع	افزایش شدیدحوادث مرگبار
آفت کشها	مسمومیت زنجیره غذایی
نگهدارنده های غذا	مواد سرطانزا
انرژی هسته ای	پرتوهای یونساز

در سالیان اخیر اثرات سوءِ توسعه های تکنولوژیکی بحدی بحران آفرین شده است که حتی روند رو به رشد انسان در زمینه فن آوریهای نوین شدیداً زیر سوال رفته است بطوریکه امروزه این سوال بکرات از طرف اندیشمندان مطرح می شود که: "آیا ما قربانی فرایند توسعه نشده ایم".

آنالیز حوادث فاجعه بار دهه های اخیر نشانگر موارد زیر است:

۱. در بسیاری از مواقع پیامدهای بروز حوادث از چنان بعدی برخوردار می شوند که حتی امکان تصور جبران خسارت وارده به دارائیها وجود ندارد.

۲. ثابت شده است که یکی از عوامل اصلی مؤثر در افزایش بهره وری در کنار کاهش هزینه حوادث و بیماری توجه به سلامتی جسمانی و روانی افراد درگیر در سیستم از طریق معاینات بدو استخدام، دوره ای و کنترل عوامل زیان آور فیزیکی، شیمیایی، روانی و بیولوژیکی می باشد.

۳. حوادث یاد شده همواره در اثر ترکیبی از عوامل مختلف بوجود می آیند که نبود یک تفکر جامع نگر و غفلت از یک عامل می تواند کلیه تلاشهای انجام شده برای کنترل حوادث را بی اثر سازد.

با توجه به مطالب یاد شده و نظر به حرکت شتابان کشورمان در زمینه توسعه و صنعتی شدن در زمینه مقابله با حوادث صنعتی و کنترل پیامدهای مختلف آن منجمله خسارات اقتصادی، انسانی، اجتماعی، زیست محیطی و ... توجه به موارد زیر حائز اهمیت است:

۱. **استفاده از فلسفه پیشگیرنده در کنترل ریسک خطرات (ایمنی سیستم)**
۲. **بکار گیری رویکرد سیستمی**
۳. **انسان محوری**

فرایند ایمنی سیستم

اساس فرایند ایمنی سیستم عبارتست از کسب اطمینان از اینکه شغل یا وظیفه در ایمن ترین شکل خود و بدون وجود ریسک غیر قابل قبول از جراحات و صدمات انجام می گیرد. این فرایند آینده نگر در محیط های کاری یعنی جائیکه افراد، روشهای عملیاتی، تجهیزات، مواد و محیط بصورت فاکتورهای مکمل هم می توانند ایمنی و انجام موفقیت آمیز شغل یا وظیفه را تحت تأثیر قرار دهند انجام می گیرد. هرکدام از فاکتورهای فوق ممکن است در طول انجام وظیفه منشاءِ درجه ای از ریسک خطر برای افراد و تجهیزات باشد برای مثال در محیط های کاری،

افراد ممکن است برای خود و دیگران مخاطره آمیز باشند؛ بی توجهی، عدم دریافت آموزشهای مناسب، شوخیهای بیجا، خستگی، فشارهای روحی، استفاده غلط از مواد و ابزارها، مشکلات خصوصی(خانوادگی، مالی و...) جزءِعوامل انسانی هستند که می توانند در کارآیی مطلوب و مناسب افراد اثر سوءِ بگذارند. تجهیزات و وسابل نیز ممکن است حتی با وجود استفاده صحیح مخاطره آمیز باشند همچنین روشهای عملیاتی غلط یا نامناسب می تو اند برای جریان عملیات و انجام وظیفه خطر آفرین باشند. بنابراین با توجه به مطالب یاد شده لازم است که فرایند ایمنی سیستم در راستای تعیین انواع خطرات بالقوه ای که ممکن است در هر شغلی وجود داشته باشد به هرکدام از فاکتورهای چهار گانه یاد شده توجهات کافی را مبذول دارد.

ایمنی سیستم نیازمند شناسایی بموقع و ارزیابی پیامدهای خطرات مربوط به عملیات یاد شده قبل از بروز تلفات و ضایعات است بعنوان نمونه در مثال قبلی برای جابجایی ایمن مواد شیمیایی خطرناک لازم است که خطرات موجود قبل از تبدیل به حادثه شناسایی شده و در مرحله بعدی کاملاً حذف و یا تا حد رسیدن به سطح قابل قبولی از ریسک کنترل شوند، بعبارت دیگر روش پرواز ـ تکمیل ـ پرواز یا تکنیکهای بعد از وقوع در فرایند ایمنی سیستم جایگاهی نداشته و در مقابل مفهوم ایمنی سیستم برای کنترل خطرات نیازمند بکارگیری تکنیکهای قبل از وقوع می باشد.

معیارهای ایمنی سیستم

شدت خطر

شدت خطر نشاندهنده وسعت و دامنه خسارات و تلفاتی است که در صورت بالفعل در آمدن خطر ایجاد خواهد شد. طبقه بندی شدت خطر می تواند بر اساس تعداد طبقات، نامگذاری آنها، اهداف و منظور هر طبقه، اصول طبقه بندی و غیره متفاوت باشد

یکی از طبقه بندیهای شدت خطر در سال ۱۹۸٤ در استانداردهای نظامی آمریکا (88213 - MIL- STD) ارائه شده که در آن خطرات از نظر شدت به چهار گروه فاجعه بار، بحرانی، مرزی و جزئی طبقه بندی شده اند. هر چند که استاندارد اخیر در ابتدا برای ارزیابی سیستمهای نظامی ارائه شده بود ولی امروزه از آن برای طیف وسیعی از صنایع که اصول ایمنی سیستم در آنها بکارگرفته می شود نیز استفاده می گردد. سیستم یاد شده که در جدول شماره ۲ نشان داده شده است یک معیار کیفی از شدت نسبی پیامدهای احتمالی شرایط مخاطره آمیز ارائه می کند.

بکارگیری تکنیک طبقه بندی شدت، در ارزیابی شرایط ایمنی سیستم از اهمیت بسزایی برخوردار است زیرا با اختصاص طبقات مختلف سیستم و شکستهای احتمالی می توان شرایط موجود را بهتر ارزیابی کرده و در نتیجه اقدامات کنترلی را اولویت بندی نمود.

جدول شماره ۲: طبقه بندی شدت حادثه

نوع خطر	طبقه	تعریف
فاجعه بار	۱	مرگ و میر یا از بین رفتن سیستم
بحرانی	۲	جراحات، بیماریهای شغلی یا آسیبهای وارده به سیستم شدید است.
مرزی	۳	جراحات، بیماریهای شغلی یا آسیبهای وارده به سیستم کوچک است.
جزئی	٤	جراحات، بیماریهای شغلی یا آسیبهای وارده به سیستم خیلی کوچک است.

لازم به یادآوری است که علاوه بر تعداد طبقات و نام آنها، تعاریف هر طبقه نیز ممکن است در کشورها، ایالات و حتی در صنایع مختلف یک کشور بسیار متفاوت از هم باشد که این امر به سیاستهای ایمنی هر کشور، ایالت و یا صنعت بستگی خواهد داشت بعنوان مثال ممکن است در کشور یا صنعتی تحمیل N دلار خسارت یک حادثه فاجعه بار تلقی شود در حالیکه حادثه یاد شده در کشور یا صنعت دیگر از نوع بحرانی قلمداد شود.

احتمال خطر

فاکتور احتمال خطر نشاندهنده امکان بالفعل در آمدن یک خطر در یک دوره زمانی معین است. طبقه بندی خطرات بر اساس احتمال وقوع نیز ممکن بسیار متعدد باشد، طبقه بندی ارائه شده در جدول شماره ۳ نشانگر یک تقسیم بندی کیفی از احتمال نسبی وقوع یک حادثه در اثر خطرات کنترل نشده است (MIL-STD - 882 B)، همچنین با استفاده از این جدول می توان براساس میزان احتمال وقوع حوادث به اهمیت آنها پی برد لازم به ذکر است که در طبقه بندیهای مشابه می توان احتمال وقوع حوادث را به شکل کمّی نیز تعریف کرد بعنوان مثال حوادثی را از نوع مکرر نامید که حداقل یکبار در هر هفته یا ماه و غیره بر حسب ماهیت سیستم رخ می دهند.

جدول شماره ۳: سطح احتمال وقوع خطر

احتمال وقوع	سطح خطر	توصیف خطر
مکرر($x > 10^{-1}$)	A	بطور مکرر اتفاق می افتد
محتمل ($10^{-1} > x > 10^{-2}$)	B	در طول عمر یک سیستم چندین بار رخ می دهد
گاه به گاه ($10^{-2} > x > 10^{-3}$)	C	گاهگاهی در طول عمر سیستم رخ می دهد
خیلی کم ($10^{-3} > x > 10^{-4}$)	D	احتمال وقوع آن در طول عمر سیستم خیلی کم است
غیر محتمل ($x > 10^{-4}$)	E	احتمال وقوع آن در طول عمر سیستم آنقدر پائین است که می توان آن را در حد صفر فرض کرد

ماتریکس ریسک خطر

جدول شماره ٤ یک نمونه از ماتریس ریسک خطر را نشان می دهد که برای فراهم کردن یک ابزار مؤثر جهت تخمین سطح قابل قبول درجه ریسک، عناصر جداول شدت و احتمال خطر را در هم ادغام کرده است. با ایجاد یک سیستم سنجش دو کاراکتری برای وقوع ریسک بر حسب شدت و احتمال خطر می توان ریسک را بر اساس درجه مقبولیت طبقه بندی وارزیابی کرد.

جدول شماره ٤: ماتریس ارزیابی ریسک

شدت خطر / احتمال وقوع	فاجعه بار(1)	بحرانی(2)	مرزی(3)	جزئی(4)
مکرر(A)	1A	2A	3A	4A
محتمل(B)	1B	2B	3B	4B
گاه به گاه(C)	1C	2C	3C	4C
خیلی کم(D)	1D	2D	3D	4D
غیر محتمل(E)	1E	2E	3E	4E

جدول شماره ٥: معیارهای تصمیم گیری بر اساس شاخص ریسک

معیار ریسک	طبقه بندی ریسک
غیر قابل قبول	1A , 1B , 1C , 2A , 2B , 3A
نامطلوب	1D , 2C , 2D , 3B , 3C
قابل قبول ولی با نیاز به تجدید نظر	1E , 2E , 3D , 3E , 4A , 4B
قابل قبول بدون نیاز به تجدید نظر	4C , 4D , 4E

اولویتها در ایمنی سیستم

استفاده از روش اولویت بندی برای برطرف کردن ضروتهای ایمنی سیستم و کنترل خطرات شناخته شده بی شباهت به کاربرد آن برای سایر مسایل ایمنی صنعتی نیست. اولویتها در ایمنی سیستم شامل پنج مرحله به شرح زیر است:

۱. طراحی ایمن (بطوریکه ریسکها به حداقل ممکن تقلیل یابند)
۲. تعبیه تدابیر ایمنی
۳. فراهم کردن وسایل هشدار دهنده
٤. گسترش و بهبود دستورالعملهای عملیاتی و آموزشها
۵. پذیرش ریسک

بررسی کمّی ریسک

در همه بحث های مدیریت ریسک و بررسی آن لازم است که پارامترهای پذیرش کمّی ریسک مورد توجه قرار گیرد. بر اساس نظریات ریچارد. ای. اولسون در سیستمهای با ریسک بالا تمایل زیادی به اعتماد پذیری کامل به احتمالات آماری وجود دارد زیرا بنظر می رسد که استفاده از عدد یک راه آسان برای اندازه گیری ایمنی و احتمال بروز نقص یا حادثه باشد ولی لازم است قبل از تلاش برای چنین اندازه گیریهایی، محدویتها و اصول اساسی چنین روشها به همراه تجربیات قبلی مهندسی بخوبی شناخته شده و پارامترهای کمّی پذیرش بطور کامل تعریف شده و قابل پیش بینی، اثبات پذیر و مهمتر از همه مفید باشد بدین معنی که براحتی قابل تبدیل به معیارهای طراحی باشند. از طرف دیگر این امکان وجود دارد که تجزیه و تحلیل گر ایمنی سیستم و مدیریت آن آنقدر به روشهای آماری علاقمند شوندکه شیوه های بسیار راحت و مهم دیگر برای بیان مسئله را فراموش کنند.

