

روش‌های واکاوی خطر در ایمنی سیستم

Hazard analysis techniques for system safety

نویسنده:

کلifton اریکسون

Clifton Ericson

مترجمین:

دکتر شیرازه ارقامی

(استادیار دانشگاه علوم پزشکی زنجان)

دکتر بحیی خسروی

(عضو هیئت علمی دانشگاه علوم پزشکی البرز)

مهندس محمدرضا حسن بیگی

(کارشناس ارشد بهداشت حرفه‌ای)

مهندس میردآود سیدی

(کارشناس ارشد بهداشت حرفه‌ای)

سرشناسه: اریکسون، کلیفتون Ericson, Clifton A

عنوان و نام پدیدآور: روش‌های واکاوی خطر در ایمنی سیستم/ نویسنده: کلیفتون اریکسون؛ مترجمین: دکتر شیرازه ارقامی - دکتر یحیی خسروی - مهندس محمدرضا حسن بیگی - مهندس میرداود سیدی
مشخصات نشر: تهران، سپاه پاسداران انقلاب اسلامی، قرارگاه سازندگی خاتم‌الانبیاء (ص)، قرب نوح (ع)، ۱۳۹۲
مشخصات ظاهری: ۶۳۶ ص.

شابک: ۹۷۸-۶۰۰-۵۹۷۴-۴۴-۷

وضعیت فهرست نویسی: فیبا

یادداشت: عنوان اصلی: Hazard analysis techniques for system safety, c 2005

موضوع: ایمنی صنعتی - داده‌پردازی - ایمنی سیستم‌ها

رده‌بندی کنگره: ۱۲۹۲۹۴/الف۵ T

رده بندی دیویی: ۶۲۰/۸۶

شماره کتاب‌شناسی ملی: ۳۳۲۱۴۹۰

نام کتاب: روش‌های واکاوی خطر در ایمنی سیستم

پدیدآور: Clifton Ericson

مترجمین: دکتر شیرازه ارقامی - دکتر یحیی خسروی - مهندس محمدرضا حسن بیگی - مهندس میرداود سیدی
ناشر: قرارگاه سازندگی خاتم‌الانبیاء (ص)، قرب نوح (ع).

ویراستاری فنی: دکتر غلامحسین پورتنی، دکتر محمد سالم، دکتر فیروز ولی پور، مهندس حامد صادقی علوی

نوبت چاپ: اول

تیراژ: ۱۰۰۰ نسخه

تاریخ انتشار: ۱۳۹۲

بهاء: ۲۵۰۰۰۰ ریال

کلیه حقوق اعم از چاپ و تکثیر، نسخه‌برداری و سایر موارد

برای مرکز مطالعات و پژوهش‌های معاونت ایمنی و اقدامات تأیینی سپاه پاسداران انقلاب اسلامی محفوظ است
(نقل مطالب با ذکر مأخذ بلامانع است).

تهران - ستاد کل سپاه پاسداران انقلاب اسلامی - معاونت ایمنی و اقدامات تأیینی - مرکز مطالعات و پژوهش‌های ایمنی و اقدامات تأیینی

ایمنی در مفهوم جامع آن در فرهنگ متعالی اسلام به عنوان یک ارزش مطرح شده و با تعبیرات لطیفی مانند برترین نعمت ها، نعمت قدر ناشناخته و از نظر دور مانده، نعمتی که بدون آن خیری در زندگی نیست، نعمتی که آدمی از شکر آن عاجز است، حسنه دنیا، دارایی مخفی، سرمایه زندگی و ده ها عنوان دیگر ذکر شده است.

لذا جامعه اسلامی با توجه به غنای فرهنگی و آموزه های دینی می بایست نسبت به جوامع دیگر از سطح ایمنی بالاتری برخوردار باشد و در این همین جهت، سپاه پاسداران انقلاب اسلامی به عنوان یک سازمان پیشرو برای ایمنی نقش و مأموریت عظیم و الهی خود، باید از آمادگی عملیاتی در سطحی عالی و مطلوب برخوردار باشد و برای تحقق این آمادگی، باید ایمنی در مفهوم جامع و پایدار خود تحقق یابد.

