جزوات آموزشی

صنایع ایمن فراز ارک

عنوان محتوا:

روش ارزیابی ریسک نیمه کمی MIL-STD 882BV

استاندارد نظامی آمریکا

کد محتوا:

ARK-FO-159-061

تهیه و تدوین: گروه تولید محتوای صنایع ایمن فراز ارک

مقدمه

در گذشته برنامه های ایمنی براساس فلسفه (بعد از واقعه) به بررسی و کنترل حوادث می پرداختند. واضح است که چنین روشی برای بعضی از برنامه های خاص از قبیل تولید سلاح های هسته ای و محصولات فضایی از قبیل ماهواره ها و ماهواره‌برها قابل قبول نبود زیرا در صورت بروز خطا در این گونه سیستم ها عواقب بسیار وخیمی ایجاد می شد. همین امر باعث شد که بسیاری از سازمان های بزرگ و صنایع نظامی و هسته ای بسیاری از کشورها، رویکرد ایمنی سیستم را پذیرفته و آن را در بستر استاندارد مطرح در این حوزه از قبیل استاندارد نظامی۸۸۸ پیاده سازی نمایند. از نتایج مهم و تاثیرگذار این سیستم می توان به قابلیت ردیابی شکست ها و موفقیت ها، شناسایی و کنترل خطرات چرخه عمر سیستم، ارتقاء سطح ایمنی محصولات، مدیریت تغییرات، کاهش تعداد حوادث و تلفات انسانی و کاهش اثرات زیست محیطی اشاره نمود.

در محیط و شرایط پروژه های بزرگ و پیچیده، با توجه به عوامل و دلایل مختلفی اعم از انجام فرایندها و فعالیت های متنوع و متعدد توسط افراد درگیر در پروژه با تخصص های مختلف، استفاده از فناوری های جدید، تغییرات شرایط محیطی و عوامل دیگر بروز خطاها، مخاطرات و ریسک های تاثیر گذار که بعضا حوادث تلخ و ناگواری را به بار می آورند امری غیرقابل اجتناب خواهد بود. بنابراین یکی از مشکلات اصلی سازمان ها که در پروژه های طراحی و توسعه محصولات خود با آن مواجه هستند، عدم شناسایی به موقع مخاطرات و خطاهای بالقوه است که امکان دارد در حین طراحی، ساخت و یا حتی در جریان عملیات برای محصول رخ دهد و باعث شکست پروژه و یا تحمیل هزینه های هنگفت به سازمان شود. یکی از مهم ترین مباحث مطرح در حوزه کنترل مخاطرات و شکست ها لزوم توجه به مبحث ایمنی سیستم است و فعالیت ها واقدامات اصلاحی مربوط به آن جزء اقداماتی به شمار می آیند که باید گام به گام همراه با سایر فعالیت های طراحی های مهندسی پیگیری و اجرا شود تا ایمنی به صورت ذاتی در سیستم لحاظ گردد. تجربیات حاصل شده در انجام فعالیت های ایمنی سیستم در برخی سازمان های مشابه نشان می دهد که برای ارتقاء میزان موفقیت یک مدیر ایمنی سیستم جهت مجاب کردن مدیران پروژه و کارشناسان طراحی، برای لحاظ نمودن ملاحظات ایمنی و رعایت موارد مربوطه در حین طراحی ها لازم و ضروری است که در بستر یک رویه استاندارد و هدفمند به اشاعه مفاهیم، تهیه و ابلاغ دستورالعمل های اجباری و تدوین روش های ارزیابی مبادرت ورزید. یکی از معروف ترین و بهترین این بسترها، استاندارد نظامی وزارت دفاع آمریکا می باشد که مبنای استقرار برنامه ایمنی سیستم در بسیاری از سازمان ها می باشد.