همانطوریکه اشاره شد در طراحی بسیاری از سیستمهای با ریسک بالا نظیر صنایع هسته ای، صنایع پیشرفته نظامی، و غیره اغلب تمایل زیادی وجود دارد که برای ارزیابی خطر تنها به تجزیه و تحلیل آماری بسنده شود زیرا بر اساس نتایج آماری (حتی اگر کاملاً واقعی هم نباشند) می

توان وضعیت ایمنی را راحت تر تفسیر کرد هرچند که ممکن است ناآگاهانه با تعیین غلط حدود مدلّل برای مقبولیت احتمال ریسک دچار اشتباه شد برای نمونه به مثال زیر توجه کنید:

فرض کنید در یک برنامه ای با ریسک بالا ریسکهای با احتمال وقوع $۱۰^{-۴۲}$ و کمتر قابل قبول باشد برای نشان دادن غیرعملی بودن این حد، سطح ریسک بر اساس یک مثال با استفاده از اسکناسهای یکصد ریالی مورد بررسی قرار می گیرد؛ اگر ضخامت یک اسکناس یکصد ریالی سه هزارم اینچ باشد احتمال انتخاب یک اسکناس یکصد ریالی از یک بسته با ضخامت سه اینچ یا یکصد هزار ریال برابر ۱×۱۰^{-۳} خواهد بود ضخامت یکصد میلیون ریال اسکناس یک صد ریالی برابر ۲۵۰فوت می باشد و شانس انتخاب همان اسکناس از میان این توده برابر ۱×۱۰^{-۶} یا یک در میلیون خواهد بود. شانس انتخاب یک در تریلیون (۱×۱۰^{-۱۲}) توده ای از اسکناس یکصد ریالی به ارتفاع ۴۷۰۰ مایل ایجاد خواهد کرد واگر احتمال این مثال برابر ۱×۱۰^{-۴۲} با شد طول اسکناس یکصد ریالی شاید در مجموعه راه شیری نیز نگنجد و رویدادی با احتمال وقوع ۱×۱۰^{-۴۲} شاید در طول حیات جهان یکبار نیز رخ ندهد لذا لازم است که اهداف ایمنی به شکلی واقعی و قابل دسترسی تعیین شوند بطوریکه مدیریت قادر باشد براساس داده های قابل فهم تصمیمات درست و عاقلانه اتخاذ نماید.

اصول مدیریت

بر اساس نظریات Olson، مدیریت ریسک شامل دوازده اصل کلی پذیرفته شده است که عبارتند از:

۱. کلیه فعالیتهای انسانی که در آنها از وسایل و تجهیزات فنی استفاده می شود مستلزم حدودی از عناصر ریسک است.
۲. از هر خطر شناسایی شده نباید هراسید زیرا همه خطرات قابل کنترل هستند.
۳. باید به مشکلات با دیدی صحیح و مناسب نگریست.
٤. ریسکها باید طبقه بندی شده و ارزیابی آنها بر اساس دانش، تجارب و همچنین نیازهای کارخانه باشد.
۵. کلیه مقررات و اصول موجود در کارخانه و عناصر سازمانی آن بایستی طوری طرح ریزی شوند که از یک فلسفه واحد تبعیت کنند.
۶. عملیات سیستم همواره با درجه ای از ریسک همراه است، یک تجزیه و تحلیل خوب بر ضرورت کاهش وقوع حوادث تأکید خواهد کرد.

۷. آنالیز ایمنی سیستم و ارزیابی ریسک مغایرتی با کنترلهای مناسب و صحیح فنی و مهندسی ندارد.

۸. تعیین دقیق اهداف و پارامترهای بررسی ریسک بسیار مهمتر از یافتن روشهای استاندارد شده معمول برای حل مشکلات است.

۹. برای برطرف کردن مشکلات و مسایل ایمنی فقط یک ٌ بهترین راه حلٌ وجود ندارد و تعداد متنوعی از روشها موجود هستند که اجرای هرکدام از آنها ممکن است درجه ای از ریسک را کاهش دهد.

۱۰. برای اطلاع و استفاده از انواع متدهای دستیابی به اهداف خاص ایمنی بهترین و مؤثرترین راه مشاوره با یک طراح است.

۱۱. در عمل رسیدن به ایمنی کامل امکانپذیر نیست.

12. در برنامه ریزی و طراحی سیستم هیچ ٌ مشکل ایمنیٌ وجود ندارد و تنها مشکلات مهندسی و مدیریتی هستند که در صورت حل نشدن می توانند منجر به بروز حادثه شوند.

تعهدات مدیریت

ایمنی سیستم بدون تعهدات کامل و اصولی مدیریت و همچنین بدون وجود اطمینان و اعتماد دو طرفه بین مدیریت کارخانه و مدیریت ایمنی سیستم قابل دسترسی نخواهد بود بدین شکل که از یک طرف بایستی مدیران رده بالا مطمئن باشند که مسایل ایمنی توسط افراد مطلع، وارد و آگاه انجام می شود و از طرف دیگر مدیر ایمنی سیستم نیز باید از حمایت کامل مدیریت کارخانه خاطر جمع باشد همچنین لازم است که شاغلین محیهای کاری نیز بخوبی از وظایف کادر ایمنی و همچنین حمایتهای مدیریت کارخانه از واحد یاد شده در راستای اجرای وظایف محوله آگاه باشند. بعلاوه وجود نهادی که در نهایت حد قابل قبول بودن ریسک، عناصر سازمانی درگیر، خروجیهای مورد نیاز و اقدامات لازم بر روی خروجیها را تعیین نماید الزامی خواهد بود.

بر طبق پیشنهاد اولسون برای مدیریت مؤثر ریسک لازم است که مدیریت سازمان:

۱- بخواهد که کلیه شاغلین و همچنین سازمانهای پیمانکار در مدیریت برنامه ایمنی سیستم همکاری کنند.

۲- مطمئن شود که ساختار سازمانی مدیریت ایمنی سیستم طوریست که آنها از قدرت و انعطاف پذیری سازمانی برای کارآیی مؤثر برخوردار هستند.

۳- مطمئن شود که ریسکهای قابل قبول و غیر قابل قبول بر اساس سیاستهای شرکت بخوبی تعریف شده و مستند سازی گردیده اند بطوریکه تصمیم گیرندگان از ریسکهای موجود در هنگام کار سیستم آگاهند.

٤- بررسی ریسک حادثه را بعنوان بخشی از هر برنامه ارزیابی یا تجدید نظر و همچنین مرحله ای از تمامی مراحل مهم تصمیم گیری الزامی سازد.

بدون کسب اطمینانهای فوق بعنوان حداقل تعهد مدیریت سازمانی تلاشهای ایمنی موفقیت آمیز نخواهد بود همچنین لازم است که مدیریت علاوه بر تأمین منابع مورد نیاز و تعهدات لازم برای رسیدن به اهداف ایمنی سیستم، آماده قبول نتایج فرایند ایمنی سیستم نیز باشد و اطمینان حاصل کند که تصمیمات متخذه بر اساس کلیه اطلاعات موجود صورت می گیرد.

پرسش های پایان فصل:

۱. حوادث به خیر گذشته یا شبه حوادث را تعریف و در باره ضرورت آنالیز آنها بحث کنید.
۲. برای محاسبه شدت و احتمال ریسک چگونه عمل می کنید.
۳. اولویتهای کنترلی در رویکرد ایمنی مدرن را نام ببرید.
٤. بر روی اصول مدیریت ریسک بر اساس نظریه اولسون بحث کنید.

فصل دوم:
روشهای آنالیز خطرات

اهداف آموزشی:

۱. آشنا ساختن شرکت کنندگان با اهمیت ارزیابی ایمنی در چرخه عمر سیستم
۲. تشریح توانمندیهای تکنیک What if Analysis در آنالیز ایمنی سیستم ها
۳. تشریح توانمندیهای تکنیک FMEA در آنالیز ایمنی سیستم ها
٤. تشریح توانمندیهای تکنیکFTA در آنالیز ایمنی سیستم ها
۵. تشریح توانمندیهای تکنیکHAZOP در آنالیز ایمنی سیستم ها
۶. تشریح توانمندیهای تکنیک OSHA در آنالیز ایمنی سیستم ها

روند توسعه سریع فن آوریهای مدرن که با بکارگیری انرژیهای نوین همراه بوده است باعث گردیده که در کنار افزایش قدرت، سرعت و دقت، نسل بشر با معضلات جدیدتری نیز مواجه گردد. یکی از مهمترین مشکلات فراروی بشر در دنیای امروزی عدم مطابقت های احتمالی در فرایند تولید محصولات جدید و یا ارائه خدمات نوین است که می تواند محصول تولیدی را از حیث انتفاع خارج و حتی آن را به عامل تخریبی شدیدی تبدیل کند، فرایند تولید را مختل سازد، به تلفات انسانی منتهی گردد، باعث آلودگی محیط زیست شود و.... بدیهی است با توجه به کیفیت و کمیت انرژیهای نهان و بکارگرفته شده در سیستم ها و محصولات تولیدی وجود یک عیب و یا نقص جزئی می تواند به پیامدی فاجعه بار منتهی شود.

با توجه به مطالب یاد شده و به منظور مقابله با مشکلات فوق، علم ایمنی در طول تاریخ شکل گیری خود مراحل مختلفی را طی کرده است. این علم با توجه به تعریف خود یعنی علم حفاظت از دارائیها از بدو تاریخ همواره همراه با انسان بوده است. هر چند که برای سده های طولانی بدلیل پائین بودن ماهیت تهدید کنندگی خطرات موجود بصورت پاسیو و منفعل عمل کرده است. با معرفی انرژیهای جدید و گسترش سریع فن آوریهای مدرن و پیچیده و از آنجائیکه پیامدهای حوادث بطور روزافزونی بزرگتر گردید علم ایمنی در یک تغییر رویکرد آشکار از حالت منفعل به حالتی اکتیو و پیشگیرنده تبدیل و بعنوان علم ایمنی سیستم مطرح

گردیده است. بدیهی است از آنجائیکه تحت هیچ شرایطی امکان به صفر رساندن حوادث در هیچ زمان و محیطی عملی نیست در ایمنی سیستمی تحقیقات حادثه که بر پایه علم ایمنی کلاسیک قرار دارد نیز از جایگاه خاص خود برخوردار بوده است.

در فلسفه امروزی، ایمنی سیستم با رویکردی پیشگیرنده و در قالبی سیستماتیک مورد توجه قرار گرفته و سعی می شود که با استفاده از ابزارهای مختلف کلیه عدم مطابقت ها قبل از بالفعل در آمدن شناسایی و کنترل گردد. با این مقدمه علم ایمنی سیستم بشکل زیر تعریف می گردد:

ایمنی سیستم عبارت است از بکار گیری مهارتهای مهندسی و مدیریتی ویژه در قالبی سیستماتیک و آینده نگر به منظور شناسایی و کنترل خطرات موجود در طول عمر یک پروژه، برنامه یا فعالیت.