بر همین اساس سپاه پاسداران انقلاب اسلامی، سرمایه گذاری در حوزه ایمنی را یک پس انداز و ذخیره سازی برای آینده تلقی می کند و آن را اقدامی لازم برای ارتقاء و افزایش توان دفاعی می داند. لذا حفظ و ارتقاء ایمنی در سازمان سپاه به عنوان یک تکلیف تلقی می شود.

در جهت انجام این تکلیف و در جریان استقرار موثر فرایند ایمنی، یکی از وظایف مهم سازمان، ایجاد بستری مناسب جهت جلب مشارکت و ایجاد انگیزه برای آحاد عناصر انسانی خویش است. در همین راستا و با هدف تعمیم و سوق دادن اطلاعات و دانش موجود در جهت رشد و ارتقای آمادگی های لازم در حوزه ایمنی و برطرف نمودن عیوب عمده و همچنین تقویت فرهنگ ایمنی سازمان سپاه این کتاب تهیه شده است.

در این کتاب سعی شده است مجموعه ای از مطالب پیرامون مبحث واکاوی خطر در اختیار افراد قرار گیرد تا با درک کاربردهای این علم نیازمندی های یگان خود را شناسایی، ارزیابی و در پیامد آن سعی در رفع آن بنمایند.

مرکز مطالعات و پژوهش های معاونت ایمنی و اقدامات تأیینی سپاه پاسداران انقلاب اسلامی

فهرست مطالب

عنوان

صفحه

فصل ۱: ایمنی سیستم.....	۱۰
فصل ۲: خطرات، حوادث و ریسک.....	۲۶
فصل ۳: روش‌ها و فنون واکاوی خطر.....	۵۰
فصل ۴: فهرست مقدماتی خطر.....	۸۲
فصل ۵: واکاوی مقدماتی خطر.....	۱۰۶
فصل ۶: واکاوی خطرات زیرسیستم.....	۱۳۲
فصل ۷: واکاوی خطر سیستم.....	۱۵۶
فصل ۸: واکاوی خطر عملیات و پشتیبانی.....	۱۷۶
فصل ۹: ارزیابی خطرات مربوط به سلامت افراد.....	۲۰۶
فصل ۱۰: واکاوی الزامات یا معیارهای ایمنی.....	۲۲۲
فصل ۱۱: واکاوی درخت خطا.....	۲۳۶
فصل ۱۲: واکاوی درخت واقعه.....	۲۸۸
فصل ۱۳: واکاوی حالت شکست و اثرات آن.....	۳۰۴
فصل ۱۴: واکاوی خطرات مربوط به نقص.....	۳۳۴
فصل ۱۵: واکاوی خطر هنگام کارکرد.....	۳۴۶
فصل ۱۶: واکاوی مدارهای پنهان.....	۳۶۸
فصل ۱۷: واکاوی شبکه پتری.....	۳۸۸
فصل ۱۸: واکاوی مارکوف.....	۴۰۲
فصل ۱۹: واکاوی حفاظ.....	۴۲۶

فصل ۲۰: واکاوی بین خمیده	۴۴۸
فصل ۲۱: واکاوی خطر و توانایی عملیات	۴۶۲
فصل ۲۲: واکاوی علت - پیامد	۴۸۳
فصل ۲۳: واکاوی شکست با علت مشترک	۵۰۱
فصل ۲۴: واکاوی درخت ریسک چشم‌پوشی مدیریت	۵۲۷
فصل ۲۵: ارزیابی ایمنی نرم‌افزار	۵۴۷
فصل ۲۶: خلاصه	۵۶۸

پیوست‌ها

پیوست الف: فهرست واژه‌های اختصاری	۵۷۸
پیوست ب: واژه‌نامه	۵۸۵
پیوست پ: فهرست‌های بازبینی خطرات	۶۱۳

پیشگفتار نویسنده

در طول ۴۰ سال کار در زمینه ایمنی سیستم، دو موضوع درباره واکاوی خطر همواره مرا رنج داده است. نخست، نبود تعریف رسمی و قطعی برای نظریه خطر به گونه‌ای که بتواند اجزاء خطر و فرایند تبدیل خطر به حادثه را توصیف کند. دوم، نبود منابع مناسب برای تعریف دقیق و جزء به جزء چگونگی انجام روش‌ها و فن‌های مورد استفاده در رابطه با خطرات. این مشکلات مرا بر آن داشت که کتاب پیش روی را برای مهندسان ایمنی سیستم و کارورزان به رشته تحریر درآوردم. مطالب این کتاب برای افراد حرفه‌ای و باتجربه و نیز برای واکاوگران تازه کار کاربرپذیر است.