مروری بر تاریخچه تغییرات استاندارد نظامی

قبل از دهه ۶۰ میلادی، برنامه های ایمنی براساس فلسفه (بعد از واقعه) یا (رویکرد پرواز- تکمیل- پرواز) به بررسی و کنترل حوادث می پرداختند. واضح است که چنین رویکردی برای بعضی از صنایع خاص از قبیل صنایع هسته ای، موشکی و فضایی مطابق دلایل زیر قابل قبول نبود:

- پیامد حوادث این سازمان ها بسیار وخیم و ناگوار و در بسیاری از موارد فرامنطقه می باشد (نظیر حادثه چرنوبیل).
- این نوع برنامه ها، وابسته به استانداردها، قوانین وکدها بودند که معمولا بعد از حوادث ایجاد شده بودند.

- کار فردی و بیشتر مسئولیت برعهده کارشناس ایمنی می باشد.

در سال ۱۹۶۳، وزارت دفاع آمریکا، رویکرد جدیدی در ارتباط با ایمنی تحت عنوان (طراحی برای ایمنی) را مطرح نمود که با عنوان ایمنی سیستم شناخته می شود. این سازمان ایمنی سیستم را به‌عنوان یکی از توابع طراحی سیستمی در کنار سایر توابع طراحی(هریک از زیرسیستم ها) تعریف نمود. براساس جایگاه تعریف شده، ایمنی سیستم، اطلاعات ورودی از قبیل نقشه های طراحی، دیاگرام های جریان عملکردی، نقشه های عملیاتی و غیره را از سایر توابع طراحی دریافت و بعد از پردازش های لازم جریان خروجی را در قالب لیست مخاطرات و ریسک های شناسایی شده، اقدامات کنترلی مربوط به ریسک های غیرقابل قبول را در اختیار توابع طراحی قرار می دهد.

در سال ۱۹۶۶ وزارت دفاع، اولین نسخه استاندارد ایمنی سیستم را با عنوان std-Mil-۸۸۲ معرفی نمود. این استاندارد به صورت مستقیم مورد بهره‌بردای کشورهایی از قبیل چین، هند، استرالیا، انگلستان و بسیاری از کشورهای اروپایی قرار گرفت و در تهیه و تدوین استانداردها و الزامات ایمنی بسیاری از سازمان ها و صنایع فضایی از قبیل استاندارد ایمنی سیستم ژاپن (JMR -۰۰۱)، سازمان های فضایی اروپا (ECSS-Q-ST-40C) و ناسا (NHB1700.1) مورد استفاده قرار گرفت. این استاندارد تاکنون چندین مرتبه مورد بازنگری قرار گرفته است. جدول زیر روند تغییرات هر نسخه از استاندارد ۸۸۲ را نسبت به ورژن قبلی را نمایش می دهد.

ردیف	نسخه استاندارد	تاریخ بازنگری	روند تغییرات
۱	۸۸۲	۱۹۶۹	فاقد ماتریس ریسک اما سطوح خطر برای آن تعریف شده بود.
۲	۸۸۲-A	۱۹۷۷	فاقد ماتریس ریسک اما سطوح احتمالاتی کیفی خطر و پذیرش ریسک برای آن تعریف شده بود.
۳	۸۸۲-B	۱۹۸۴	تعریف ماتریس کیفی شدت و احتمال خطر، ماتریس تصمیم گیری.
۴	۸۸۲-C	۱۹۹۳	تعریف ماتریس کمی شدت و احتمال خطر، ماتریس تصمیم گیری، تعریف وظایف ۱۰۰،۲۰۰،۳۰۰،۴۰۰
۵	۸۸۲-D	۲۰۰۰	توجه به قراردادها و نوع مالکیت قراردادها، حذف وظایف ۱۰۰،۲۰۰،۳۰۰،۴۰۰
۶	۸۸۲-E	۲۰۱۲	بازگشت به روال تعریف شده برای نسخه C و اضافه نمودن چند فعالیت جدید به وظایف و اضافه نمودن سطح احتمال F به ماتریس احتمال.