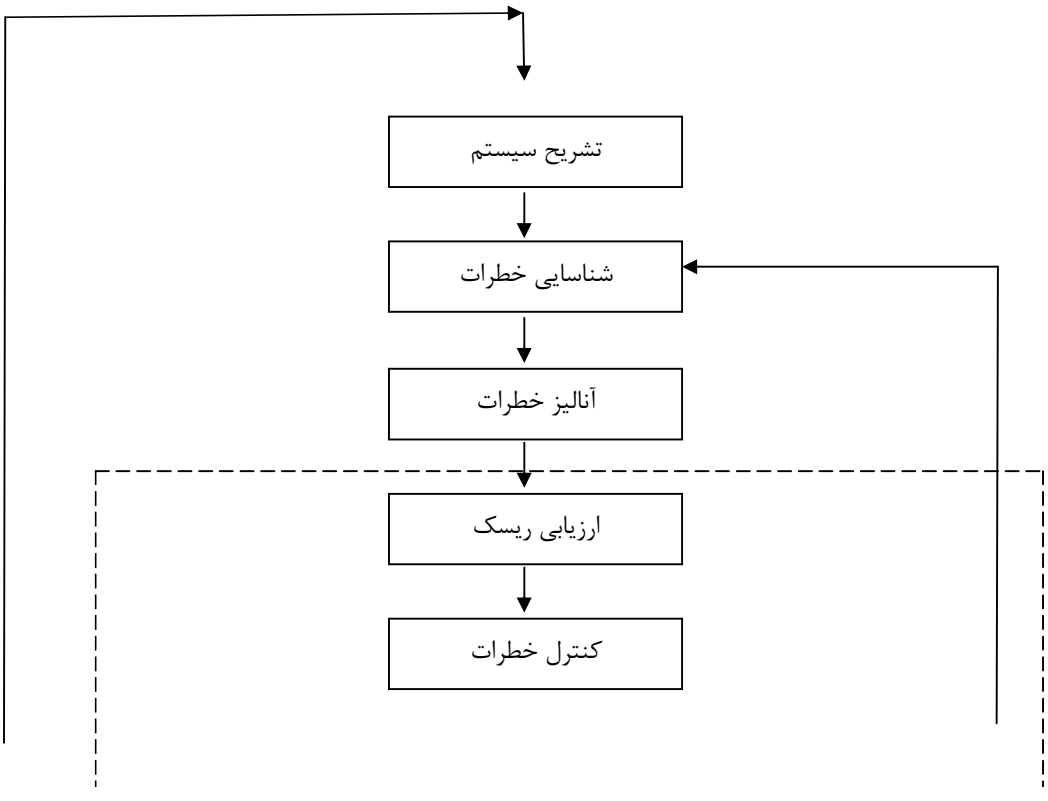
همانگونه که از تعریف فوق بر می آید ایمنی سیستم دارای مشخصه های زیر است:

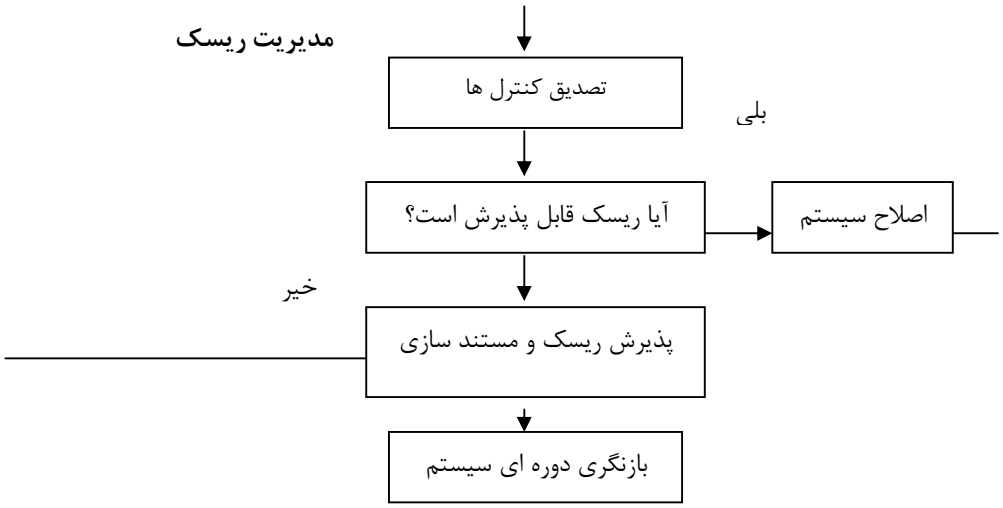
۱.استفاده از علم ایمنی سیستم نیازمند کسب مهارت در تکنیکهای مختلف مهندسی و مدیریتی است.

۲.نگاه فلسفه ایمنی سیستم یک نگاه جامع و همه جانبه نگر است.

۳.علم ایمنی سیستم بر اساس یک فلسفه پیشگیرنده بنا نهاده شده است.

٤.در علم ایمنی سیستم تاکید بر بکارگیری اصول علمی کنترل خطر در طول چرخه عمر سیستم از مرحله قبل از تولد آن تا پس از مرگ سیستم است.





شکل شماره ۳: فرایند آنالیز ایمنی سیستم

در فلسفه امروزی ایمنی سیستم تأکید بر روی سطح قابل قبول ایمنی در فازهای اولیه عمر سیستم یعنی فازهای ایده و تفکر، طراحی و قبل از تولید یا عملیات واقعی محصول یا سیستم و ارزیابی خطرات سیستم قبل از تحمیل خسارات می باشد. برای اینکه سیستم بطور ایمن مراحل ساخت، آزمایش، عملیات و نگهداری را طی کند لازم است که خطرات موجود در آن حذف شده یا تا رسیدن به سطح قابل قبول کنترل شوند در این حالت لازم است که فعالیتهای تصحیحی نیز از قبل مشخص شده باشند. کاربرد درست ایمنی سیستم نیازمند بکارگیری دقیق روشهای مهندسی به همراه کنترلهای مدیریتی لازم جهت اطمینان از کاربرد دقیق و اقتصادی آن است. با توجه به مطالب یاد شده مهندسی ایمنی سیستم یک بخش حیاتی از فرایند طراحی، راهبری و نگهداری است که بایستی بر روی سیستم یا محصول اجرا گردد.

لازم بذکر است که در میان فازهای مختلف عمر سیستم فاز طراحی از دیدگاه فلسفه ایمنی سیستم بسیار حیاتی است. در این فاز هر چند که بدلیل کمبود داده های لازم، یافته های حاصل نیز در حد کیفی خواهند بود ولی انجام ارزیابیهای ایمنی در این مراحل از چند بعد زیر حائز اهمیت است:

- یک ارزیابی منطقی از نقاط ضعف سیستم را در زمان مناسب فراهم می آورد.

- یک روش ارزیابی ایمنی اکتیو و پیشگیرانه را در مقابل روشهای پاسیو ارائه می نماید
- اطلاعات لازم برای تصمیم‌گیری در مورد تخصیص منابع و او لویت‌بندی فعالیتها جهت پائین آوردن ریسک تا حدود قابل قبول را در اختیار مدیریت قرار می‌دهد.
- یک تشریح و بازنگری نسبتاً سریع از مهمترین ریسکهای مربوط به سیستم فراهم می‌کند.
- هزینه های اجرای مطالعات در این مراحل بسیار پائین می باشد.
- بکارگیری اقدامات اصلاحی پیشنهادی بسیار مقرون بصرفه بوده و به همین دلیل براحتی مورد پذیرش مدیریت قرار می گیرد.

با توجه به مطالب فوق مشخص می شود که از دیدگاه ایمنی سیستم اولین و در عین حال اساسی ترین فاز در تولید و نگهداری یک محصول ایمن، فاز ایده و تفکر است که یافته های حاصل از این مرحله خود پایه ای برای ادامه ارزیابیهای سیستماتیک ایمنی در فازهای بعدی عمر سیستم/ پروژه/ محصول و غیره خواهد بود.

با توجه به اهمیت بکارگیری و پیاده سازی اصول ایمنی سیستم، در فصول بعدی تعدادی از تکنیکهای مورد استفاده در آن مرور خواهد شد.

تکنیکهای مورد استفاده در ایمنی سیستم

برای آنالیز ایمنی سیستم ها تکنیک های بسیار زیادی معرفی شده است که هر کدام از نقاط قوت و ضعف خاص خود برخوردار می باشند. تکنیکهای موجود که تعداد آنها از عدد ۱۰۰ تجاوز می کند را می توان از دیدگاههای مختلف طبقه بندی کرد. برای مثال تعدادی از این تکنیکها کاربرد مدیریتی و تعدادی دیگر کاربرد مهندسی دارند هر چند که در اغلب آنها سیستم مورد مطالعه از هر دو دیدگاه یاد شده ارزیابی می گردد. هم چنین تکنیکها را می توان از نظر تناسب آنها از نظر چرخه عمر سیستم نیز تقسیم بندی کرد. برای مثال در حالیکه روشهای نظیر لیست مقدماتی خطر (PHL) یا آنالیز مقدماتی خطر (PHA) ابزاری مناسب برای ارزیابی سیستم در فازهای اولیه محسوب می شوند بکارگیری تکنیک آنالیز علل معمول (CCA) بدلیل نیاز به اطلاعات جامع جهت تکمیل آن در فازهای ابتدائی قابل توصیه نخواهد بود. علاوه بر این انواعی از تکنیکها از ماهیتی استقرائی و تعدادی دیگر از نوع قیاسی می باشند. برای مثال روش آنالیز درخت رویداد (ETA) برای آنالیز از ساختار کل به جزءِ استفاده می کند در صورتیکه این ساختار در روش حالات شکست و آنالیز اثرات (FM&EA) از نوع جزءِ به کل است. علاوه بر این روشهای نظیر آنالیز درخت خطا (FTA)امکان کمی سازی نتایج را فراهم می سازد ولی تکنیکهای نظیر آنالیز خطرات خطا (FHA) از توانمندیهای یاد شده برخوردار نمی باشد. از تفاوتهای دیگر روشهای مورد بحث می توان به تناسب آنها با توجه به سیستم مورد مطالعه اشاره کرد. برای

نمونه روش آنالیز جریان پنهان (SCA) یک متد اختصاصی برای سیستم های الکترونیکی بوده ولی در روش خطرات عملیات و پشتیبانی (O&SHA) تاکید اصلی بر روی انسان و تعامل او با سیستم است. همانگونه که ملاحظه شد برای آنالیز ایمنی سیستم می توان از تکنیکهای مختلفی استفاده کرد که انتخاب اشتباه روش با توجه به فاز عملیاتی، ماموریت سیستم، ماهیت کار، اهداف مطالعه و... علاوه بر اینکه قادر نخواهد بود اطلاعات مفیدی ارائه کند می تواند با دادن اطلاعات غلط و یا ناقص به گمراهی محقق بیانجامد.

از مهمترین روشهای آنالیز می توان به موارد زیر اشاره کرد که تعدادی از آنها به اختصار تشریح می شود:

1. Cause-Consequence Analysis(CCA)
2. Change Analysis(CA)
3. Chemical Process Quantitative Risk Analysis (CPQRA)
4. Common Cause Analysis(CCA)
5. Energy Trace and Barrier Analysis (ETBA)
6. Event Tree Analysis (ETA)
7. Failure Modes And Effects Analysis (FMEA)
8. Failure Modes, Effects, and Criticality Analysis (FMECA)
9. Fault Hazard Analysis(FHA)
10. Fault Tree Analysis (FTA)
11. Hazard and Operability Study (HAZOP)
12. Health Hazard Assessment (HHA)
13. Human Error Analysis(HFA)
14. Human Reliability Analysis (HRA)
15. Job Safety Analysis(JSA)
16. Management Oversight and Risk Tree (MORT)
17. Operating and Support Hazard Analysis (OSHA)
18. Preliminary Hazard Analysis (PHA)
19. Preliminary Hazard List(PHL)
20. Probabilistic Risk Assessment (PRA)l
21. Root Cause Analysis(RCA)
22. Software Failure Modes and Effects Analysis (SFMEA)
23. Technique for Human Error Prediction (THERP)
24. What-If Analysis

تجزیه و تحلیل ٌ چه می شود اگر[1]؟

در ایمنی فرایند روش ٌ What If Analysis? ٌ و استفاده از چک لیستهای ایمنی دو ابزار جداگانه تلقی می شوند اما درحال حاضر این دو روش بصورت مکمل هم مورد استفاده قرار می گیرند البته این امر به این معنی نیست که از روشهای یاد شده نتوان بطور مجزا استفاده کرد زیرا هر دو روش بعنوان ابزارهای تجزیه و تحلیل ایمنی پذیرفته شده اند که در این بخش تنها روش ٌ What If Analysis? ٌ تشریح خواهد شد.