یکی از مهم‌ترین ویژگی‌های این کتاب، توصیف کامل نظریه خطر و ارتباط خطر-ریسک- حادثه است. به بیان دیگر، سه جزء اصلی خطر همراه با مدل مثلث خطر در این کتاب عرضه شده است.

از دیگر جنبه‌های مهم این کتاب آن است که ۲۲ تکنیک از رایج‌ترین روش‌های مورد استفاده در واکاوی ایمنی سیستم را ارائه می‌دهد و برای هر یک، فصلی جداگانه اختصاص یافته است. افزون بر این، به منظور یکسان‌سازی و ایجاد همسانی در پاسخ‌گویی به پرسش‌های رایج در رابطه با انواع روش‌های واکاوی همه فصل‌های مربوط به روش‌شناسی‌ها در قالب‌هایی همانند ارائه شده‌اند. همچنین، به منظور کمک به یادگیری و فهم این روش‌ها، در هر فصل نمونه‌هایی با جزئیات ارائه شده است.

ایمنی سیستم، رشته‌ای است مهندسی که همراه با گسترش سیستم به شناخت خطر و سپس حذف و یا کاهش آن می‌پردازد تا ریسک بروز حوادث و اتفاقات ناگوار را حذف کرده یا کاهش دهد. از آنجایی که این رشته در نهایت با نجات و حفظ جان افراد سروکار دارد، بزرگترین آرزوی من آن است که مخاطبان این کتاب بتوانند مطالب آن را برای درک بهتر از ساخت و واکاوی خطرات به کار برند تا به طراحی و ساخت سیستم‌هایی ایمن کمک شود و از جان افراد حفاظت شود.

کلیفتون اریکسون

هرملتی که زبان خود را فراموش کند تاریخ خود را
گم کرده و عظمت خویش را از دست داده است و برای
همیشه در بندگی و اسارت باقی خواهد ماند.
سیدجمال‌الدین اسدآبادی

پیشگفتار برگردانندگان

اگر نگوئیم بقاء زندگی بشر، بی‌تردید باید گفت رفاه زندگی بشر در گرو فعالیت‌های صنعتی و تولیدی است. اما همراه با به خدمت درآوردن فناوریهای نوین، انسان با خطرات بیشتر و جدیدتر روبه‌رو شده است. بنابراین سازمان‌های بشرو به رویکرد شناسایی و واکاوی خطرات روی آورده‌اند. این رویکرد، توان مدیریت ایمنی را برای کشف خطرات افزایش می‌دهد. در نتیجه، بودجه و امکانات به گونه‌ای مصرف خواهد شد که زیان‌ها به شکلی معقول کنترل شود.

کنترل موثر خطرات نیازمند واکاوی نظام‌یافته، فراگیر و کاربرپذیر است. در دنیای واقعی، متخصص ایمنی / بهداشت حرفه‌ای باید سه نکته را دریابد. نخست اینکه شماری از خطرات، نسبت به برخی دیگر، در درجه‌ای بالاتر از اهمیت قرار دارند. دوم اینکه منابع و امکانات محدود است و هرگز نیروی انسانی و مالی کافی برای کنترل همه خطرات در دسترس نیست. سوم اینکه در صورتی می‌توان بهترین شرایط برای کارگران، کارفرمایان و جامعه را فراهم آورد که منابع در دسترس، به گونه‌ای موثر و اقتصادی برای کنترل خطرات به کار گرفته شود. مسئولیت متخصص ایمنی و بهداشت حرفه‌ای این است که با استفاده موثر از منابع و بر اساس اولویت‌بندی تلاش کند تا خطرات حذف یا کنترل شوند.

