الگوی دسته بندی انواع خطاهای انسانی بر اساس مدل‌های قابلیت اطمینان انسان

رقیه رمضانی
مهدی کرباسیان
مهسا قندهاری

تاریخ دریافت: ۹۱/۱۱/۲۶
تاریخ پذیرش: ۹۲/۱/۲۵

چکیده:

گسترش پیچیدگی های فناوری موجب فراتر رفتن مسئولیت مدیران از بهبود توان تولید به توان رویارویی با بحران های مختلف شده است. بررسی حوادث در صنایع،نشانگر این است که خطای انسان دلیل اصلی بسیاری از حوادث به شمار می رود. به عبارت دیگر، انسان نقش اساسی در افزایش یا کاهش ایمنی و قابلیت اطمینان سامانه ایفا می کند و درطی همه ی مراحل عملکرد یعنی نگهداری، تست و پاسخ به رویدادهای مختلف، تعاملات زیادی با ماشین دارد. تعاملات بین انسان وماشین می تواند با انجام اقدامات کنترلی وبهینه سازی، منجر به کاهش اثر رویدادهای ناگوار شود. یابرعکس، این تعاملات می تواند در نتیجه ی خطای فرد منجر به رخداد رویدادهای خطرناک شود . با بررسی دلایل ریشه ای وقوع خطای انسانی، توجه به عوامل انسانی نیز اهمیت یافته است و امروزه حتی روش هایی وجود دارند که به صورت کمی وکیفی میزان احتمال وقوع و تاثیر خطاهای انسانی در قابلیت اطمینان و ایمنی سامانه را تحلیل می کنند که به آنها قابلیت اطمینان افراد گفته می شود. در این تحقیق خطاهای انسانی ریشه یابی و به سه دسته‌ی فردی، تیمی و محیطی تقسیم بندی شده و مدلی کلی ازخطاهای انسانی ارایه گردیده است. این مدل می تواند با استفاده از داده های کمی برای محاسبه‌ی قابلیت اطمینان استفاده شود.

واژه های کلیدی:
خطای انسانی، قابلیت اطمینان انسان، دسته بندی خطا

۱) مقدمه

صنعتی شدن جوامع، گسترش ارتباطات و بزرگتر شدن سازمان های اجتماعی که همراه با موفقیت های فراوان فناورانه و اجتماعی بوده است، نه تنها میزان بروز خطرات غیرمنتظره را کاهش نداده است، بلکه در بسیاری موارد افزایش خطر را نیز به داشته است. از این رو، سازمان ها موظفند، همراه با افزایش پیچیدگی و توان تولیدی خود، توان مواجهه با بحران های مختلف را بااستفاده از فن های به موقع و هوشمندانه افزایش دهند. شناخت چرایی و چگونگی این حوادث، به منظور پیشگیری از وقوع مجدد آنها، جایگاه حیاتی در بالا بردن قابلیت اطمینان سامانه، میزان تولید، کیفیت محصول و بهره وری سازمان دارد.

تحقیقات اخیر، علت اصلی بسیاری از حوادث را، خطای انسانی گزارش کرده اند. طبق آمار ارایه شده، خطای انسان مهم ترین عامل صدمات وار دشده به کارکنان و ضررهای مالی در صنایع شیمیایی است (مختاری،۹۰) .

با پیشرفت فناوری و پیچیده شدن سامانه ها، مهندسان طراح همواره در پی جلوگیری از وقوع خرابی در سامانه‌ها و تجهیزات بوده اند. در دوره های قبل، تفکر بنیادی بر این بود که با بهبود طراحی و افزایش قابلیت اطمینان سخت افزاری سامانه ها و تجهیزات تأثیرگذار در ایمنی می توان از بروز حوادث جلوگیری کرد. اما به رغم تلاش‌های به عمل آمده در طول چند دهه گذشته، شاهد وقوع حوادث غم انگیز با پیامدهای سنگین جانی، اقتصادی و سیاسی، در سامانه‌های پیچیده ی فناورانه نظیر نیروگاه های هسته ای، تأسیسات شیمیایی و صنایع هوایی بوده ایم که

نشان می‌دهد برای جلوگیری از وقوع حوادث، تمهیدات مهندسی به تنهایی کافی نیست. نتایج تحقیقات در زمینه ی ریشه‌یابی حوادث در صنایع بزرگ نشان دهنده جایگاه اساسی عوامل انسانی و سازمانی در بروز حوادث است. اگرچه هدف اصلی سرزنش مسئولان در پی وقوع حوادث نیروهای انسانی هستند، تحقیقات نشان می دهد علاوه بر خطاهای انسانی، عواملی نظیر عدم توجه به چگونگی تقابل انسان و سامانه در طراحی، ضعف های مدیران در اتخاذ تصمیمات کلیدی، ضعف در برنامه ریزی، عدم آموزش کافی کارکنان، روش‌های نامناسب مدیریتی، ساختارهای سازمانی نامناسب و ضعف فرهنگی ایمنی در زمان های مختلف عمر هر سامانه بزرگ صنعتی می تواند وقوع حوادث را تشدید کند. از آنجا که عوامل انسانی و سازمانی در مقایسه با خرابی های سخت افزاری ناشناخته‌تر و از پیچیدگی بیشتری برخوردار است، روش های معمول شناسایی اشکالات پاسخگو نیست و باید از روش های دیگری برای شناسایی و رفع آنها استفاده کرد.

به کار گرفتن نتایج تحلیل عوامل انسانی در مرحله طراحی یکی از عوامل مؤثر در کاهش وقوع خطاست. این تحلیل‌ها با در نظر گرفتن نکات قوت و نقاط قابل بهبود افراد، محدودیت های موجود چه در قالب سازمانی و چه فردی، نیازهای سازمان، توانایی های کارکنان برای برآورده سازی نیازها، استفاده از تجربیات قبلی و توجه به عوامل سازمانی مؤثر در رفتار کارکنان با هدف شناسایی فرصت های بهبود به عنوان عواملی برای افزایش بازدهی انجام می شوند. (هسو وهمکاران، ۲۰۰۸ و پیپودولس و همکاران، ۲۰۰۹)

۲) پیشینه ی تحقیق

تاریخچه ی قابلیت اطمینان و خطا به بعد از سال ۱۹۵۰ بر می گردد، یعنی هنگامی که دانشمندان مدعی شدند که قابلیت اطمینان عناصر انسانی باید شامل پیش بینی ومحاسبه‌ی قابلیت اطمینان سامانه باشد. ازطرفی، قابلیت اطمینان محاسبه شده‌ی سامانه ها، تصویر واقعی را مجسم نمی‌کرد (ویلیام، ۱۹۵۸). دیهیلون(۱۹۸۶) وکریستنس هاوارد(۱۹۸۱)، دلایل متفاوتی را برای علت وقوع خطای انسانی در نگهداری ومسائل اساسی نیروی انسانی ارایه کردند که عبارتند از پیچیده بودن وظایف نگهداری، ابزار کاری ناکافی و معیوب، طراحی ضعیف تجهیزات، رویه نگهداری با محتوای ضعیف، طرح بندی ضعیف کاری، دستورالعمل نگهداری منسوخ و قدیمی، خستگی پرسنل، محیط کار نامناسب (مانند روشنایی، رطوبت، دما و ....)، تمرین وآموزش ناکافی. درسال۱۹۹۶ نیز تحلیل قابلیت اطمینان پرسنل حمل ونقل راه آهن انجام گرفت و بدین صورت احتمال خطای انسانی برای اندازه گیری عملکرد قابلیت اطمینان نیروی انسانی بیان شد و به دنبال آن احتمال وقوع برخی خطاهای انسانی برآورد زده شد. این تحلیل نشان می داد که یکی ازعوامل تاثیرگذار برعملکرد انسان، استرس می باشد. بر این اساس مدل ساده تاثیر سطوح استرس بر احتمال خطای انسانی پیشنهادشد. (النکا، ۱۹۹۶) رایت و باسول(۲۰۰۲) سطوح تحلیل خطا را به سطح فردی وسازمانی و مدیریت قابلیت اطمینان انسان را به دونوع واحد وچندگانه تقسیم کردند که در جدول شماره ۱ نشان داده شده است.