1 - W hat If Analysis?

نام واقعی روش" چه می شود اگر؟" از عبارت" اگر این امر رخ دهد پیامدهای آن چه خواهد شد" مشتق شده و هدف اصلی از اجرای آن، اعمال توجه و تمرکز به اثرات رویدادهای ناخواسته بر روی سیستم می باشد. اساس این روش آنالیز طرح سوالاتی که با عبارت ساده" چه می شود اگر... ؟" و یافتن پاسخهای واقعی و دقیق آنها قرار دارد. درصورتیکه تکنیک توسط افراد با تجربه و دارای دانش کافی از سیستم اجرا شود می تواند یک ابزار بسیار مفید در تجزیه و تحلیل ایمنی سیستمها باشد.

این تکنیک همانند روش HAZOP برای ارزیابی انحرافات احتمالی فرایند از حدود استاندارد طراحی شده و لذا همان اطلاعاتی که برای اجرای HAZOP مورد نیاز می باشند برای اجرای این تکنیک نیز ضروری خواهد بود. روند اجرای روش" What If Analysis?" به شکل زیر است:

الف) تعیین حیطه مطالعه و تعریف اهداف اصلی

ب) انتخاب تیم عملیاتی

ج) اجرای مطالعه با طرح سوالات" چه می شود اگر... ؟" و یافتن پاسخهای مناسب

د) مستند سازی نتایج

و) پیگیری فعالیتهای انجام شده در راستای کنترل خطرات شناسایی شده

قبل از اجرای روش" What If Analysis?" ، بر اساس اهداف مطالعه سطوح مختلف کارکردی تعریف شده و بعبارت دیگر برای تمرکز بیشتر و بهتر، سیستم به بخشهای کوچکتری تقسیم می شود و سپس مجموعه سوالات برای هر سطح کارکردی مطرح می گردد. برای شناسایی راحتتر خطرات موجود در سیستم می توان از چک لیستهای ایمنی مختلفی نیز استفاده کرد. همچنین از این چک لیستها می توان بعنوان پایه ای برای برای طرح سوالات" What If Analysis?" نیز سود برد. برای تسریع کار لازم است همزمان با طرح سوالات و یافتن جوابهای آنها نتایج بدست آمده نیز مستند سازی شوند.

بعضی از سوالاتی که ممکن است در جریان مطالعه" What If Analysis?" مطرح شوند عبارتند از:

الف) **چه** اتفاقی خواهد افتاد **اگر** عملیات اختلاط بطور کامل صورت نپذیرد ؟

ب) **چه** اتفاقی رخ می دهد **اگر** دمای عملیات از دمای محیط تجاوز کند ؟

ج) **چه** اتفاقی خواهد افتاد **اگر** پمپ A از کار بیافتد ؟

د) اپراتور از **چه** دستورالعملی استفاده خواهد کرد **اگر** فشار بیش از حد باشد ؟

حالت شکست و تجزیه و تحلیل اثرات آن(FM&EA)

FM&EA[۲] که امروزه یکی از آشناترین تکنیکهای تجزیه وتحلیل ایمنی سیستم هاست برای اولین بار در اواخر دهه ۱۹۵۰ میلادی بوسیله مهندسین قابلیت اعتماد جهت ارزیابی ایمنی سیستمهای نظامی پایه گذاری و بعد از آن استفاده از این روش بسرعت گسترش یافت بطوریکه در ایالات متحده آمریکا و فرانسه از آن بترتیب برای ارزیابی ایمنی هواپیماهای کنکورد و ایرباس استفاده شد. بدنبال حادثه تری مایل آیلند، کاربرد این تکنیک به ارزیابی ایمنی صنایع هســـته ای نیز توسعه یافت. این تکنیک که اساساً یک تجزیه و تحلیل کیفی است سیستم یا زیر سیستمها را برای شناسایی نقصهای احتمالی کلیه اجزای آن را بررسی کرده و تلاش می کند که اثرات نقصهای احتمالی را بر روی سایر بخشهای سیستم ارزیابی کند. اگرچه لازم است FM&EA در مراحل اولیه عمر محصول بالاخص در فاز طراحی و بر اساس داده های دقیق موجود انجام شود ولی در صورت نیاز، تجزیه و تحلیل گر ایمنی سیستم می تواند از این ابزار برای شناسایی و ارزیابی نقصهای اجزاءِ در سراسر عمر محصول یا سیستم استفاده کند.

اجرای FM&EA

FM&EA یک روش استقرایی[۳] (رسیدن از جزءِ به کل) بوده که برای مطالعه سیستماتیک نقصهای اجزاءِ یک سیستم و اثرات احتمالی آنها بکار می رود.

بطور کلی اهداف یک مطالعه FM&EA عبارتند از:

ـ شناسایی حالات نقص مهم که قابلیت اطمینان[٤]، قابلیت دسترسی[٥]، نگهداشت پذیری[٦] و بطور کلی ایمنی سیستم را تحت تأثیر قرار می دهند.

ـ تعیین اثرات حالات مختلف نقص اجزاءِیک سیستم بر روی کارکردهای مختلف همان سیستم.

اجرای FM&EA دارای چهار مرحله زیر است:

۱- شناسایی سیستم، کارکردها و اجزای آن

۲- شناسایی حالات نقص اجزاءِ و علل آنها

۳- بررسی اثرات نقصهای شناسایی شده

٤- بحث و نتیجه گیری و ارائه راه حلها و پیشنهادات کنترلی و اصلاحی

شناسایی سیستم، کارکردها و اجزای آن

2 - Failure Mode and Effect Analysis (FM&EA)
3 - Inductive Method
4 - Reliability
5 - Maintainability
6 - Availability

در این روش نیز بایستی همانند سایر روشهای دیگر قبل از هر چیزی سیستم و کارکردهای آن بخوبی تعریف شده و حالات عملیاتی مختلف آن مشخص شود. علاوه بر موارد یاد شده داشتن اطلاعات زیر نیز ضروری خواهد بود:

- کارکردهای اصلی سیستم
- محدودیتهای کارکردی سیستم با توجه به کل سیستم و هر کدام از اجزاء آن
- خصوصیات محیطی که سیستم در آن کار می کند

اطلاعات فوق را می توان از طریق منابع زیر کسب کرد:

- نقشه طرح
- طرحواره سیستم
- نمودار کارکردی
- تشریح سیستم
- داده های سازنده سیستم و اجزاءآن
- داده های حاصل از سایر تآنالیز های قبلی انجام شده از سیستم (در صورت وجود)

شناسایی حالات نقص اجزاء و علل آنها

در این مرحله لازم است حالات نقص اجزاء درکلیه حالات عملیاتی سیستم مشخص شود. قابل ذکر است که حالت نقص هر جزء بصورت اثراتی که نقص بر اساس آن مشخص می شود تعریف می گردد. مرحله مشخص کردن حالات نقص بایستی بطور کامل، جامع و دقیق صورت پذیرد زیرا آنالیز اصلی بر اساس آن انجام خواهد شد. بنابراین در اولین مرحله حالات نقص احتمالی یا بالقوه شناسایی شده و همزمان با آن علل احتمالی هر حالت نقص نیز مشخص می شود. باید توجه داشت که تمیز دادن بین حالت نقص و علت نقص همیشه راحت نیست و این امر شاید اولین مشکل در اجرای FM&EA باشد برای تسهیل در افتراق بین حالت و علت نقص می توان حالات نقص را بصورت اثرات علت نقص بر روی کارکرد جزء تعریف کرد.

لازم به یادآوری است که مشخص کردن همه علل احتمالی یک حالت نقص غیرممکن بوده ولی بسیار دشوار است. برای شناسایی حالات نقص می توان از پیسنهادات زیر استفاده کرد:

۱ـ اگر جزء قبلاٌ در سیستم تحت مطالعه یا سیستمهای دیگر مورد استفاده قرار گرفته باشد تجارب عملیاتی، تست و نگهداری آن می تواند راهگشا باشد.

۲ـ اگر جزء برای اولین بار طراحی شده و سابقه استفاده نداشته باشد می توان آن را با اجزایی که از نظر طرح یا کارکرد مشابه هستند مقایسه و از نتایج تجزیه و تحلیل قابلیت اعتماد جزء استفاده کرد.

برای تسهیل مرحله شناسایی حالات نقص می توان از طبقه بندی زیر که بعضی از حالات نقص مهم را نشان می دهد نیز استفاده کرد:

ـ پیش از موعد عمل کردن

ـ عمل نکردن در موعد معین

ـ متوقف نشدن در موعد معین

- بروز نقص در طول عملیات

بنابراین تجزیه و تحلیل گر بایستی حداقل چهار حالت احتمالی نقص فوق را مد نظر داشته باشد. همچنین بـــرای شناســـایی حالات نقص می توان از حالات نقص عمومی که در جدول شماره ۶ ارائه شده است نیز استفاده کرد. البته لازم است که حالات نقص برای کلیه مراحل عملیاتی سیستم بطور مجزا تعیین شود، بعنوان مثال ممکن است باز بودن یک دریچه برای یک وضعیت سیستم، نقص و برای وضعیت دیگر حالت طبیعی باشد. برای درک بهتر و راحتتر موضوع در بخش زیر حالات نقص یک موتور پمپ ارائه شده است:

۱ـ نقص در روشن شدن

۲ـ نقص در خاموش شدن

۳_ کمتر بودن میزان جریان پمپ از حد مورد نیاز (نقص در طول عملیات)

٤ـ کمتر بودن فشار تخلیه پمپ از حد ضروری (نقص در طول عملیات)

۵ـ روشن شدن ناخواسته

۶ـ نشت خارجی

جدول شماره۶: حالات نقص عمومی

ردیف	نقص	ردیف	نقص
۱	نقصهای ساختاری (ترکیدن)	۱۶	نقص در خاموش کردن
۲	از کار افتادن و خرابی فیزیکی	۱۷	نقص در روشن کردن

۳	ارتعاش	۱۸	نقص در راه انداختن
٤	ناتوانی در ماندن در وضعیت دلخواه	۱۹	پیش از موعد عمل کردن
۵	نقص در باز کردن	۲۰	دیرتر از موعد عمل کردن
۶	نقص در بستن	۲۱	ورودی اشتباه (بیش از حد)
۷	بطور اشتباه باز شدن	۲۲	ورودی اشتباه (کمتر از حد)
۸	بطور اشتباه بسته شدن	۲۳	خروجی اشتباه (بیش از حد)
۹	نشت داخلی	۲٤	خروجی اشتباه (کمتر از حد)
۱۰	نشت خارجی	۲۵	فقدان ورودی
۱۱	عمل کردن ناخواسته	۲۶	فقدان خروجی
۱۲	عمل کردن نامنظم	۲۷	اتصال کوتاه (الکتریکی)
۱۳	نشان دادن غلط	۲۸	باز بودن مدار (الکتریکی)
۱٤	جریان محدود شده	۲۹	نشت (الکتریکی)
۱۵	بکار گماری غلط	۳۰	غیره

بررسی حالت نقص اجزاء

در این مرحله اثرات هر حالت نقص بطور قانونمند روی کارکرد سیستم و همچنین روی اجزاءِ آن تعیین و بررسی می شود، این اثرات با فرض اینکه تنها یک حالت نقص وجود داشته و سایر اجزاءِ در حالت طبیعی کار می کنند بطور کامل تشریح می شوند. مطالعه اثرات با مد نظر قرار دادن متغیرهای مهم سیستم و تغییرات آنها آسانتر می شود. در مواقعی ممکن است مدلسازی پدیده های فیزیکی و یا دعوت از متخصصین برای مشخص کردن اثرات احتمالی تحت شرایط خاص الزامی باشد.