تاکنون چندین کتاب در زمینه واکاوی ریسک به زبان فارسی چاپ شده است، اما در غالب آنها فنون واکاوی به صورت جزایر پراکنده و بی ارتباط به یکدیگر و نیز به دور از بحث های نظری و علمی بیان شده و مثال های عملی نیز در این کتاب ها از قوام کافی برخوردار نمی باشد. کتاب Hazard Analysis Techniques For System Safety از چنین نقص هایی به دور است. در این کتاب نه تنها جنبه های نظری و بنیادین مطرح شده است، بلکه نمونه های عملی آن حاصل تجربیات چندین دهه تلاش نویسنده در عرصه واکاوی خطر است. به همین دلیل بر آن شدیم تا این کتاب به زبان فارسی برگردانده شود و از این راه کارشناسان ایمنی و بهداشت حرفه ای را در اجرای هرچه بهتر مسئولیت هایشان یاری رسانیم. به گونه ای که این متخصصان پس از شناسایی خطرات بتوانند ریسک مربوط به این خطرات را برآورد و ارزیابی کرده و درباره پذیرش ریسک های سازمان خود تصمیم گیری کنند و در نهایت امکان مدیریت درست و مناسب ریسک های سازمان خود را با توجه به محدودیت های مالی، انسانی و فنی فراهم آورند.

از ویژگی های مربوط به ترجمه حاضر آن است که دست کم چند فصل از کتاب پیش از آنکه آماده چاپ گردد، چندین بار در کلاس های دانشگاه تدریس شده و نیز به صورت عملیاتی در ارزیابی ریسک محیط های شغلی گوناگون به کار رفته است. همچنین خاطرنشان می گردد که ضمن تلاش برای امانت داری متن، نهایت کوشش برای درک پذیری محتوا به کار گرفته شده است.

بنابراین مطالعه این کتاب می تواند برای مدیران صنایع در راستای آشنایی آنها با فنون اختصاص منابع مبتنی بر ریسک، متخصصان فرایند و مهندسی صنایع برای آشنایی آن ها با ملاحظات ایمنی در فرایند طرح ریزی سیستم و الزامات ارتقاء اعتمادپذیری سیستم و در نهایت متخصصان ایمنی، بهداشت حرفه ای و ارگونومی به منظور به کارگیری روش ها و فنون اعتمادپذیر در فرایند شناسایی خطرات، ارزیابی و مدیریت ریسک کمک شایانی ارائه کند.

دکتر شیرازه ارقامی

دکتر یحیی خسروی

مهندس محمدرضا حسن بیگی

مهندس میردواد سیدی

فصل ۱

ایمنی سیستم

برگرداننده: دکتر شیرازه ارقامی

۱-۱ مقدمه

ما در دنیایی زندگی می‌کنیم که سیستم‌ها و ریسک‌ها آن را فرا گرفته‌اند. از دیدگاه مهندسی، غالب جنبه‌های زندگی به شکل سیستم است برای نمونه، خاک یک سیستم است، خودرو نوعی سیستم دیگر و شبکه‌های خطوط انتقال برق نیز شکلی دیگر از سیستم هستند. هواپیماهای تجاری سیستم‌هایی هستند که در حوزه سیستم اقتصاد، ترابری و سیستم کنترل پرواز جهانی فعالیت می‌کنند. به این ترتیب در می‌یابیم که در زندگی امروزی وجود سیستم‌ها ضروری است.

همگام با سیستم‌ها و کاربرد فن‌آوری، در معرض حوادث نیز قرار می‌گیریم. زیرا، هر سیستمی ممکن است دچار نقص شود و درست کار نکند. در نتیجه، خسارت، آسیب بدنی و مرگ رخ می‌دهد. احتمال آنکه یک سیستم درست کار نکند و موجب بروز مرگ یا آسیب بدنی و خسارت شود، «ریسک حادثه» نامیده می‌شود. برای نمونه، هنگامی که خطر نقص در کارکرد چراغ راهنمایی وجود دارد، ممکن است خودرویی با خودروی شما برخورد کند. خودروها، ترافیک و چراغ‌های راهنمایی، سیستم واحدی را تشکیل می‌دهند که ما هر روز