واحد	شیوه های HRM[1] چندگانه		
توابع مجزا، مانند اهداف پژوهش در نمایش دادن یک رابطه بین ناحیه کارکردی مخصوص با عملکرد ثابت	بیان روابط صنعتی HRM در مورد عملکرد بالای سامانه ها	سازمانی	**سطوح تحلیل**
بیان رابطه HRM کارکردی/سنتی با روانشناسی سازمانی/صنعتی	بیان رابطه‌ی اشتغال قراردادی باتوجه به جنبه های روانشناسی	فردی	

جدول شماره ۱. طبقه بندی سطوح تحلیل خطا (رایت و باسول،۲۰۰۲)

1. human reliability management

چایودو و دیگران، ۲۰۰۴ درمقاله خود با نشان دادن ارتباط بین عدم اطمینان و دانش انسان برای کنترل فرایندها، مدل جدیدی برای نشان دادن نرخ خطای انسانی بیان کردند. این مدل براساس نرخ خرابی با پارامترهای مقیاس تصادفی برای توزیع های لگ-نرمال[1] وگاما[2] وگوس معکوس[3] با شرایط وایبال[4] ارایه شده است. بدین صورت که، با در نظر گرفتن نرخ خرابی و با استفاده ازاین توزیع ها می توان خطاهای انسانی را کمّی کرده و قابلیت اطمینان انسان را محاسبه کرد. لیو و دیهیلون(۲۰۰۶)، درمقاله خود ادبیات موضوعی قابلیت اطمینان نیروی انسانی و خطاهای نگهداری را جمع آوری نمودند.

اولیور استراتر در سال ۲۰۰۴ در مقاله‌ای با عنوان "توجه به عناصر کمی‌سازی قابلیت اطمینان انسان" تا حدودی به این مسئله پرداخته است که اصطلاح داده چه معنایی دارد و چگونه می‌توان دید کیفی را به دید کمی تبدیل کرد. او بیان کرده است که اصطلاح داده کمی و داده کیفی تفاوتی با یکدیگر ندارند اما در گستره‌ای کامل تر و در فرآیند HRA تفاوت این دو(داده کمّی و کیفی) موثر می‌باشد. او در این مقاله، به دقت، منطق پشت شکل های مختلف کمی‌سازی قابلیت اطمینان را شرح داده است و یک راه علمی برای تعیین داده‌های بهتر برای ارزیابی قابلیت اطمینان انسان پیشنهاد کرده است (استراتر،۲۰۰۴) .

دیهیلون، ۲۰۰۷، درکتاب خود با عنوان "قابلیت اطمینان پایه و مفهوم خطا" دربحث تحلیل سامانه های انسان-ماشین تحلیل سامانه های ماشینی را که وابسته به کاهش تاثیر خطاهای انسانی است، در پنج گام بیان کرده است که عبارتند از تعریف اهداف سامانه و توابع وابسته به آن، تعریف مشخصه های مناسب و عامل های شکل‌دهی عملکرد مانند کیفیت، روشنایی ، مشخص نمودن سطح ویژگی های فردی پرسنل مانند (مهارت ،تجربه، انگیزش وآموزش)، تعریف وظایف انجام شده متناسب با پرسنل، تحلیل مشاغل برای معرفی شرایط احتمالی خطا ودیگرمشکلات اتفاقی.

درسال ۲۰۰۷ روشی به نام AHP-SLIM[5] ارایه شد که برای غلبه بر مشکلات بوجود آمده از داده های تجربی وابسته به قضاوت کارشناسان هر رشته وهمچنین برای بدست آوردن برآورد درست و صحیح پیشنهاد شد. این روش نوعی از برآوردHEP[6] (احتمال خطای انسانی) با استفاده از AHP (تحلیل سلسله مراتبی) است (جی این لی ,۲۰۰۷) . در سال ۲۰۰۹ ، دکر و می، در مطالعه ای که انجام دادند، آموزش را به عنوان کلید پیش گیری از بسیاری از خطاها معرفی کردند و پیام اصلی آن این است که خطای انسان دلیل عمده حوادث و شکست ها تلقی می‌شود و آموزش راهی مناسب برای پیش گیری از خطاهای غیر عمد انسانی است.

نیاز به برآورد قابلیت اطمینان انسان در بیشتر صنایع مانند هسته ای، فضایی و ... احساس می شود. در رشته مدیریت آمد و شد هوایی تحلیل قابلیت انسان با داده های خطای انسانی بیان شد که به شکل احتمال خطای انسانی برای اولین مرحله در نظرگرفته شد و احتمال خطای انسانی باتحلیل نتایج شبیه سازی زمان واقعی شامل کنترل کننده های حمل ونقل هوایی با تمرکز برخطاهای مرتبط بدست آمد (باری کروان، ۲۰۰۸)، بسیاری حالات نشان می‌دهد که ساختار شکست ممکن است باعث خطای کلی و در نتیجه خطای انسانی شود و این در اصل، برای تحلیل خطای انسانی است. تحلیل خطای انسانی (HEA)[7]، می‌تواند علل وقوع احتمال خطای انسانی(HEP) رادر ساختاری به روش AHP برآورد کند. که این مدل روشAHP-FLIM[8] رابیان می کند که در مدل می توان تاثیر قضاوت کارشناسان را بررسی کرد (ژو چونگ،۲۰۱۰) . سانکاران ماهدوران و دیگران (۲۰۱۱) اثر خستگی را بر عملکرد انسانی به عنوان عامل مهم دربسیاری تصادفات بیان کردند ولی اندازه گیری آن به آسانی امکانپذیر نیست و مشکلاتی مانند تاثیرات خستگی بر PRA (برآورد احتمال ریسک) درسامانه را ایجاد می کند. در این مقاله، تاثیر خستگی برعملکرد ومشکلات وابسته به تعریف و اندازه‌گیری خستگی بررسی شده است و جهت گیری های آینده و چالش های آن به ویژه کمبود استراحت را تشریح می کند.

1. Log-normal
2. Gamma
3. Inverse Gouse
4. weibull
5. Analytic hierarchy process-Success likelihood index method
6. Human error probability
7. Human error analysis
8. Analytic hierarchy process-fault likelihood index method

سایمون فرنچ و همکارانش در سال ۲۰۱۱ یک مقاله انتقادی و مروری برای مدیران سازمان‌ها در زمینه تحلیل‌های قابلیت اطمینان انسان ارایه کردند. آنها در این مقاله روش‌های HRA را مرور و راجع به آنها بحث کردند و به مدیران توصیه کردند که قبل از توسعه و پژوهش‌های بعدی شان یک سری ملاحظات را قبل از اینکه نیازمند تحلیل قابلیت اطمینان و ریسک‌های مدرن شوند، در نظر بگیرند و چگونه ایمنی سامانه‌های پیچیده را مدیریت کنند و همچنین پیشنهاداتی ارایه کردند که چگونه مدیران بتوانند در چنین سامانه‌های پیچیده‌ای کار خود را با توجه به ایمنی سامانه، توسعه دهند(سایمون فرنچ و همکاران،۲۰۱۱).

لی پنگ و دیگران(۲۰۱۲) بااستفاده از فن BN[1] فازی روشی را برای پیشرفت کمی سازی تاثیرات سازمان ها در HRA، بیان کردند که نتایج حاصله نشان داد این مدل به تنهایی نمی تواند رابطه‌ی بین عامل های انسانی و قابلیت اطمینان انسان را کمی کند ولی می تواند قابلیت اطمینان تجهیزات انسانی را اندازه گیری کرده و علل خطا را مشخص کند و یا علت خطاهای انسانی را اولویت بندی کند. همچنین، ژی کیوانگ، (۲۰۱۲) در مقاله ای با عنوان "برآورد احتمال خطای انسانی با استفاده از روش تحلیل خطای اطمینان شناختی CREAM[2]"، ابتدا درجه ای از کنترل را به چهار روش بیان کرد که باتوجه به زمینه مورد نظر به شرایط عملکرد رایج بستگی دارد و سپس رابطه‌ی بین کنترل و بازه های HEP را برآوردکرد و این روش را به عنوان مبنایی برای برآورد نقطه HEP اجرا کرد. سپس مشخصه های روش را جمع آوری کرد که نشان می داد نتایج حاصل با داده های عملکرد انسانی ثبت شده مطابقت دارد.