MIL-STD-882 (روش استاندارد برای امنیت سیستم)

استفاده از استاندارد امنیتی سیستم MIL-STD-882 به منظور از بین بردن هر چه بیشتر خطرات و به حداقل رساندن خطرات غیر قابل حذف، توسط وزارت دفاع آمریکا طراحی شده است. این استاندارد خطرات مربوط به کلیه زیرساخت ها از جمله سیستم ها، محصولات، تجهیزات و سخت افزار و نرم افزار را در فرآیند های طراحی، توسعه، آزمایش، تولید، استفاده و دفع شامل می شود.

رویه استاندارد MIL-882 به یک رویکرد (یک رویه استاندارد که معمولاً به عنوان سیستم ایمنی شناخته می شود) می پردازد که در مدیریت خطرات ناگوار زیست محیطی، ایمنی و سلامتی که در زمینه های توسعه، آزمایش، تولید، استفاده و دفع سیستم های وزارت دفاع با آن مواجه می شوند، مفید است.

این سند حداقل الزامات اجباری را برای یک برنامه ایمنی سیستم قابل قبول، برای هر سیستم وزارت دفاع مشخص می کند. الزامات امنیتی سیستم، الزامات امنیتی سیستم را در طول چرخه عمر هر سیستم تعریف می کند. این الزامات در صورت اجرای صحیح، شناسایی و مدیریت خطرات مرتبط با آن در طول فعالیت های مهندسی توسعه و نگهداری سیستم می باشد.

فرآیند امنیت سیستم از هشت عنصر تشکیل شده است: مستند سازی رویکرد امنیت سیستم، شناسایی و مستند سازی خطرات، ارزیابی و مستند سازی خطرات، شناسایی و مستند سازی اقدامات کاهش خطر، کاهش خطرات، تأیید و مستند سازی اقدامات کاهش، پذیرش خطرات و مدیریت چرخه حیات خطرات.

الزامات ایمنی سیستم شامل موارد زیر است:

۱. مستندسازی رویکرد امنیت سیستم

رویکرد مهندسی ایمنی سیستم تایید شده توسط توسعه دهنده و مدیر برنامه را مستند کنید.

۲. شناسایی و مستند سازی خطرات

شناسایی خطرات از طریق یک فرآیند تجزیه و تحلیل سیستماتیک خطر؛ شامل تجزیه و تحلیل دقیق سخت افزار و نرم افزار سیستم، محیط (که سیستم در آن وجود خواهد داشت)، و کاربر مورد نظر. داده‌های مخاطرات و حوادث ناگوار گذشته، از جمله تجارب ناشی از سیستم‌های دیگر را در نظر بگیرید و از آن ها استفاده کنید. شناسایی خطرات بر عهده همه اعضای برنامه است. در طول شناسایی خطر، خطراتی را که ممکن است در طول چرخه عمر سیستم رخ دهد، در نظر بگیرید.

۳. ارزیابی خطرات

شدت و احتمال خطر مرتبط با هر خطر شناسایی شده را ارزیابی کنید، به عنوان مثال، تأثیرات منفی احتمالی خطر را بر پرسنل، تأسیسات، تجهیزات، فرایند، مردم و محیط زیست و همچنین بر خود سیستم تعیین کنید.

۴. تعیین اقدامات لازم کاهش خطر

جایگزین های بالقوه کاهش خطر حادثه و اثربخشی قابل قبول برای هر جایگزین را شناسایی کنید. کاهش ریسک یک فرآیند مکرر است که زمانی به اوج خود می رسد که ریسک نامطلوب باقیمانده به سطح قابل قبول کاهش یابد.

۵. اقدامات کاهش خطر حادثه به سطح قابل قبول

از طریق رویکرد کاهشی که مورد توافق دوجانبه توسعه‌دهنده و مدیر برنامه است، خطر تصادف را کاهش دهید.