بحث، نتیجه گیری وارائه پیشنهادات

پس از انجام مراحل سه گانه فوق تجزیه و تحلیل گر سیستم قادر خواهد شد که در راستای اهداف مطالعه بحث و نتیجه گیری را انجام داده و پیشنهادات و راه حلهای احتمالی را ارائه کند. نتایج این مرحله می تواند بسیار جالب باشد که تعدادی از آنها عبارتند از:

۱- اطمینان از اینکه کلیه حالات نقص قابل تصور و اثرات آنها بر روی عملیات سیستم از مرحله طراحی بررسی شده اند.

۲- تهیه لیستی از حالات نقص بر اساس شدت اثرات آنها بر روی کارکرد سیستم

۳- شناسایی نقص های ثانویه[۷] و افزونگی های[۸] لازم

٤- طراحی و سایل و تدابیر خاص (آلارمها، تستهای دوره ای و...) جهت شناسایی حالات نقص و نحوه ارزیابی آنها

۵- طراحی روشهای نگهداری مطابق با هر حالت نقص و در نتیجه مطالعه و بررسی قابلیت نگهداری سیستم

ارائه آنالیز نتایج آن

برای نشان دادن مراحل آنالیز FM&EA و نتایج آن از برگه های کار مختلفی استفاده می شود که بسته به نوع مطالعه و وسعت آن در پاره ای از موارد باهم دیگر تفاوتهای دارند. در شکل های زیر نمونه های از برگه کار ارائه شده است:

برگه کار FM&EA									
نام سیستم:					تکمیل کننده:				
تاریخ:					تائید کننده:				
تشریح مختصر سیستم:									
ردیف	جزء	حالت نقص	علت نقص	اثرات نقص	شدت نقص	ردیابی	نرخ نقص	احتمال ردیابی	اقدامات کنترلی

شکل ۱: نمونه ای از برگه کار FM&EA

7- Secondary Failure
8 - Redundancy

سیستم: تکمیل کننده: تائید کننده:	محل اجراء: تاریخ: ص ... از ص.....:

تشریح مختصر سیستم:

ردیف	جزء	حالت نقص	اثر نقص	علل نقص	کنترلهای موجود	ریسک اولیه	اقدامات پیشنهادی	ریسک ثانویه	مسئولیت اجراء و تاریخ اتمام

شکل ۲: نمونه ای از برگه کار FM&EA

گزارش FM&EA

پس از تکمیل برگه کار FM&EA داده های حاصل از تجزیه و تحلیل به فرمهای گزارش که حداقل شامل بخشهای زیر می باشد منتقل می شوند:

اطلاعات مقدمه ای:

این بخش از گزارش شامل تشریح اهداف مطالعه، محدودیتهای موجود در اجرای آن و متدولوژی می باشد.

تعاریف:

در این قسمت آن دسته از کلمات و اصطلاحاتی که در بین پرسنل ایمنی متداول نیست، تعریف و تشریح می شود.

توصیف سیستم:

گزارش FM&EA بایستی شامل اطلاعات توصیفی دقیق در باره سیستم یا زیرسیستم های مورد مطالعه نظیر وظیفه یا وظایف سیستم و روابط دقیق بین اجزای آن، شرایط محیطی، نقش اپراتورها در سیستم و غیره باشد. در صورتیکه FM&EA برای یک سیستم در حال کار اجرا می شود بیان تاریخچه دقیق سیستم از ابتدای طراحی تا حال حاضر و تشریح مشکلات ایمنی گزارش شده مستند از سیستم در مراحل قبلی نیز ضروری خواهد بود. لازم به ذکر است که ارائه اطلاعات توصیفی بیش از حد بویژه در مواردی که ارتباطی با اهداف مطالعه نداشته باشد تنها بر مشکلات مطالعه خواهد افزود.

بررسی بحرانیت:

در این قسمت از گزارش میزان بحرانی بودن عمل سیستم، زیر سیستم یا اجزاء تشریح می شود. این بخش از بررسی معمولاً بر اساس بعضی از معیارهای از پیش تعیین شده که مورد

موافقت مدیریت نیز می باشد صورت می گیرد. در ارزیابی یک سیستم با استفاده از تکنیک FM&EA ، بحرانیت عبارت است از بیان اهمیت اثرات احتمالی نقص بر روی سیستم. اثرات احتمالی نقص ممکن است باعث تحمیل اثرات سوءِ بر روی افراد (مرگ، جراحات وخیم، بیماری و...)، سایر تجهیزات و خود سیستم بشود. در این قسمت همچنین لازم است در راستای ارائه راه حلها و پیشنهادات کنترلی که در بخشهای بعدی ارائه می شود دلیل یا دلایل پذیرش یا رد ریسکها نیز بطور دقیق ذکر شود.

لیست اسناد و مدارک:

جهت تکمیل FM&EA، تجزیه و تحلیل گر معمولاً نیازمند مرور کلی و ارائه کلیه مدارک و اسناد مرتبط با سیستم تحت مطالعه می باشد. در این بخش لیست اسناد، مدارک، نقشه ها و شکلهای شماتیک سیستم به همراه اسناد فروشنده، سازنده و غیره ارائه شده و استانداردهای مورد استفاده بررسی می شوند.

بخش داده ها:

کلیه داده های مورد استفاده در اجرا وتکمیل FM&EA به همراه کلیه داده های که در ارائه تجزیه و تحلیل نهایی از آنها استفاده می شود بایستی در گزارش نهایی FM&EA آورده شود. این داده ها می تواند شامل عکسهای از سیستم، زیر سیستم یا بعضی از اجزای مورد مطالعه، نقشه جانمایی، شمای الکتریکی و برگه کار FM&EA باشد.

حالات شکست و آنالیز بحرانیت[9]

FM&CEA یکی از روشهای مشتق شده از تکنیک FM&EA است که علاوه بر تعیین اثرات حالات شکست، سطح بحرانیت آنها را نیز ارزیابی می کند. سازمان هوا فضای ملّی آمریکا[10] NASA از این تکنیک بطور گسترده ای بویژه در طراحی مدل ماهواره ها استفاده می کند. از این روش همچنین در سایر حیطه های صنعتی نیز استفاده شده است برای مثال می توان به مطالعات انجام شده در کارخانه تویوتای ژاپن اشاره کرد.

FM&CEA اساساً از دو بخش تشکیل شده است:

ـ FM&EA

ـ تجزیه و تحلیل سطح بحرانیت به منظور تعیین شدت و احتمال وقوع برای هر حالت نقص

9- Failure Mode and Criticality Effect Analysis(FM&CEA)
10- National Airspace Administration(NASA)

برای تخمین شدت حالات مختلف نقص، شدت پیامدها و اثرات آن، هر حالت نقص بر اساس جداول خاص مورد بررسی قرار گرفته و به هر حالت یک شدت خاص اختصاص می یابد و احتمال وقوع حالات نقص بر اساس نرخ نقص های آنها که در برگه کار FM&CEA از قبل تعیین شده مشخص می گردد(جدول شماره ۷ و ناگفته پیداست اثراتی که از شدت و احتمال وقوع بالاتری برخوردار باشد حساستر بوده و حذف یا کاهش آنها از اهمیت بیشتری برخوردار خواهد بود.

جدول شماره ۷: مثالی از درجه بحرانیت

احتمال / شدت	بسیار پائین	پائین	متوسط	بالا
طبقه ۱ (اثرات کوچک)				
طبقه ۲ (اثرات بزرگ)				
طبقه ۳ (اثرات بحرانی)				
طبقه ٤ (اثرات فاجعه بار)				

آنالیز درخت خطا

تجزیه و تحلیل درخت خطا[11] یا روش درخت علت[12] برای اولین بار در سال ۶۲ - ۱۹۶۱ در آزمایشگاههای تلفن بل بوجود آمد و سپس توسط آقای ٌ واتسونٌ جهت تعیین و بهبود قابلیت اطمینان سیستم کنترل موشکهای قاره پیما توسعه یافت. این تکنیک در سالهای بعد توسط شرکت هواپیمایی بوئینگ گسترش یافته و بصورت قانونمند در آمد، اولین مقاله در باره آن در سال ۱۹۶۵ در سمپوزیوم ایمنی سیستم ها که توسط دانشگاه واشنگتن و شرکت بوئینگ برپا شده بود ارائه گردید.

ازسال ۱۹۶۵ استفاده از تکنیک FTA به صنایع مختلف نظیر هوافضا، هسته ای، شیمیایی و غیره گسترش یافت و از آن بطور گسترده ای جهت تجزیه و تحلیل قابلیت اطمینان، قابلیت دسترسی و ایمنی سیستمها استفاده شد.

تکنیک تجزیه و تحلیل خطا یا روش درخت علت بعنوان یکی از قویترین ابزارهای تجزیه و تحلیل فرایند ایمنی سیستم بویژه در هنگام ارزیابی سیستمهای بسیار پیچیده و دقیق محسوب می

11- Fault Tree Analysis (FTA)
12- Cause Tree Method (CTM)

شود. بدلیل استفاده از روش قیاسی[۱۳] (رسیدن از کل به جزءِ) در این متد، بسیاری از تجزیه و تحلیل گرهای ایمنی سیستم، بکار گیری روش FTA را در بررسی حالات احتمالی مختلف که می توانند منجر به بروز رویدادهای مطلوب یا نامطلوب در سطح سیستم شوند بسیار مفید می دانند.

هرچند که FTA بعنوان یک ابزار مقدماتی در تجزیه و تحلیل خطاهای موجود در یک سیستم و یا در طول یک فرایند عمل می کند ولی بایستی در نظر داشت که از این تکنیک می توان در ارزیابی فعالیتهای لازم جهت رسیدن به یک رویداد مطلوب و مورد نظر نظیرً عدم وقوع حادثه X نیز استفاده کرد. با ساخت درخت خطا که نشان دهنده کلیه رویدادهای لازم برای وقوع رویداد اصلی خواهد بود تجزیه و تحلیل گر می تواند از آن برای تشکیل پایه های یک برنامه پیشگیری از بروز حوادث صنعتی نیز استفاده کند. در این جزوه هر دو نوع کاربرد FTA (یعنی ارزیابی رویداد های مطلوب یا مثبت و نامطلوب یا منفی) با استفاده از مثالهای مناسب مورد بحث قرار خواهد گرفت.

تکنیک FTA در بررسی ایمنی سیستم بصورت یک روش سازمان یافته، دقیق و چند سونگر عمل می کند؛ سازمان یافته از این نظر که هر رویدادی را با توجه به نوع رویداد، عملکرد و جایگاه آن در سیستم یا فرایند ارزیابی می کند، دقیق به این دلیل که ارتباط و نقش رویدادها را بصورت تکی یا ترکیبی از آنها در وقوع رویداد اصلی مورد بررسی قرار می دهد و چند سونگر از این جهت که تجزیه و تحلیل گـر را قادر می سازد که اثرات بالقوه رویدادهای احتمالی موجود در ساختمان درخت خطا برروی رویداد اصلی را ارزیابی کنـد.