مهر آرا مولان و اله یاری نیک درمقاله‌ای ترکیبی از روش‌های ارزیابی و مدیریت ریسک کنش گرایانه، واکنش‌پذیر و تعاملی و دو ابزار ارزیابی و مدیریت ریسک شامل سامانه کیفی ارزیابی مدیریت کیفیت و سامانه کمی تحلیل ریسک را به کار گرفتند. کاربرد سامانه ارزیابی مدیریت کیفیت برای بررسی عامل های عملکرد سازمانی و بشری است که به عنوان ورودی برای استفاده در سامانه کمی تحلیل ریسک به کار می‌رود. در این پژوهش، یک زیرساختار بین‌المللی از سازه‌های فراساحلی که کالاها و خدمات مورد نیاز را عرضه کرده اند تا شرکت‌ها، خدمت‌رسانی لازم را انجام دهند، مورد بررسی قرار گرفته است. عامل های بشری و سازمانی چالش اصلی در توسعه سامانه‌های سازه‌ای فراساحلی هستند که بر قابلیت اطمینان و کیفیتی مطلوب اثر می‌گذارند. همچنین واضح است که تلاش اصلی پیکره دانش مدیریت و ارزیابی قابلیت اطمینان، رفع این چالش و انجام خردمندانه و صحیح این دانش به شکل پیوسته و همیشگی است(مهر آرا مولان و اله یاری نیک،۱۳۹۱) .

هادی شعبانی و صمد نجفی مجد در سال ۱۳۹۰ مقاله‌ای ارایه کردند که هدف آن بررسی خطای انسانی در بین کارکنان مدیریت طراحی سامانه یکی از صنایع دفاعی بود. جمع‌آوری داده‌ها و اطلاعات در آن پژوهش با استفاده از روش مشاهده و مصاحبه صورت گرفت و سپس تحلیل شغلی وظایف توسط فن HTA، انجام شد و برای شناخت احتمال رخداد خطا در آن وظایف از فن HEART استفاده شد (هادی شعبانی و صمد نجفی مجد، ۱۳۹۰) .

فرهاد آل علی در سال ۱۳۹۰ مقاله‌ای ارایه کرد با عنوان عوامل انسانی اثر گذار بر قابلیت اطمینان و ایمنی در طراحی که در آن عوامل انسانی موثر بر قابلیت اطمینان که در حوزه ارگونومی و عامل های انسانی مطرح می‌گردد، مورد تجزیه و تحلیل قرار گرفته و فن‌های ارزیابی و تحلیل قابلیت اطمینان مربوط به عوامل انسانی معرفی شده است. وی در پایان به بررسی خطاهای انسانی و چگونگی تجزیه و تحلیل و طبقه‌بندی آنها به عنوان کلیدهای شناخت مشکلات ناشی از عوامل تاثیر گذار بر قابلیت اطمینان در حوزه عوامل انسانی برای طراحی محصولات صنعتی و طراحی سامانه‌ها پرداخته است. (فرهاد آل علی، ۱۳۹۰)

محمد امین موعودی و سیده مریم قربانی در سال ۱۳۹۰ به منظور پیش‌بینی و تجزیه و تحلیل خطای انسانی در اتاق کنترل مرکزی، بخش پخت کلینکر و راهبری کوره، یک مطالعه مورد پژوهی کمی انجام دادند و عوامل موثر بر عملکرد انسان را شناسایی کرده و در نهایت با استفاده از

1. Bayesian network
2. cognitive reliability error analysis method

رویداد THERP میزان خطای انسان و یا میزان خطای تجهیزات که در خطای انسان موثر هستند را به صورت احتمال خطای انسانی ارایه کردند. این فن که به منظور پیش بینی و تجزیه و تحلیل خطای انسانی است، در ابتدا باید با کمک سرپرست شیفت و مشاهده مستقیم فعالیت کارورها، مطالعه کل وظایف و کل زیر وظایف کارور هنگام کار، شناسایی شده و در قالب فلوچارت HTA(تجزیه و تحلیل سلسله مراتبی) ارایه گردد، و سپس رویدادهای مهم شناسایی شده و اطلاعات حاصل در قالب نمودار درختی رویداد THERP نمایش داده شود و میزان خطای تجهیزات که در خطای کارور موثر هستند به صورت درخت احتمال HEP ارایه شود(محمد امین موعودی و سیده مریم قربانی، ۱۳۹۰).

دراین مقاله، با توجه به اهمیت خطا ونقش انسان در بروز آن، سعی شده است مدلی کلی و جامع از انواع خطاهای انسانی در دسته بندی مشخص ارایه گردد. این مدل با در نظرگرفتن علل بروز خطاها می تواند با شناسایی نقاط ضعف، باعث کاهش خطا و یا اصلاح آن گردد.

۳) ارایه‌ی مدل خطاهای انسانی برای برآورد قابلیت اطمینان انسان

در این تحقیق به بررسی خطاهای انسانی و عوامل بوجود آورنده‌ی آن پرداخته شده است که هریک از عوامل درگروه‌های متفاوت قرار می گیرند. مطابق با مدل کلی بدست آمده، می توان قابلیت اطمینان کل سامانه و یا هریک از عوامل را بدست آورد. با استفاده از این مدل و براساس داده های کمی و برآورد قابلیت اطمینان می توان تاحدودی خطاهای انسانی راشناسایی کرد و راهکارهایی را برای کاهش خطا بیان نمود. با بررسی خطاهای انسانی وعلل بوجود آورنده‌ی آنها به ارایه‌ی مدل کلی با سه دسته خطاهای فردی، خطاهای تیمی وخطاهای محیطی پرداخته شد که تقسیم بندی انواع خطا و زیر مجموعه های موجود به صورت زیر می باشد:

۱. خطاهای فردی: در این زمینه، ۵ دسته خطا که عبارتند از طراحی، نگهداری تجهیزات، بازرسی، جابجایی وکارور قرار می گیرند. در ادامه، هرکدام ازخطاها با بررسی علل بوجود آورنده و مثال های مربوطه بیان می شوند.

۱-۱. خطای طراحی: این خطا درنتیجه طراحی ناقص رخ می دهد. ازعوامل بوجودآورنده‌ی آن می توان به انتساب وظیفه نامناسب به فرد، خطا درهنگام پیاده سازی برنامه‌ها توسط فرد و خطا در اطمینان از اثربخشی تعامل انسان و ماشین که به عامل های انسانی مشابهت دارند، اشاره کرد. به عنوان مثال درجای گزاری وکنترل قسمت های مجزا ازهم که کارور در استفاده موثر از هر دوی آنها با مشکل مواجه می شود.

۱-۲. خطای نگهداری تجهیزات: اینگونه خطاها به طور معمول به علت تعمیر ونگهداری نادرست، خطا در نصب و راه اندازی تجهیزات و اشتباه در نگهداری و تعمیرات مانند برنامه ریزی زمانی رخ می دهد. به عنوان مثال خصلت یابی نادرست وسایل و تجهیزات و استفاده اشتباه ازگریس و روغن کاری در نقاط مناسبی از تجهیزات.

۱-۳. خطای بازرسی: این خطا به پذیرش خارج از تحمل اقلام و موارد یا رد تحمل آن مربوط است. از علل بروز آن می توان به اشتباه درکنترل کیفیت و اشتباه در نمونه گیری برای پذیرش، به بیان دیگر رد اقلام استاندارد و یا پذیرش اقلام غیراستاندارد اشاره کرد. باتوجه به مطالعات مختلف، خطای بازرسی به طور متوسط حدود ۸۵ درصد بوده است.