۶. تأیید کاهش خطر

از طریق تجزیه و تحلیل، آزمایش یا بازرسی مناسب، صحت کاهش خطر حادثه را تأیید کنید. خطر نامطلوب باقیمانده را مستند کنید. تمام خطرات جدید شناسایی شده در طول آزمایش را به مدیر برنامه و توسعه دهنده گزارش دهید.

۷. بررسی خطرات و پذیرش خطرات نامطلوب باقیمانده توسط مسئول مربوطه

به مدیر برنامه درمورد خطرات شناسایی شده و خطرات نامطلوب باقیمانده اطلاع دهید. مدیر برنامه باید اطمینان حاصل کند که خطرات نامطلوب باقیمانده توسط مرجع مناسب پذیرش ریسک بررسی و پذیرفته شده است.

۸. شناسایی و تعیین خطرات موجود، حذف آن ها و خطرات باقیمانده

خطرات موجود، اقدامات لازم جهت حذف آن ها و خطرات باقیمانده را شناسایی کنید و بررسی این موارد را در طول چرخه عمر سیستم، حفظ کنید. مدیر برنامه باید کاربر سیستم را در مورد خطرات موجود و خطرات باقیمانده آگاه کند.

MIL-STD 882BV یک روش ارزیابی ریسک نیمه کمی

روش MIL-STD-882B یکی از طبقه بندهای شدت خطر است که در سال ۱۹۸۴ در استانداردهای نظامی آمریکا ارائه شده در این روش، خطرات از نظر شدت به چهار گروه فاجعه بار، بحرانی، مرزی و جزئی طبقه بندی شده‌اند. هر چند که استاندارد اخیر در ابتدا برای ارزیابی سیستم های نظامی ارائه شده بود ولی امروزه از آن برای طیف وسیعی از صنایع که اصول ایمنی سیستم در آن ها به‌کار گرفته می‌شود نیز استفاده می‌گردد.

شدت خطر (Severity)

نشان دهنده وسعت و دامنه خسارات و تلفاتی است که در صورت بالفعل در آمدن خطر ایجاد می شود. شدت خطر نشان دهنده وسعت و دامنه خسارات و تلفاتی است که در صورت بالفعل در امدن خطر ایجاد خواهد شد. طبقه بندی شدت خطر می تواند براساس تعداد طبقات، نام گذاری آن ها، اهداف و منظور هر طبقه بندی و غیرمتفاوت باشد. برای مثال می توان به طبقه بندی های زیر که توسط سازمان ها و گروه های مختلف ارائه شده است اشاره کرد:

- فاجعه بار، بحرانی، شدید، جدی (طبقه بندی های هیئت ایمنی حمل ونقل ملی آمریکا)
- فاجعه بار، بزرگ، جدی، کوچک (طبقه بندی سازمان هوا فضای ملی آمریکا)
- طبقه ۱، طبقه ۲، طبقه۳، طبقه ۴ (طبقه بندی شورای ایمنی ملی آمریکا)

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

لازم به یادآوری است که علاوه بر تعداد طبقات و نام آن ها، تعاریف هر طبقه نیز ممکن است در کشورها، ایالات و حتی در صنایع مختلف یک کشور بسیار متفاوت هم باشد، این امر به سیاست های ایمنی هر کشور، ایالت و یا صنعت بستگی خواهد داشت.

نوع خطر	طبقه	تعریف
جزئی یا قابل چشم پوشی	۴	جراحات، بیماری های شغلی و آسیب های خیلی کوچک
مرزی یا حاشیه ای	۳	حوادث و بیماری های شغلی جزئی، آسیب های نسبتا کوچک به سیستم
بحرانی	۲	جراحات، بیماری های شغلی شدید، آسیب های شدید به سیستم
فاجعه بار	۱	مرگ و میر یا از بین رفتن سیستم

احتمال وقوع خطر (Probability)

نشان دهنده امکان به وقوع پیوستن یک خطر در یک دوره زمانی معین است.