بدلیل انعطاف پذیریهای موجود در تکنیک FTA از این روش در مرحله طراحی از عمر سیستم نیز استفاده می شود، FTA قادر است که نقصهای بالقوه در طی فاز طراحی را پیش بینی کرده و تغیرات و تصحیحات ضروری را مشخص سازد از این روش همچنین می توان در طول فاز عملیاتی نیز برای تعیین ماهیت رویدادهای مطلوب یا نامطلوب ناشی از فعالیت سیستم استفاده کرد.

تجزیه و تحلیل درخت خطا ممکن است بدنبال اجرای یک برنامه PHA یا FM&EA صورت گیرد هرچند که هیچکدام از آنها پیش نیازی برای FTA محسوب نمی شوند.

قبل از بحث در باره درخت خطا ذکر این نکته ضروری است که اگر برای دو رویداد دو تجزیه و تحلیل گر دو درخت خطا طراحی نمایند لزومی ندارد که درختهای خطای حاصله بخصوص در سیستمهای پیچیده کاملاً شبیه هم باشند ولی در صورت انجام تجزیه و تحلیل کیفی و کمّی بایستی نتایج حاصله مشابه هم باشند.

13 - Deductive Method

آنالیز درخت خطا

اولین گام در آنالیز درخت خطا شناخت کامل و دقیق سیستم است. اطلاعات دقیق و جزئی در باره کلیه اجزاءِ سیستم، اثرات متقابل فیزیکی وکارکردی مابین اجزاءِ و شرایط طبیعی و غیرطبیعی آنها را می توان از منابع مختلفی نظیر بررسی نقشه ها، نمودارها، لیست اسامی اجزاءِ، دستورالعملهای عملیاتی، روشهای تعمیر ونگهداری، مصاحبه با کارکنان، متخصصین و غیره بدست آورد بعلاوه مقایسه سیستم با سیستمهای مشابه نیز می تواند اطلاعات مفید دیگری را تأمین کند.

اطلاعات مورد نیاز در آنالیز درخت خطا می تواند شامل موارد زیر باشد:

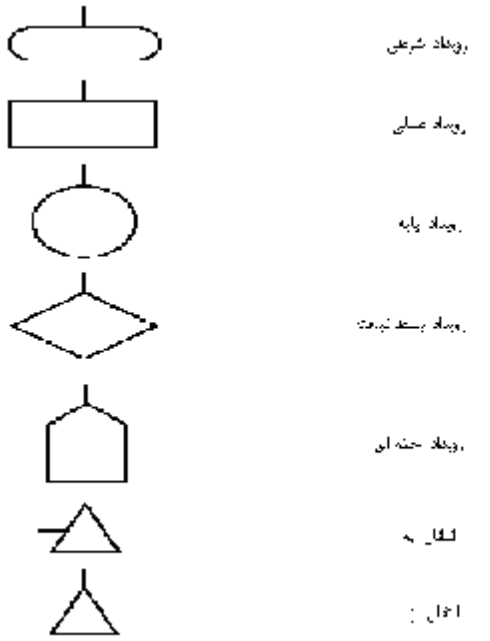
- لیست کامل کلیه اجزاءِ سیستم
- عمل و وظیفه هر جزءِ
- وضعیت اولیه هر جزءِ (نظیر باز یا بسته بودن دریچه های فن و...)
- شرایط طبیعی محیطی و عملیاتی هر جزءِ (دما، فشار، استرسهای مکانیکی، ارتعاشات و...)
- شرایط غیرطبیعی و عملیاتی هر جزءِ در شرایط اضطراری و بروز حوادث
- حالات نقص هر جزءِ
- ارتباط نقص اجزاءِ با یکدیگر
- تداخل کارکردی جزءِ با سایر اجزاءِ
- وظیفه اپراتورها
- روشهای عملیاتی، تعمیر و نگهداری و...
- کنترلهای کامپیوتری
- و...

قابل ذکر است که در صورتیکه رویداد اصلی درخت خطا یک رویداد مثبت و مطلوب باشد توصیه می شود که بجای عبارت درخت خطا از عبارتً درخت علتً استفاده شود.

نمادهای مورد استفاده در تکنیک FTA

در ساخت درخت خطا از نمادهای مختلفی استفاده می شود که تجزیه و تحلیل گر را قادر می سازد نوع رویداد ها وهمچنین ارتباط آنها با همدیگر را بصورت تصویری نشان دهد در شکل زیر نمادهای اصلی مورد استفاده در تکنیک FTA نشان داده شده است با درک معانی،

مفاهیم و کاربرد های ویژه نمادها که در شکل زیر بیان شده است ساخت درخت خطا ساده تر و راحتتر خواهد شد.



شکل ٤: تعدادی از نمادهای مورد استفاده در ساخت درخت خطا

مفاهیم بعضی از اصطلاحات معمول در تکنیک FTA بشرح زیر می باشد:

رویداد اصلی[14]: عبارت است از رویدادی که در بالاترین نقطه درخت خطا جای می گیرد و علل بوجود آورنده آن شناسایی و تجزیه و تحلیل می گردد. رویداد اصلی در هر درخت خطا منحصر بفرد بوده و می تواند یک حادثه (انفجار، رها شدن گازهای سمی و...)، از کار افتادن سیستم، بدکارکردن آن (عدم کارآیی مورد انتظار) و یا یک رویداد مطلوب باشد. بعبارت ساده تر می توان گفت که رویداد اصلی رویدادی است که تجزیه و تحلیل بدنبال یافتن علل و راههای بوقوع پیوستن آن است.

رویداد میانی[15]: هر رویدادی در ساختمان درخت خطا به استثنای رویداد اصلی که مورد تجزیه و تحلیل بیشتر قرار گرفته و علل بوجود آورنده آن تعیین می گردد رویداد میانی نامیده می شود.

14 - Top event
15 - Intermediate event

رویداد پایانی[16]: رویداد پایانی که ممکن است تحت عناوینی نظیر رویدادهای انتهایی یا اولیه نیز خوانده شود رویدادی است که نمی توان علل بوجود آورنده آن را تعیین کرد. رویدادهای پایانی به سه گروه زیر طبقه بندی می شوند:

رویداد پایانی پایه ای[17]: هر رویدادی در سطح جزءِ که قابل تشریح بیشتر نباشد را رویداد پایه ای گویند رویدادهای خارجی نظیر سیل، گردوباد، زلزله و...که ایمنی سیستم را تهدید می کنند از نوع رویداد پایه ای محسوب می شوند.

رویداد پایانی بسط نیافته[18]: رویدادی است هر چند می تواند مورد تجزیه و تحلیل بیشتر قرار بگیرد ولی این امر بنا بدلایلی صورت نمی گیرد.

رویداد پایانی خانه ای[19]: نوع خاصی از رویداد پایانی است که در تجزیه و تحلیل درخت خطا در دو حالت ٌ روشنٌ یا ٌ خاموشٌ بکار گرفته می شود. احتمال رویداد خانه ای در حالت روشن و خاموش بترتیب برابر یک و صفر می باشد. رویداد خانه ای ممکن است رویداد کلیدی، طبیعی و ماشه ای نیز خوانده شود.

دروازه ٌ یا ٌ[20]: این دروازه برای نشان دادن این حالت که برای وقوع رویداد خروجی رخ دادن یکی از رویداد های خروجی کافی می باشد بکار گرفته می شود. رویداد خروجی ممکن است رویداد میانی یا اصلی بوده و رویدادهای ورودی نیز می توانند رویداد میانی، پایانی و یا ترکیبی از آنها باشد.

دروازه ٌ وٌ[21]: این دروازه به این معنی است که وقوع رویداد خروجی مستلزم رخ دادن کلیه رویدادهای ورودی است. رویداد خروجی می تواند رویداد اصلی یا میانی بوده و رویداد ورودی نیز ممکن است رویداد میانی، پایانی و یا ترکیبی از آندو باشد.

برش[22]: ترکیبی از رویدادهای پایانی است که می توانند باعث بروز رویداد اصلی بشوند، رویداد اصلی ممکن است بیش از یک برش داشته باشد.

برش حداقل[23]: بـــه کوچکترین زیر مجموعه برش که بـرای وقوع رویداد اصلی لازم و کافی باشد برش حداقل گویند.

نمادهای انتقال[24]: زمانیکه تجزیه و تحلیل گر درخت خطا در حین کار بر روی یک شاخه درخت خطا به مرحله ای برسد که از آن به بعد در شاخه دیگری از آن درخت خطا نیز تکرار شده باشد

16 - Terminal event
17 - Basic event
18 - Undeveloped event
19 - House event
20 - OR Gate
21 - AND Gate
22 - Cut Set
23 - Minimal Cut Set

می تواند آن را به شاخه یاد شده منتقل و کار خود را در شاخه جدید به پایان برساند که برای این عمل از نمادهای انتقال استفاده می شود، از این نمادها همچنین برای نشان دادنٌ ادامه کار در صفحات بعدٌ بویژه در درخت خطای سیستمهای بزرگ و پیچیده که در یک صفحه جای نمی گیرند نیز استفاده می شود.

تکنیک تجزیه و تحلیل درخت خطا شامل سه مرحله زیر است:

۱- ساخت درخت خطا[۲۵]

۲- تجزیه و تحلیل کیفی درخت خطا [۲۶]

۳- تجزیه و تحلیل کمّی درخت خطا[۲۷]

با توجه به اهداف مطالعه ممکن است هر کدام از مراحل فوق به تنهایی و یا همراه یکدیگر صورت گیرد.

تجزیه و تحلیل درخت خطا ممکن است بصورت کیفی، کمّی و یا هر دو شکل صورت گیرد:

الف) تجزیه و تحلیل کیفی درخت خطا

مهمترین روشهای تجزیه و تحلیل کیفی درخت خطا عبارتند از:

الف -۱) رده بندی کیفی برشهای حداقل

الف -۲) رده بندی کیفی رویدادهای پایانی

الف -1) رده بندی کیفی برشهای حداقل

هر یک از برشهای حداقل نمایانگر یک راه احتمالی برای وقوع رویداد اصلی می باشند بدین ترتیب که با رخ دادن رویدادهای که در یک برش حداقل قرار دارند رویداد اصلی بوجود خواهد آمد، بنابراین تجزیه و تحلیل آنها ارزیابی اهمیت هر یک از راههای احتمالی بروز رویداد اصلی خواهد بود.

تعداد رویدادهای پایانی موجود در یک برش حداقلٌ طبقهٌ آن برش نام دارد، در صورتیکه احتمال وقوع رویدادهای پایانی تقریباً یکسان بوده و وقوع آنها مستقل از هم باشد برشهای حداقل کم طبقه مهمتر از نوع پر طبقه خواهد بود.

لازم به ذکر است که دو رویدادی را مستقل از هم می گویند که نتیجه وقوع یکی بر نتیجه وقوع دیگری هیچ اثری نداشته باشد.

---

24 - Transfer Symbols
25 - Fault Tree Construction
26 - Qualitative Fault Tree Analysis
27- Quantitative Fault Tree Analysis

رده بندی برشهای حداقل نسبت به رده بندی رویدادهای پایانی از اهمیت کمتری برخوردار است.

الف -2) رده بندی کیفی رویدادهای پایانی

رده بندی کیفی رویدادهای پایانی بر حسب اهمیت آنها در ایجاد رویداد اصلی ممکن است بر اساس برشهای حداقل و به شرح زیر صورت گیرد:

۱ـ رویدادهای پایانی موجود در برشهای حداقل کم طبقه معمولاً مهمتر از آنهایی هستند که در برشهای حداقل پرطبقه قرار دارند.