۱-۴. خطای جابجایی: درنتیجه حمل نامناسب یا ذخیره سازی نامناسب تجهیزات انبار می باشد. ازعلل آن می توان به عدم به کارگیری صحیح صفحه های هم‌گذاری حمل ونقل و نحوه حمل(انسان یا دستگاه) برای مواردی مانند لرزش، ضربه و ارتعاش اشاره کرد.

۱-۵. خطای کارور: این خطا به طور معمول در زمینه استفاده از تجهیزات محیط رخ می دهد که مرتبط با پرسنل عملیاتی می باشد. از علل آن می توان به بی دقتی کارور در تولید، ضعف در آموزش دستورالعمل مناسب به کارور، سهل انگاری کارور در به کارگیری دستورالعمل های عملیاتی صحیح، انگیختگی هیجانی، فشارها و احساسات و ادراک و ارزیابی ها اشاره نمود. هرکدام از این موارد به صورت تفکیک شده زیر بیان می گردند:

۱-۵-۱. بی دقتی کارور در تولید

مانند لحیم کاری اشتباه، سیم پیچی برعکس، استفاده از یک جزء اشتباه، حذف نامناسب یک جزء.

۱-۵-۲. ضعف در آموزش دستورالعمل مناسب به کارور

۱-۵-۳. سهل انگاری کارور در به کارگیری دستورالعمل‌های عملیاتی صحیح

۱-۵-۴. انگیختگی هیجانی: در این مورد علت اصلی و تاثیرگذار، استرس می باشد.

درتعریفی از گیلاردز آمده است: استرس حالتی است که کارور احساس تهدید و ترس از دست دادن کنترل یک وضعیت را دارد (گیلاردز،۱۹۹۳) . نوکروگوتمان بیان می‌کند که استرس، تنش روانی یا فیزیکی، درنتیجه عوامل روانی یا فیزیکی استرس زا یا هردوی این موارد می باشد (نوکروگوتمان،۱۹۸۳) .

استرس عدم قطعیت ناشی ازعدم وجود یک تصویر روشن در این شرایط است و ترویج رفتارهایی است که برای دستیابی به اعتماد به نفس کمک کننده می باشد و بر چهار نوع فشار، تعارض، سرخوردگی و عدم قطعیت و اطمینان است (لویس، ۱۹۹۴وکاپلان وهمکاران،۱۹۸۹).

۱-۵-۴-۱. استرس فشارناشی از یک تقاضای بزرگ می‌تواند در یک کارور منجر به بسیج بیشتر منابع در دسترس برای روبرو شدن با تقاضا باشد.

۱-۵-۴-۲. استرس تعارض ناشی از نیازهای متضاد برای توزیع منابع در میان اهداف متعدد است که کارور را وادار به کاهش تقاضا می کند. به عنوان مثال با منصرف شدن یا تعویق انداختن پی گیری برخی اهداف یا به دست آوردن بیشتر منابع با درخواست کمک.

۱-۵-۴-۳. استرس سرخوردگی زمانی به وجود می آید که تلاش برای رسیدن به یک هدف مسدود شده باشد و کارور به دنبال ایجاد انگیزش روش جایگزین برای رسیدن به هدف یا رهاکردن هدف باشد.

۱-۵-۵. فشارها و احساسات که خود شامل عواملی چون بار محدودیت زمانی، بار مرتبط با وظیفه(کار)، بار غیرمرتبط با کار، بار اطلاعات غیرفعال و اعتماد به نفس درعملکرد می باشد.

۱-۵-۵-۱. بار محدودیت زمانی، فشار ناشی از احساس نداشتن زمان کافی برای حل یک مشکل است. استرس زمانی وفشار زمانی، معانی مشابهی دارند و به طور معمول، خواص ترکیب کار ناشی ازکفایت زمان، ضرورت وپیچیدگی کار وکمیت کار را به دنبال دارد (اسونسون ومایول،۱۹۹۳) . شکل شماره ۱ بیان گرافیکی زمان و بارمحدودیت زمانی است، که به وسیله طول نسبی زمان از زمان در دسترس(مثلا زمان در دسترس برای عمل برروی سامانه) و درک زمان مورد نیاز(به عنوان مثال زمان مورد نیاز برای کارور تا روند کنترل را کامل کند) برای یک کار، تعیین می شود. نسبت پایین تر زمان درک شده دردسترس به زمان درک شده موردنیاز، بالاتر از نمره بار محدودیت زمانی است.

شکل ۱. بیان گرافیکی بارمحدودیت زمانی

هر وظیفه، بارگذاری محدودیت زمانی آن است. همچنین یک بار محدودیت زمانی وجود دارد که کل محدودیت های زمانی جمع آوری شده از تمام کارها را نشان می دهد. تعاریف دیگر عبارتند از تفاوت بین مقدار زمان در دسترس و مقدار زمان مورد نیاز برای حل یک کار (رستگاری ولندی، ۱۹۹۳) و نرخی که در آن وضعیت به سمت زمانی حرکت می کند که پیامدهای منفی در آن تحقق می یابد (ویکنز،۱۹۹۲). بدیهی است که هر دو در طول زمان واقعی و زمان درک شده وجود دارند. همچنین بار محدودیت زمانی بیشتر به احساس فرد از کفایت زمان مربوط است نه زمان واقعی در دسترس (فاگرجورد،۹۹۹۱) .

۱-۵-۵-۲. بار مرتبط با وظیفه ناشی از جمع آوری مطالبات برخواص مرتبط با کار ازجمله کمیت کار، پیچیدگی، اهمیت و دقت مورد نیاز (مثلا تحمل خطا) در واحد زمان است. درک سطح این ویژگی ها در نتیجه به مهارت فردی کارور وآشنایی با وظایف تعریف شده در IDAC[1] در بار مرتبط با کار در واحد زمان نرمال مربوط است، که این بار را از یک بعد مستقل و جدا برای بار محدودیت زمانی بررسی می‌کند.

1. information, decision, and action in crew context

بنابراین، بار محدودیت زمانی وابسته به یک کار است و بار مرتبط با کار از جهاتی به نتایج جمع آوری شده‌ی بارهای مرتبط با کار فردی برمی گردد.

۱-۵-۵-۳. بار غیر مرتبط با کار بار ناشی از کار خارجی که لازم است علاوه بر انجام کارهای در دست برای حل مشکلات، اجراشود.

برای مثال پاسخ دادن به تماس های تلفنی یا مدیریت برای گزارش وضعیت جاری سامانه درحالی که حضور دیگر وظایف لازم می تواند استرس زا باشد.

۱-۵-۵-۴. بار اطلاعات غیر فعال همان ایجاد ادراک اطلاعات نشان داده شده به جهان خارج می باشد.

به طورمثال در حادثه‌ی Three-Mile Island NPP، کارورها به وسیله‌ی تعداد زیادی نشانه های فعال در عرض چند دقیقه پس از آغاز رویداد تحت الشعاع اطلاعات غیر ضروری قرار گرفتند که توسط یکی از کارورها برای کمیته بررسی آماده شده بود و کارورهای اتاق کنترل بیان کردند که اطلاعات مفیدی بدست آنها نرسیده است.(چانگ و مصلح، ۲۰۰۷)

۱-۵-۶ . ادراک وارزیابی‌ها: از زیرمجموعه‌ی خطاهای فردی می باشد که علل بوجود آورنده‌ی آن عبارتند از شدت نتایج درک شده وابسته به تشخیص/تصمیم جاری، میزان بحرانی بودن شرایط ادراک شده‌ی سامانه، میزان آشنایی با موقعیت درک شده، پاسخ های ادراک شده در تایید یا نقض سامانه، درک هشدارها، درک مسئولیت تصمیم گیری، ادراک پیچیدگی وظیفه، سبک حل مساله، آگاهی ازنقش یامسئولیت.

۱-۵-۶-۱. تشخیص/تصمیم جاری عبارت است از ادراک فوری از پیامدهای ناگوار که می تواند منجر به این وضعیت شود. یک اولویت عملگر خاص به طورکلی به دو ویژگی اهمیت و ضرورت وابسته است. درک شدت تشخیص پیامدهای جاری، نشان دهنده‌ی اهمیت یک وظیفه است و ضرورت، به وسیله‌ی بار محدودیت زمانی نشان داده شده است.