احتمال خطر	سطح خطر	تعریف
غیر محتمل	E (Improbable)	احتمال آن انقدر کم است که می توان از آن صرفه نظر نمود یا هیچ گاه رخ نمی دهد و غیر محتمل است.
خیلی کم یا بعید	D (Remote)	غیر محتمل است اما امکان دارد و خیلی کم رخ می دهد.
گاه به گاه	C (Occasional)	گاهی اوقات اتفق می افتد.
محتمل	B (Probable)	چندین بار یا غالبا رخ می دهد.
مکرر	A (Frequent)	به طور مکرر اتفاق می افتد.

عدد اولویت ریسک NUMBER PRIORITY RISK

عدد اولویت ریسک حاصل ضرب دو فاکتور شدت و احتمال وقوع است.

برای اعداد ریسک به‌دست آمده در محدوده بالا، باید اقدامات اصلاحی و پیشگیرانه فوری انجام گیرد.

عدد ریسک				
احتمال وقوع	شدت خطر			
	فاجعه بار (۱)	بحرانی (۲)	مرزی (۳)	جزئی (۴)
مکرر (A)	۱A	۲A	۳A	۴A
محتمل (B)	۱B	۲B	۳B	۴B
گاه به گاه (C)	۱C	۲C	۳C	۴C
خیلی کم (D)	۱D	۲D	۳D	۴D
غیر محتمل (E)	۱E	۲E	۳E	۴E

جدول نتیجه گیری	
معیار ریسک	طبقه بندی ریسک
غیر قابل قبول	۱A-۱B-۱C-۲A-۲B-۳A
نامطلوب	۱D-۲C-۲D-۳B-۳C
قابل قبول ولی نیاز به تجدید نظر	۱E-۲E-۳D-۳E-۴A-۴B
سیستم قابل قبول است	۴E-۴D-۴C

سطح ریسک	فعالیت و زمان بندی
غیر قابل قبول	تا زمانیکه ریسک کاهش نیافته کار نباید آغاز شود. حتی اگر با استفاده از تمامی منابع؛ کاهش ریسک امکان پذیر نباشد، فعالیت باید متوقف شود.
نامطلوب	تا زمانیکه ریسک کاهش نیافته کار نباید آغاز شود. منابع قابل توجهی باید جهت کاهش میزان ریسک تخصیص داده شود.
قابل قبول ولی نیاز به تجدید نظر	باید در جهت کاهش ریسک تلاش شود، لذا هزینه های صرف شده به دقت بررسی و محدود شوند. اندازه گیری میزان کاهش ریسک می تواند در دوره های زمانی مشخص انجام شود. زمانی که ریسک متوسط در ارتباط با پیامد های صدمه زای شدید است، باید احتمال وقوع آن ریسک به دقت ارزیابی شده و بر اساس آن نیاز به افزایش و بهبود اندازه گیری های کنترلی بررسی شود.
قابل قبول	کنترل بیشتری نیاز نیست، باید به راه حل مقرون به صرفه توجه شود و همچنین اطمینان حاصل شود که کنترل ها برقرار هستند.

منابع

- https://aldservice.com/Safety/mil-std-882
- http://sunnyday.mit.edu
- https://www.laboratuvar.org
- https://www.hsearya.com
- https://acgih.ir
- file:///F:/hse%206/%D8%A7%D8%B1%D8%B2%DB%8C%D8%A7%D8%A8%DB%8C%20%D8%B1%DB%8C%D8%B3%DA%A9/%D8%A7%D8%B1%D8%B2%DB%8C%D8%A7%D8%A8%DB%8C-%D8%B1%DB%8C%D8%B3%DA%A9.pdf

- file:///C:/Users/Alan%20Computer/Downloads/7941395H16163%20(1).pdf