۲ـ اگر دو رویداد پایانی تنها در برشهای حداقل n طبقه وجود داشته باشند آن رویدادی که به تعداد دفعات بیشتری در برشهای حداقل یاد شده تکرار گردیده است از اهمیت بیشتری برخوردار خواهد بود. دو اصل فوق در صورتی معتبر خواهد بود که احتمال وقوع رویدادهای پایانی یکسان بوده و از نظر آماری مستقل از هم باشند

ب) تجزیه و تحلیل کمّی درخت خطا

از روابط احتمالاتی موجود بین رویدادهای ورودی و خروجی و همچنین دروازه های ٌوٌ و ٌیاٌ می توان بشکل زیر برای محاسبه احتمال وقوع رویدادهای میانی و در نتیجه رویداد اصلی استفاده کرد. مهمترین روشهای تجزیه و تحلیل کمّی درخت خطا عبارتند از:

ب -1) تجزیه و تحلیل کمّی دروازه ٌوٌ

ب -2) تجزیه و تحلیل کمی دروازه ٌیاٌ

ب- 3) رده بندی کمّی رویدادهای پایانی

در صورت کوچک بودن سیستم تحت مطالعه یا انجام کامپیوتری تجزیه و تحلیل درخت خطا که امکان تعیین کلیه برشهای حداقل وجود دارد برای تعیین نقش رویدادهای پایانی در کمک به وقوع اصلی می توان از فرمول پیشنهادی VESELY - FUSSELL بشرح زیر استفاده کرد:

$$I_A = \Sigma U_a / \Sigma U_a$$

I_A: اهمیت رویداد پایانی A در ایجاد رویداد اصلی

ΣU_a: حاصل جمع احتمال وقوع برشهای حداقلی که رویداد A در آنها وجود دارد

U_S: احتمال وقوع رویداد اصلی

در صورتیکه در درخت خطای بنا به هر دلیلی امکان تغییر برشهای حداقل وجود نداشته باشد اهمیت رویدادهای پایانی با توجه به احتمال وقوع و همچنین نوع دروازه بین آنها و رویداد اصلی تعیین خواهد شد. بطور کلی با افزایش تعداد دروازه های "و" بین رویداد های پایانی و رویداد اصلی، نقش رویداد پایانی در وقوع رویداد اصلی کاهش خواهد یافت زیرا وجود دروازه "و" به این معنی است که رویداد مورد نظر برای رسیدن به رویداد اصلی نیازمند وقوع رویداد یا رویدادهای دیگری نیز می باشد که حاصلضرب احتمال وقوع دو یا چند رویداد همواره کوچکتر از احتمال وقوع هرکدام از آنها خواهد شد، اما تعداد دروازه های "یا" از تأثیر رویداد پایانی در کمک بوقوع رویداد اصلی نخواهد کاست.

مطالعه عملیات و خطر(Hazop)[۲۸]

تولید و عملیات مربوط به هر چیزی، نیازمند الزامات و پیش نیازهای است که قصور از هر کدام از آنها می تواند به بروز پیامدهای ناخواسته ای در قالب جراحات تولید کنندگان، کاربران، آسیب به فرآیندها و محصولات تولیدی و سایر دارائیهای با اهمیت بیانجامد. در یک شرکت با خط مشی ایمنی سیستم، الزامات یاد شده از مرحله قبل از تولد سیستم یعنی فاز ایده و تفکر شروع شده و تا پایان فاز کنار گذاشتن سیستم (فاز انهدام یا دفع) ادامه می یابد. در پایان هر مرحله لازم است در راستای اصلاح سیستم و بهبود مداوم آن برپایه یافته های حاصل از ارزیابیهای انجام شده، فرآیند تصمیم گیری مبتنی بر چرخه دمینگ (طرح ریزی، انجام، کنترل و اجراء) به مرحله اجراء گذاشته شود.

تکنیک مطالعه عملیات و خطر بعنوان یکی از پرکاربردترین تکنیکهای کیفی است که با دیدی سیستماتیک به ارزیابی ایمنی سیستم های فرآیندی می پردازد.

تکنیک Hazop برای اولین بار در سالهای ۱۹۷۰ بر اساس تکنیکی که "آزمایش بحرانی" خوانده می شود توسط صنایع شیمیایی سلطنتی بریتانیای کبیر معرفی و سپس توسط T.A.Kletz بصورت قانونمند درآمد. اساساً تکنیک Hazop که ماهیتی آینده نگر و مبتنی بر پیشگیری قبل از وقوع دارد بعنوان واکنشی به استفاده از متد چک لیست که مبتنی بر فلسفه گذشته نگر است بود. هر چند که تکنیک Hazop اولین بار بمنظور شناسایی و ارزیابی خطرات فرآیندی معرفی و بکار گرفته شد ولی در ادامه کاربرد آن با معرفی توانمندیهای دیگر آن به سایر صنایع نیز گسترش یافت.

تعریف Hazop

28 -Hazard and Operability Study(HAZOP)

کلمه Hazop برگرفته از سه حرف اولیه کلمه Hazop به مفهوم خطر و دو حرف اولیه Operability به معنی قابلیت عملیات می باشد. تکنیک Hazop را می توان بشرح زیر تعریف کرد:

ـ Hazop تکنیک شناسایی، ارزیابی و کنترل خطرات برپایه نگرش سیستمی است و بر پایه این اصل استوار است که: سیستم زمانی ایمن است که کلیه پارامترهای عملیاتی آن نظیر فشار، درجه حرارت، میزان جریان و غیره در حالت طبیعی قرار داشته باشد. با توجه به تعریف اخیر، برای موفقیت آمیز بودن نتایج Hazop، شناسایی دقیق سیستم تحت مطالعه، تعیین کلیه پارامترهای عملیاتی و حدود طبیعی و قابل قبول آنها آنهم در شرایط طبیعی و اضطراری و با در نظر داشتن تغییرات قابل تحمل از اهمیت حیاتی برخوردار است.

بنابراین به اختصار می توان گفت هدف از اجرای مطالعه Hazop شناسایی خطرات بالقوه و مشکلات عملیاتی است که ممکن است در اثر انحراف پارامترهای عملیاتی از شرایط طرح شده در سیستم های جدید یا اصلاح شده رخ دهد.

زمان اجرای Hazop

هر چند که می توان مطالعه Hazop را در کلیه فازهای عمر یک سیستم انجام داد ولی اجراء و استفاده از یافته های آن در فاز طراحی بسیار مفیدتر بوده و نتایج آن از قابلیت اجرائی بیشتری برخوردار خواهد بود. هر چند که ممکن است در منابع مختلف مراحل اجراء متفاوتی برای Hazop بیان شده باشد ولی مراحل اصلی عبارتند از:

۱ـ تعیین عمق کار و اهداف یک مطالعه
۲ـ انتخاب تیم عملیاتی
۳ـ انتخاب حیطه مطالعه
٤ـ اجراء Hazop

کلمات کلیدی مورد استفاده در تکنیک Hazop

معمولترین کلمات کلیدی مورد استفاده در ارزیابیهای ایمنی با استفاده از تکنیک Hazop عبارتند از:

جدول شماره ۸: تعدادی از کلمات کلیدی مورد استفاده در تکنیک Hazop

کلمه کلیدی	مفهوم
هیچ (No/Not)	پارامتر مورد نظر انجام نمی شود. وجود ندارد
کمتر از (Less than)	پارامتر مورد نظر کمتر و یا پائین تر از حد طبیعی است- کاهش کمی

بیش از (Morethan)	پارامتر بالاتر و بیشتر از حد استاندارد است ـ افزایش کمی
بعلاوه (As well As)	موارد دیگری به غیر از پارامتر تعریف شده وجود دارد ـ افزایش کیفی
بخشی از (Part of)	بجای کل پارامتر مورد تنها قسمتی از آن وجود دارد ـ کاهش کیفی
معکوس (Reverse)	پارامتر عکس حالتی که تعریف شده است اتفاق می افتد
بجای اینکه (Other than)	نوع پارامتر جابجا شده و عوض می شود.

هنگامیکه در جریان ارزیابی ((زمان)) نیز حائز اهمیت باشد ممکن است از کلمات کلیدی زیر استفاده شود:

کلمه کلیدی	مفهوم
زودتر (Early)	وظیفه زودتر از موعد مقرر انجام می گیرد
دیرتر (Late)	وظیفه دیرتر از موعد مقرر انجام می گیرد
قبل از (Before)	وظیفه در طول توالی خود قبل از موعد مقرر انجام می شود
بعد از (After)	وظیفه در طول توالی خود بعد از موعد مقرر انجام می شود.

درانتخاب کلمات کلیدی توجه به موارد زیر ضروری است:

ـ کلمات کلیدی باید متناسب و هماهنگ با سیستم موجود باشد.

ـ کلمات کلیدی باید متناسب و هماهنگ با خصوصیات طراحی سیستم باشد.

ـ ممکن است برای یک پارامتر خاص همه کلمات کلیدی قابل استفاده نباشد. بعنوان نمونه برای پارامتر سرعت یک موتور الکتریکی نمی توان از کلمات کلیدی بعلاوه و بخشی از استفاده کرد، همچنین برای جریان داده نمی توان از کلمه کلیدی کمتر استفاده کرد زیرا مفهوم آن با کلمه کلیدی در بخشی از پوشش داده می شود.

ـ عموماً کلمات کلیدی توسط رهبر تیم انتخاب شده و پس از تفسیر مفاهیم آنها بر اساس خصوصیات طراحی سیستم برای استفاده دراختیار اعضاءِ تیم قرار می گیرد.

مراحل مختلف Hazop فرایندی عبارت است از:

ـ بازنگری دیاگرامهای جریان مربوط به فرایند مورد مطالعه

ـ تقسیم سیستم به زیر سیستم های متناسب

ـ بکارگیری کلمات کلیدی به پارامترهای مختلف موجود در فرآیند به منظور شناسایی انحرافات احتمالی

ـ یافتن نتایج و مستند کردن آنها

و نهایتاً اینکه:

ـ Hazop یک متد ساختاری طوفان مقری برای آنالیز ریسک است.

ـ Hazop می تواند در اشکال مختلف بر اساس عناصر تشکیل دهنده سیستم های ایمنی اجراء شود.

ـ هماهنگی خوبی با سایر متدهای آنالیز ریسک دارد.

ـ توانمندیهای آن توسط سازمانهای نظیر وزارت دفاع آمریکا، شرکت موتورولا و طیف وسیعی از شرکتهای شیمیایی به اثبات رسیده است.

آنالیز خطرات عملیات و پشتیبانی

آنالیز خطرات عملیات و پشتیبانی[29] یک تکنیک تجزیه و تحلیل ایمنی سیستم است که اساساً بر روی خطرات مرتبط یا ایجاد شده توسط انسان یا وظایف دخیل در عملیات سیستم متمرکز می شود. این تکنیک ممکن است تحت عنوان آنالیز خطرات عملیاتی[30] نیز خوانده شود.

اهداف اصلی استفاده از تکنیک عبارت است از:

۱- شناسایی کلیه خطرات احتمالی در طول عملیات سیستم که ماهیتاً برای افراد مخاطره آمیز بوده و عملیاتی که در آنها بروز یک خطای انسانی برای افراد و همچنین تجهیزات مخاطره آمیز می باشد.

۲ـ ارائه پیشنهاداتی در راستای کاهش ریسک در کلیه مراحل انجام وظیفه یا عملیات که از طریق دستورالعمل های مکتوب کنترل می شوند.

بعبارت ساده تر O&SHA شامل یک مرور تجزیه و تحلیلی از اسناد کنترل کننده جهت اطمینان از حذف مخاطرات یا کنترل آنها بوده که در این راه عملکرد انسان (عوامل انسانی) و ارتباط آن با مخاطرات مرتبط با شغل بطور دقیق مورد ارزیابی قرار می گیرد بنابراین در روش O&SHA توجه اصلی به سیستمهای عملیاتی و نگهداری است تا خود اجزاء سیستم.