۱-۵-۶-۲. بحرانی بودن شرایط ادراک شده‌ی سامانه، ارزیابی حاشیه‌ی ایمنی سامانه است که به طور معمول به وسیله‌ی ارزش های مطلق، سرعت تغییر و تغییر جهت چند پارامتر کلیدی انجام می شود. هر پارامترکلیدی محدوده عمل معمولی دارد و افزایش چنین طیفی به این معنا است که امنیت سامانه تهدید شده است. ادراک شرایط بحرانی بودن سامانه، با عواقب درک شدت با تشخیص جریان آن متفاوت است. درک شدت باتشخیص جریان، پیامد بالقوه‌ی شکست و یا از دست دادن تمامیت سامانه را نشان می‌دهد ولی درک بحرانی بودن سامانه چگونگی نزدیک شدن سامانه به حالت شکست رانشان می دهد.

۱-۵-۶-۳. آشنایی با موقعیت ادراک شده عبارت است از شباهت و درک توسط کارور بین وضعیت کنونی و آنچه کارور تجربه کرده است یا آموزش دیده است(مثلا آموزش شبیه ساز). درک و آشنایی با وضعیت می تواند توضیح دهد که چرا کار یکسان توسط کارورهای مختلف، به ارزیابی متفاوتی از پیچیدگی می رسد. بر اساس مفهوم تقاضا و منابع همان کار نشان می دهد که مطالبات کارها یکسان است. با این حال آشنایی با کار می تواند کارور را با منابع اضافه برای روبرو شدن با تقاضا آماده کند.

۱-۵-۶-۴. پاسخ های ادراک شده در تایید یانقض: عبارت است از نشانه های جمع آوری شده از مشاهدات واکنش های مثبت و منفی مربوط به سامانه در رابطه با آنچه که از کارور انتظار می رود.

۱-۵-۶-۵. ادراک هشدارها: ادراک هشدار دهنده با توجه به عواملی مانند مقدار، شدت و اهمیت آن خطا قابل بررسی می باشد.

این مورد بیشتر در اتاق های کنترل در NPPS[1] کاربرد دارد. ادراک از مقدار هشدار دهنده، تعداد کل زنگ های هشدار فعال شده توسط کارور را انعکاس می دهد. ادراک از شدت هشداردهنده، نشان دهنده‌ی بالاترین نرخ وقوع هشدار را در فاصله زمانی کوتاه دریافت آن نشان می دهد و ادراک از اهمیت هشدار دهنده نشان دهنده‌ی اهمیت جمع آوری تاثیرات رنگ ها (دراتاق کنترل؛ اهمیت هر نوع هشدار با رنگ های متفاوت نشان داده می شود) بر روی کارور است.

۱-۵-۶-۶ . درک مسئولیت تصمیم گیری: آگاهی از

1. nuclear power plant state

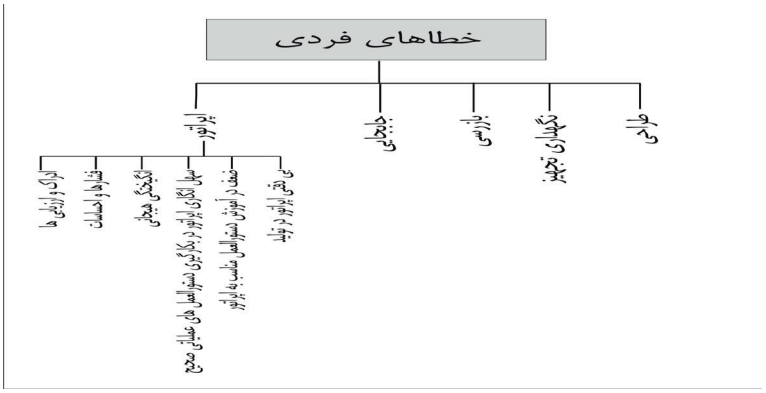
مسئولیت و پاسخگویی نسبت به تصمیم گیری یا فعالیت کارور می باشد. به طور مثال، هنگامی که برخی کارورها به طور بالقوه با نتایج منفی درگیر هستند، تمایل دارند که آن را به نماینده یا مسئول تصمیم گیری انتقال دهند و نمی‌خواهند که مسئول ضرر و زیان عمده شوند (ویکنز،۱۹۹۲).

۱-۵-۶-۷. درک پیچیدگی وظیفه: پیچیدگی وظیفه به سطح شناخت و تلاش فیزیکی مورد نیاز برای تکمیل کار یک کارور اشاره دارد. به عنوان مثال، الزامات دقت و نیازهای محاسباتی عامل هایی در تعیین پیچیدگی کار می باشند. چنین عواملی دراصل ، اندازه گیری عینی نمی‌شوند. به عنوان مثال در مرحله‌ی اندازه گیری پیچیدگی، محاسبه‌ی پیچیدگی انجام گام به گام یک روش راه اندازی فوری می باشد. درک این پیچیدگی ذاتی، درک پیچیدگی وظیفه است و هنگامی که با نتایج ادراک شده از وضعیت ترکیب می شود ادراک دشواری وظیفه‌ی فردی نام می‌گیرد. (پارک جی وهمکاران،۲۰۰۱)

۱-۵-۶-۸. درک منابع حل مسئله: ارزیابی سطح بالای کارور از منابع در دسترس داخلی و خارجی برای اینکه مساله را حل کند. نمونه هایی از یک منبع داخلی، تعداد روش هایی است که کارور برای حل مساله می شناسد و نمونه منابع خارجی هم تیمی ها، روش ها و سامانه های تصمیم و مراکز پشتیبانی فنی از راه دور می باشند.

۱-۵-۶-۹. آگاهی از نقش/مسئولیت: شامل آگاهی کارور از مسئولیت اولیه(مثلا مسئولیت اختصاص داده شده به طور رسمی) و مسئولیت های فرعی(مسئولیت اختصاص داده شده غیررسمی مانند کمک به هم تیمی در زمان موردنیاز) می باشد. اولین نوع از آگاهی کارور از مسئولیت خودکارور مشتق می شود و نوع دوم مطابق با افزایش آگاهی ازهم تیمی.

خطاهای فردی و تقسیم بندی عوامل بوجود آورنده‌ی آن، بطور کلی در شکل شماره‌ی ۲ آمده است.



شکل ۲. انواع خطاهای فردی وعلل بوجودآورنده‌ی آن(دیهیلون،۲۰۰۷ وچانگ ومصلح ۲۰۰۷)

۲. خطاهای تیمی: دسته ی دیگری از خطاهای انسانی در مجموعه‌ی خطای تیمی رخ می دهد و در این دسته بندی ۶ نوع خطا قرار می گیرد که مشابه با دسته‌بندی‌های بیان شده در بالا، انواع آن به تفصیل بیان می گردد:

۲-۱. پیوستگی وانسجام: گاهی اوقات به نام روحیه‌ی گروه یا احساسات گروه شناخته شده و نشانه ای از تمامیت تیم است. به بیان دیگر عبارت است از همبستگی گروه، هارمونی گروه و رفتاری که اعضای گروه همراه با همه‌ی جنبه های یکپارچگی دارند.

مولن وکوپر،۲۰۰۱، سه جنبه از انسجام را تشخیص دادند که عبارتند از جاذبه های میان فردی از اعضای تیم، تعهد به تیم کاری و غرور تیم و روحیه‌ی تیمی.