O&SHAآندسته از کارکردهای عملیاتی را که ممکن است ماهیتاً برای افراد خطرناک بوده و همچنین شرایطی که در آن خطاهای انسانی می توانند برای افراد یا تجهیزات مخاطره آمیز باشند را مورد بررسی قرار می دهد بنابراین با این تفاسیر علم ارگونومی (مطالعه علمی ارتباط بین افراد، شغل و محیط کار) یک عنصر اساسی در مطالعات O&SHAخواهد بود.

29 - Operational and Support Hazard Analysis (O&SHA)
30 - Operational Hazard Analysis (OHA)

انسانها معمولاً بنحوی در ساخت و بهره برداری از اغلب سیستمها دخیل بوده و کاملاً مشخص شده است که خطاهای انسانی یک عامل مهم (چه بصورت عامل اصلی و چه عامل کمک کننده) در بروز بسیاری از حوادث می باشد بنابر این نقش انسانها یک فاکتور و عامل حساس و بحرانی در تجزیه و تحلیل ایمنی سیستمها می باشد.

در جدول شماره ۹ لیست خطاهای معمول که اغلب نتیجه خطای عنصر انسانی سیستم است ارائه شده است.

جدول شماره ۹: خطاهای انسانی که سیستم را تحت تأثیر می دهند

خطاهای معمول انسانی	
اپراتور	انجام ندادن یک عمل لازم انجام یک عمل غیرضروری ناتوانی در تشخیص یک عمل ضروری پاسخ نامناسب (زود، دیر، غلط) خطای نگهداری
طراح	فقدان آگاهی و شناخت از خطرات طرح عدم اطلاع کافی از ضرورتهای طراحی در زمینه وظایف تکراری طرح نیازمند پاسخ سریع اپراتور برای تشخیص و بر طرف کردن خطر است طرح ارائه شده نیازمند عمل سریع اپراتور و محاسبات پیچیده است در طرح ارائه شده نیازمندیهای سنسور خارج از دامنه عمل فرد است طرح ارائه شده نیازمند توجه مداوم اپراتور است طرح ارائه شده ایجاب می کند که اپراتور در یک محیط نامساعد کار کند طرح ارائه شده نیازمند فعالیت فیزیکی و برقراری ارتباط بطور همزمان است طراحی و تهیه ابزارهای نامناسب تهیه دستورالعملهای مکتوب نامناسب یا غلط
مدیر	ارائه آموزشهای نامناسب یا غلط برنامه ریزی غیرواقعی تولید و فراوری

اطلاعات ارائه شده در این جدول وظیفه و نقش مهم طراحها را در کاهش احتمال خطاهای انسانی که بروز آنها در هنگام بهره برداری از سیستم مشکلات بیشتر و پیچیده تری بدنبال خواهد داشت نشان می دهد. بنابر این لازم است که طراح بتواند کلیه نتایج احتمالی ناشی از یک خطای انسانی را پیش بینی کرده و با آنالیز دقیق آن سیستم را بنحوی طراحی کند که نتایج نهایی خطاهای انسانی وخیم و بحرانی نباشد. از آنجائیکه در بعضی مواقع بخشی از رفتارهای انسانی قابل پیش بینی است تجزیه و تحلیل گر لازم است که در هنگام ارزیابی سیستم انسان ـ ماشین عوامل یاد شده را نیزمورد توجه قرار دهد. برای مثال شاغلین معمولاً روشها و تکنیکهای را ترجیح می دهند که دارای خصوصیات زیر باشد:

الف) نیازمند حداقل تلاشهای فیزیکی و روانی هستند

ب) برای انجام یک وظیفه به صرف زمان کمتری نیاز دارند

ج) ناراحتی های حاصل از انجام آن بسیار اندک می باشد

د) یکنواختی و خستگی کمتری ایجاد می کنند.

خطاهای انسانی

هر عمل یا فعالیتی که از حدود مجاز تعریف شده توسط سیستم خارج شود "خطای انسانی"[۳۱] نامیده می شود. علل عمده خطاهای انسانی را می توان به چهار گروه زیر طبقه بندی کرده و با تکنیک O&SHA ارزیابی کرد:

۱ـ فیزیکی

۲ـ ضرورت های فضای کار

۳ـ محیطی

٤ـ محدودیت عملکرد انسان

دربخش زیر برای درک بهتر و راحتتر هر کدام از طبقات چهار گانه خود به بخشهای کوچکتر تقسیم شده اند. با تعیین و بررسی هر کدام از علل فوق در مورد یک فعالیت یا یک وظیفه خاص تجزیه و تحلیل گر قادر خواهد شد که اصول طراحی و متدهای کنترلی را برای پیشگیری از بروز یا کاهش احتمال خطاهای انسانی پیشنهاد کند (جدول شماره ۱۰).

جدول شماره ۱۰: خصوصیا ت خطاهای انسانی معمول

31 - Human Error

علل خطای انسانی	توصیف
فیزیکی	داده های نامناسب آنتروپومتریکی، محدودیتهای کنترلها و حفاظها شامل نوع، جهت، عملیات کور و غیره نارسائی در طراحی تجهیزات و سخت افزار
ضروتهای فضای کار	وضعیت اپراتور نسبت به فعالیتی که انجام می دهد نیازمندیهای وظیفه - فضای نامناسب برای کار محدویتهای ورود و خروج به محیط کار جداسازی نامناسب وظایف از همدیگر وظایف فوق العاده سنگین
محیطی	نامناسب بودن: روشنایی شرایط جوی تراز صدا لرزش و ارتعاش درجه حرارت
محدویتهای عملکرد انسان	تمرکزهای طولانی استرسهای جسمانی و روحی استراحتهای نامناسب بیماریها ناراحتی و اندوه

زمان اجرای O&SHA

بدلیل اهمیت زیاد عامل انسانی و لزوم کاهش ریسک جراحات وارده به افراد لازم است O&SHA در اولین مرحله از عمر محصول و در دیرترین حالت قبل از استفاده و بهره برداری از سیستم انجام گیرد. البته بایستی توجه داشت که این امر همیشه عملی نیست زیرا طراحی محصول یا سیستم معمولاً قبل از تعریف و تعیین دستورالعملهای عملیاتی و نگهداری صورت می گیرد. در بسیاری از مواقع لازم است که O&SHA در انتهای فاز ساخت و قبل از اولین استفاده تکمیل شود. تعیین زمان دقیق اجرای O&SHA بطور کامل به سیستم یا محصول نهایی مطلوب و قابل قبول بستگی خواهد داشت. بطور مثال در بسیاری از موارد محصول نهایی نوع جدید یا

اصلاح شده ای از محصول قبلی است. امروزه اجرای تکنیک O&SHA در کل چرخه عمر سیستم انجام می گیرد بنابراین لازم است که دستورالعملهای کاری مختلف، آموزشهای عملیاتی و روشها و دستورات نگهداری از قبل وجود داشته باشد. از طرف دیگر اگر یک محصول یا سیستم شکل اصلاح شده یا مدرن محصول یا سیستم قبلی باشد کاربرد نهایی محصول مشابه حالت تعریف شده قبلی خواهد بود و لذا O&SHA را می توان در همان مراحل اولیه فرایند انجام داد.

برای اجرای درست و دقیق یک مطالعه O&SHA لازم است که تجزیه و تحلیل گر شناخت کامل و دقیقی از سیستم بدست آورد، به کلیه اطلاعات مرتبط با طراحی دسترسی داشته باشد، دیاگرامهای تسلسل عملیاتی، تسلسل کارکردی، جانمایی پانل تجهیزات (در صورت وجود) و همچنین سایر نقشه ها را مورد بررسی قرار دهد و مقررات، قوانین و استانداردهای کارآیی را ارزیابی کند. لیست مقدماتی خطر، آنالیز مقدماتی خطر و آنالیز خطرات سیستم انجام شده می توانند منابع خوبی برای کسب اطلاعات مستند از سیستم مورد مطالعه در هنگام اجرای O&SHA باشند. همانطوریکه قبلاً نیز عنوان گردید یکی از اهداف اولیه O&SHA، آنالیز روشهای نگهداری و مدارک عملیاتی برای کنترل یا حذف خطرات می باشد بنابراین بررسی اسناد یاد شده نیز الزامی خواهد بود. علاوه بر موارد یاد شده بررسی داده های عملکرد عملیاتی، خصوصیات و مشخصات اختصاصی وسایل، اطلاعات مربوط به افراد شاغل در قسمتهای بهره برداری و نگهداری سیستم (آموزش مهارتها، تعداد افراد درگیر، ابعاد سازمان و غیره)، ضروری می باشد. پس از شناسایی و ارزیابی کامل کلیه خطرات مرتبط یا ایجاد شده بوسیله هر کدام از عوامل یادشده می توان به تکمیل برگه کار O&SHA اقدام کرد.

گزارش نهاییO&SHAبایستی شامل شرح کاملی از سیستم یا محصول، دستورالعملها، سازمانها یا افراد مسئول کارهای نگهداری و عملیاتی باشد بخش اصلی این گزارش را یافته های کلیدی تجزیه و تحلیل و پیشنهادات و توصیه های ارائه شده جهت کنترل خطرات تشکیل خواهد داد. معمولاً یک برنامه زمان بندی شده که نشانگر زمان اجرای مطالعات بعدی O&SHA است به همراه برگه کار تکمیل شده O&SHA ضمیمه گزارش نهایی خواهد بود.

بکارگیری مناسب تکنیک O&SHA علاوه بر اینکه نقش سیستم را مشخص کرده و ابزارهای کنترلی برای خطرات ایجاد شده در اثر تعامل انسان با سیستم را ارائه می کند می تواند تمامی افراد و تجهیزاتی که در طول عملیات در دامنه خطرات قرار دارند را شناسایی کرده و ضرورتهای احتیاطی و هشداردهنده را ارزیابی کند همچنین در یک مطالعه O&SHA تکمیل شده نیاز به مهارتهای ویژه یا ضرورت آموزش های بیشتر نیز شناسایی خواهد شد.

پرسش های پایان فصل:

۱. اهمیت ارزیابی ایمنی در فازهای مختلف چرخه عمر سیستمها را تشریح کنید.
۲. حادثه نشت یک ماده شیمیایی را با استفاده از تکنیک FTA آنالیز کنید.
۳. ایمنی یک مخزن تحت فشار با با استفاده از تکنیک HAZOP آنالیز نمائید.
٤. ایمنی یک موتور همزن را با استفاده از تکنیک FMEA بررسی کنید.

منابع:

۱.محمدفام ایرج، مهندسی ایمنی، همدان: انتشارات فن آوران، ۱۳۸۳.
۲. محمدفام ایرج، تکنیکهای ایمنی: مطالعه عملیات و خطر، همدان: انتشارات فن آوران، ۱۳۸٤.
۳.محمدفام ایرج، تکنیکهای ایمنی: آنالیز مقدماتی خطر، همدان: انتشارات فن آوران، ۱۳۸٤.
٤.محمدفام ایرج، تکنیکهای ایمنی: آنالیز درخت خطا مطالعه عملیات و خطر، همدان: انتشارات فن آوران، ۱۳۸٤.

5. Kohn, JP, Friend, MA, Winterberger, CA,. Fundamentals of Occupational Safety and Health. Rockville, MD: Government Institutes, Inc.1996.
6. Manuele, FA,. In Safety through Design, Ed.Christensen, W.C and Manuele, F.A., Chicago: NSC Press. 1999.
7. Hammer, W.: "Handbook of System and Product Safety;" Prentice-Hall, Inc.; 1972.
8. Malasky, S.W.; "System Safety: Technology and Application;" Garland STPM Press; 1982.
9. Roland, H.E. and Moriarty, B.; "System Safety Engineering and Management;" John Wiley & Sons; 2nd Edition; 1990.
10. Jeffrey W. Vincoli. Basic Guide to System Safety. Van Nostrand Reinhold; Hard cover; 1993.
11. MIL-STD-882C. System Safety Program Requirements. The most frequently cited military contract requirements document related to the practice of system safety. Soft cover; large format. 1993.