۲-۲. هماهنگی تیم: اشاره به اثربخشی یک تیم سازمانی به عنوان واحدی برای انجام کار در هر دو بعد زمان و فضا دارد. به عبارتی دیگر، این مفهوم تقسیم مسئولیت‌ها و فرماندهی و کنترل می باشد. همچنین مرتبط است با درجه ای از هماهنگ سازی سهم فردی کارور درکار تیم(هویجل وجمیوندن،۲۰۰۱). دربعضی مطالعات به این مورد، هنجارگروه می گویند که یک ایده و فکر در ارضای گروه می باشد. یک ایده که می تواند به شکل بیانیه‌ی مشخص باشد که اعضا یا افراد دیگر باید آن را انجام دهند و انتظار می رود افراد تحت شرایط

خاص به آن اقدام کنند(هومانز،۱۹۵۰). درتعریفی دیگر، یک انتظارمشترک از محدوده‌ی قابل قبول رفتار و رابطه با بعضی ارزش ها می باشد (کروسبی،۱۹۷۵). هماهنگی تیم، انتظارات مشترک گروه است که برای کلاس اشیاء با داشتن یک اساس ارزیابی اخلاقی، استاندارد شده اند و تعمیم یافته اند و طیف وسیعی از رفتارهای غیرقابل قبول، تحت شرایط داده شده را تجویز می کند (نیکسون،۱۹۷۹). عامل مهم و موثر بر هنجار گروه، آموزش خدمه در تیم است.

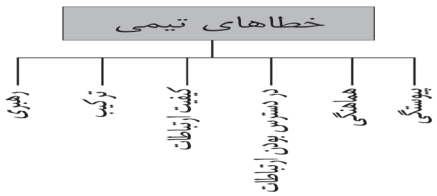
۲-۳. در دسترس بودن ارتباطات: به در دسترس بودن ابزار، وسایل و ساز وکارها برای تبادل اطلاعات به اعضای تیم اشاره دارد، به ویژه وقتی خدمه در نقاط مختلف فیزیکی پراکنده اند. هماهنگی کار معمولا به شدت بر وسایل ارتباطی متکی است. ارتباط به خدمه اجازه می دهد تا دانش در مورد یک وضعیت را به اشتراک گذارند.(روگنین و بلنکورت،۲۰۰۱)

۲-۴. کیفیت ارتباطات: به درجه ای اشاره دارد که اطلاعات دریافت شده به وسیله‌ی گیرنده، به انتقال اطلاعات توسط فرستنده مربوط می شود. برخی از علل آن کیفیت ارتباطات ضعیف، درست عمل نکردن تجهیزات ارتباطی و اختلال در سیگنال است.

۲-۵. ترکیب تیم مربوط به اندازه و همگن بودن: ناهمگونی و عدم تکمیل و افزونگی دانش مورد نیاز و مهارت‌های لازم برای تکمیل کار را فراهم می کند (پیریس سی ار وهمکاران، ۲۰۰۰). به طور معمول اندازه‌ی تیم با ماهیت ماموریت تیم تعیین می شود. اندازه‌ی بیش ازحد کوچک، حجم کار بیش از حد زیاد برای اعضای تیم ایجاد می کند.

نیروی کار بطورکلی شامل اجرایی، نظارت و تدارکات پشتیبانی است. اطمینان از همگنی و ناهمگنی نشان می دهد که تیم گزارش کافی دارد و قادر است وظایف را بدرستی در دست گیرد.

۲-۶ . رهبری: گرین و پاجلیس(۲۰۰۲) رهبری را به عنوان فرایند تشخیص برای گروهی که در آن کار می‌کند و جایی که نیاز دارد تا در آینده در آن جایگاه باشد و تدوین راهبرد برای آن وجود دارد، تعریف می کنند. رهبری همچنین شامل اجرای تغییر و پیشرفت پایه تحت تاثیر با همکاری پیروان، انگیزه‌ی آنها برای سخت کارکردن در تعقیب اهداف تغییر و کار با آنها برای غلبه بر موانع برای تغییر می باشد. بر اساس این تعریف، اثربخشی رهبری می‌تواند با آنچه رهبری با آن جهتی را برای گروه تعیین می کند، اندازه گیری شود. رابطه‌ی ایجاد روابط با پیروان به منظور به دست آوردن تعهد دیگران برای تغییر اهداف و کار با آن‌هاست تا بر موانع غلبه کنند و تغییر را انجام دهند. شکل شماره‌ی ۳ انواع خطاهای تیمی را بصورت نمودار نشان می دهد.



شکل ۳. انواع خطاهای تیمی(چانگ و مصلح، ۲۰۰۷)

۳. خطاهای محیطی: دسته بندی دیگری از خطاهای انسانی، خطای محیطی می باشد . عامل های محیطی به تدریج و با سرعت بالا تحت تاثیر تغییرات محیطی موثر بر عملکرد انسان قرار می گیرند. برای مثال دربعضی اتاق‌های کنترل NPP[1]، تعداد زیادی از قطعه ها بارنگ نشان کدبندی شده است تا اهمیت موارد را نشان دهد. حالت یک نشان می تواند در نور روشن ثابت، خاموشی ثابت و یاچشمک زدن باشد. فعال سازی زنگ با صدای اعلام هشدار دهنده همراه است. جلوه های بصری و صوتی ازجمله تغییرات اطراف می تواند عملکرد کارور را تحت تاثیر قراردهد.(چانگ ومصلح، ۲۰۰۷). مثال هایی از تغییرات شدید محیط، اتاق کنترل غیرقابل سکونت (مثلا

1. nuclear power plant

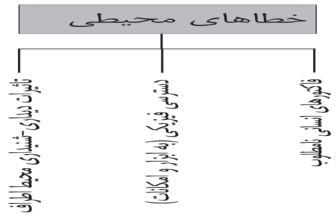
ناشی ازآتش) و مسدود شدن دسترسی فیزیکی می باشد. موارد دیگر محیطی نورضعیف، درجه حرارت بیش ازحد، سرو صدای بیش ازحد و... می باشد.

پس ازبررسی، خطاهای محیطی به سه دسته‌ی اصلی تقسیم و به صورت زیر دسته بندی شدند(نمودار در شکل شماره ۴) :

۳-۱. عامل های انسانی نامطلوب(به عنوان مثال محیط ناملایم وخشن)

۳-۲. دسترسی فیزیکی به ابزار وامکانات

۳-۳. .تاثیرات دیداری- شنیداری محیط اطراف (مانند تمرکز- سرعت- دقت)



شکل ۴. انواع خطاهای محیطی(چانگ و مصلح، ۲۰۰۷)

در این مقاله خطاهای انسانی به صورت کلی و با تقسیم‌بندی‌های فردی، تیمی و محیطی همراه با عوامل بوجودآورنده‌ی این خطاها بررسی شده وبا استفاده از مدل‌های بررسی شده توسط چانگ ومصلح،۲۰۰۷ و دیهیلون، ۲۰۰۷ به صورت مدلی جامع در شکل شماره ۵ آمده است. با استفاده از این مدل و بررسی علل بروز خطا و قابلیت اطمینان آن می توان قابلیت اطمینان کلی هر سامانه را محاسبه نمود. همچنین می توان عدد قابلیت اطمینان هر مورد را با استفاده از نظرخبرگان و به صورت فازی اعمال کرد و قابلیت اطمینان کل سامانه را بصورت فازی محاسبه کرد.

۴) نتیجه گیری

انسان نقش اساسی در قابلیت اطمینان سامانه ایفا می‌کند و با بررسی دلایل اساسی وقوع خطای انسان، توجه به عواملی انسانی اهمیت یافته است. با توجه به عوامل بیان شده درمقاله، می توان گفت علت های بروز خطاهای انسانی، تنها از جنبه فردی برخوردار نیست و نمی توان تنها فرد را مقصر بروز حادثه دانست، بلکه فرد جزء کوچکی از سامانه به حساب می آید و عوامل متعددی در کنار هم قرار می‌گیرند و باعث بروز خطا و حوادث می شوند. در این تحقیق، خطاهای انسانی ریشه یابی و به سه دسته‌ی فردی، تیمی و محیطی تقسیم بندی شدند. براین اساس مدلی کلی از خطاهای انسانی ارایه گردید و از آنجا که امروزه حتی روش هایی وجود دارند که به صورت کمی و کیفی میزان احتمال وقوع و تاثیر خطاهای انسانی در قابلیت اطمینان و ایمنی سامانه را تحلیل می کنند، این مدل می‌تواند با استفاده از داده های کمی برای محاسبه‌ی قابلیت اطمینان استفاده شود . همچنین دسته بندی های مذکور می تواند با مشخص نمودن علل بوجودآورنده‌ی خطا باعث افزایش قابلیت اطمینان هر مورد گردد و از طرفی نیز بروز خطا را کاهش دهد. بنابراین، استفاده از این مدل در محاسبه قابلیت اطمینان، تحلیل های مالی، محاسبه کفایت و شایستگی انسان بر اساسHRM و ارایه‌ی مدل های ریاضی پیشنهاد می گردد.

شکل ۵. مدل کلی خطاهای انسانی

۵) منابع

۱. آل علی، فرهاد- (۱۳۹۰) - " عوامل انسانی اثرگذار بر قابلیت اطمینان و ایمنی در طراحی" - دومین کنفرانس مهندسی قابلیت اطمینان- پژوهشگاه هوافضا- آبان ماه.
۲. کرباسیان،مهدی و طباطبایی،لیلا- (۱۳۸۸) - "آشنایی با قابلیت اطمینان انسان"- چاپ اول - انتشارات ارکان اصفهان- ص ۱۵.
۳. مختاری،زهرا وهمکاران- (۱۳۹۰)-"بررسی قابلیت اطمینان انسان در چارچوب اچ اس ای با در نظر گرفتن عواملی مؤثر در عملکرد و سبک های تصمیم گیری"-
۴. موعودی، محمد امین و قربانی نیا، سیده مریم- (۱۳۹۰)-

info@idsc.tridi.ir

" تحلیل خطای انسانی و قابلیت اطمینان با استفاده از فن THERP در اتاق کنترل مرکزی واحد پخت کلینکر، یکی از صنایع سیمان" – دومین کنفرانس مهندسی قابلیت اطمینان– پژوهشگاه هوافضا، آبان ماه.

۵. مهر آرا مولان،امیرارسلان و اله یاری نیک،اشکان– (۱۳۹۱)– " بررسی عوامل بشری و سازمانی در ارزیابی قابلیت اطمینان سامانه‌های سازه‌ای فراساحل"– اولین کنفرانس بین المللی مهندسی کیفیت – تهران.

1.Barry Kirwan , W. Huw Gibson, Brian Hickling, ,)2008(, " human error data collection as a precursor to the development of a human reliability assessment capability in air traffic management", Reliability Engineering and System Safety 93, pp 217–233.

2. Chang Y.H.J., Mosleh. A , ,)2007(, "Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents. Part 2: IDAC performance influencing factors model", Reliability Engineering and System Safety 92,pp 1014–1040, available online at www.sciencedirect.com.

3. Chiodo .E., Gagliardi.F. and Pagano.M. ,(2004), "Human reliability analyses by random hazard rate approach" ,The Emerald Research Register for this journal www.emeraldinsight.com/0332-1649.htm.

4. Christensen J.M and Howard J.M, (1981) ," Field Experience in Maintenance. In Human Detection and Diagnosis of System Failures", edited by J. Rasmussen and W.B. Rouse,Plenum Press, New York, pp 111–113.

5.Crosbie PV.,(1975), ' Interactions in small group". New York: Macmillan Publishing Co.

Dhillon B.S and Liu Y, (2006) ," Human Error in Maintenance": A Review. J of Qual in Maint Eng 12(1). pp 21–36.

6. Dhillon B.S,)1986(," Human Reliability: With Human Factors". Pergamon Press, New York.

7. Dihillon B.S,)2007(,"basic human error and error concept" ،Human Reliability and Error in Transportation Systems, Springer Series in Reliability Engineering, pp 43-55.

8. Fagerjord M,)1999(,"Human reliability assessment", In: Department of production and quality engineering. Norwegian University of Science and Technology, p. 124.

9. Ferench, S., Bedford , T., Pollard , S. and Soane, E.,) 2011 ،("Human reliability analysis: A critique and review for managers". Safety Science.

10. Gaillard AWK.,)1993(,"Comparing the concepts of mental load and stress", Ergonomics, 36(9), pp 991–1005.

11. Hoegl M, Gemuenden HG.,) 2001(, "Teamwork quality and the success of innovative projects:, a theoretical concept and empirical evidence. Organization Science,

fuzzy Bayesian network approach to improve the quantification of organizational influences in HRA frameworks" , Safety Science 50 ,pp 1569–1583. Published by Elsevier Ltd. All rights reserved.

19. Maule AJ, Maillet-Hausswirth P., (1995)," The mediating effects of subjective appraisal cognitive control and changes in affect in determining the effects of time pressure on risk-taking", In: 15th research conference on subjective probability, Utility and Decision Making (SPUDM15).. Jerusalem.

20. May.I. L. and Deckker E, (2009)," Reducing the risk of failure by better training and education", Engineering Failure Analysis.

21. Mullen B, Copper C., (1994)," The relation between group cohesiveness and performance", an integration. Psychological Bulletin, 115(2), pp 210–27.

22. Nixon HL.,(1979), "The small group. Prentice-Hall Series" . In: Smelser NJ, editor. Sociology. 1 ed. Englewood, NJ: Prentice -Hal"l, Inc.

23. Paglis L.L, Green SG.,(2002)," Leadership self-efficacy and managers' motivation for leading change", Journal of Organizational Behavior, 23(2), pp 215–35.

24. Papodopoulos. J. , Georgiadou. P. , Papazoglou .C. and Michaliou. K. ,(2009), "Occupational and pub-

12(4),pp 435–49.

12. Homans GC.,)1950(, "The human group", New York: Harcourt, Brace, Jovanovich, Inc.

13. Hsu .H, Lee . C. C., Wu. M. C. and Takano. K, (2008), "A cross cultural study of organizational factors on safety: Japanese vs Taiwanese oil refinery plants", Accident Analysis and Prevention.

14. Huey BM, Wickens CD, editors,,(1993), "Workload transition: implications for individual and team performance", Washington DC.: Commission on Behavioral and Social Sciences and Education, National Research Council.

15. Kaplan RM, Saccuzzo DP. ,(1989)," Psychological testing: principles, applications, and issues, 2 ed" . Pacific Grove, California: Brooks/ Cole Pub. Co.

16. Kyung S. Park, Jae in Lee, (2008)," A new method for estimating human error probabilities: AHP–SLIM", Reliability Engineering and System Safety 93,pp 578–587, available online at www.sciencedirect.com.

17. Lewis GW., (1994)," Critical incident stress and trauma in the workplace: recognition response recovery. Muncie, Indiana", Accelerated Development Inc.

18. Li Peng- cheng , Chen Guo- hua , Dai Li- cao , Zhang Li, (2012)," A

lic health and safety in a changing work environment", Safety Science.
25. Paris CR, Salas E, Cannon-Bowers JA.,(2000)," Teamwork in multi-person systems", a review and analysis. Ergonomics , 43(8), pp 1052–75.
26. Park J, Jung WD, Ha J., (2001)," Development of the step complexity measure for emergency operating procedures using entropy concept", Reliability Eng Syst Saf;71(2),pp 115–30.
27. Rastegary H, Landy FJ. , (1993)," The interaction among time urgency, uncertainty, and time pressure".
28. Rognin .L, Blanquart J-P.,(2001)," Human communication, mutual awareness and system dependability", Lesson learnt from air-traffic control field studies. Reliability Engineering and System Safety ,71, 327–36.
29. Sankaran Mahadevan Candice D. Griffith,, (2011), "Inclusion of fatigue effects in human reliability analysis" ,Reliability Engineering and System Safety 96 ,pp 1437–1447.
30. Strater, Oliver, "Considerations on the elements of quantifying human reliability", Reliability Engineering and System Safety, Vol. 83,pp. 255–264, 2004.
31. Svenson O, Maule AJ, (1993), editors. "Time pressure and stress in human judgment and decision making" , New York: Plenum Press, p 333.
32. Swain AD, Guttmann HE., (1983)," Handbook of human reliability analysis with emphasis on nuclear power plant applications" . NUREG/CR- 1278: Nuclear Regulatory Commission.
33. Wickens C.D. ,(1992)," Engineering psychology and human performance" . 2nd ed. Harper Collins Publishers..
34. Wright, P.M. and Boswell, W., (2002), "Desegregating HRM: a review and synthesis of micro and macro human resource management", Journal of Management, Vol. 28 No. 3, p. 247.
35. Zhiqiang Sun.a.n, ZhengyiLi b, Erling Gong a, Hong weiXie a, (2012),"Estimating Human Error Probability using a modified CREAM", Reliability Engineering and System Safety 100 ,pp 28–32
36. Zhou Chong, Kou Xin-jian, (2010), "Method of Estimating Human Error Probabilities in Construction for Structural Reliability Analysis Based on Analytic Hierarchy Process and Failure Likelihood Index Method", J. Shanghai Jiaotong Univ. (Sci.), 15(3),pp 291-296.

6) References

1. ISO 28000. First edition, 2007-09-15. “Specification for security management systems for the supply chain”.

2. ISO 28001. First edition, 2007-10-15. “Security management systems for the supply chain- Best practices for implementing supply chain security, assessments and plans- Requirements and guidance”.

3. Supply Chain Security Management: An Overview: JuhaHintsa, Dr. Philippe Wieser, Ximena Gutierrez, Dr. Ari-PekkaHameri: HEC University of Lausanne, Ecole Polythecnique Fédéral de Lausanne Cross-border Research Association (CBRA), Lausanne, Switzerland,2007.

4. Corporate Response to Terrorism: Creating Resilient and Secure Supply Chains; James B. Rice, Jr.; Global and Homeland Security: Science, Technology; MIT ;2003.

5. Official website and portals of ISO “www.iso.org” and ISIRI “www.ISIRI.org.”

6.ISO/PAS 28002: First edition, 2010-09-01: Security management systems for the supply chain- Development of resilience in the supply chain- Requirements with guidance for use.

7. ISO 28003. First edition, 2007-08-01. “Security management systems for the supply chain- Requirements for bodies providing audit and certification of supply chain security management systems”.

8. ISO 28004. Parts 1-4, 2007-2012. “Security management systems for the supply chain- Guidelines for the implementation of ISO 28000”.

9. ISO/PAS 28005. Part 1 -2, 2011-2012. “Security management systems for the supply chain- Electronic port clearance (EPC)”.

10. ISO 20858.First edition, 2007-10-15. “Ships and marine technology — Maritime port facility security assessments and security plan development”.

11. BUILDING THE RESILIENT SUPPLY CHAIN; Martin Christopher and Helen Peck; International Journal of Logistics Management, Vol. 15, No. 2, pp1-13, 2004.

Step 4. Quantify and prioritize risks including quantification of each risk in terms of likelihood of occurrence and potential impact and using the quantification of the risks to prioritize the risks according to defined objectives.

Step 5. Execute risk treatment programs including development of risk management actions consistent with each risk's priority, definition of each action's value in terms of reducing the likelihood and impact of the risk and development and execution an implementation plan for the identified actions.

Step 6. Monitor supply chain environment for risks including continuously monitor the supply chain environment for risk events or precursors, execution of applicable mitigation actionswhen thresholds are triggered and documentation of results for after action review and program improvement.

5) Managerial implications and Conclusion

Companies need to simultaneously build secure and resilient supply chains. The main challenge of this approach is to manage and mitigate supply chain risk by creating more resilient (flexible, agile) supply chains so that increase security without jeopardizing trade or burdening themselves and businesses with additional excessive operational costs.

In this paper, the necessity of using comprehensive measures for securing our company supply chain, with implementation of 28000 family standards, explained.

The important factors for implementing a reliable supply chain security system is identifying and implementing risk assessment and resilience methodology. A secure supply chain is not necessarily a resilient supply chain; therefore, this paper first presented an applicable methodology for security risk assessment and second, described a process approach for resilience management in the supply chain.

And finally, our research suggests that logistics should implement a supply chain security management system (SCSMS) with special attention to security and resilience as key success factors of implementation. Also they should use comprehensive standards such as ISO 28000 family, document a risk assessment methodology to determine the appropriate countermeasures, focus on creating resilience for different failure modes, Make choices about source of resiliency, ultimately assess security and resilience intimately for their entire supply network.

formation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process.[4]
The application of a system of processes within an organization, together with the identification and interactions of these processes and their management, can be referred to as a "process approach". Figure 2 depicts the process approach for resilience management in the supply chain .[6]

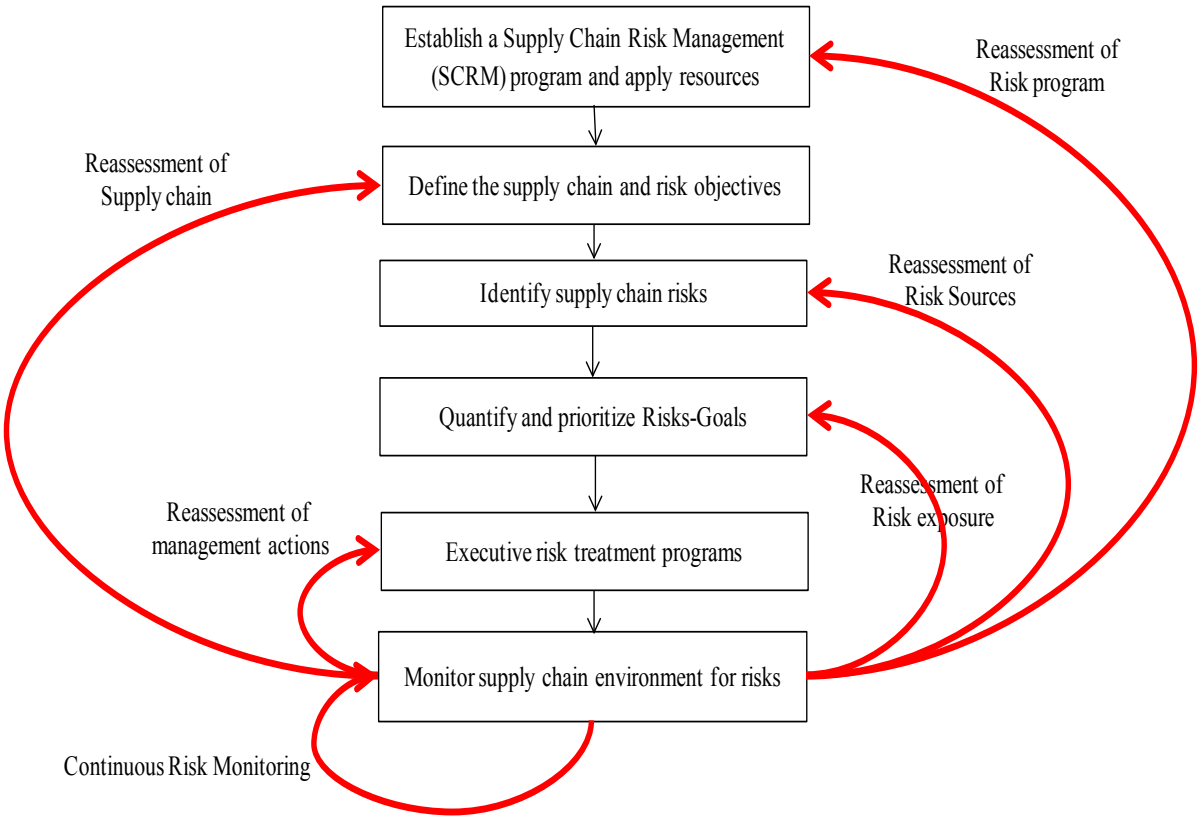


Figure 2: Process approach for resilience management in the supply chain

Step 1. Establish a supply chain resilience program and apply resources including recognition of supply chain risk management as a priority, securing of top management support for the program and resources necessary to execute the program.
Step 2. Define the supply chain and resilience objectives including definition of supply chain scope and map the supply chain and the objectives of managing risk in the subject supply chain.
Step 3. Identify supply chain risks including comprehensively review the supply chain to identify risks and documentation of identified risks to the extent possible.

The process of assessment is continual. As figure 1 illustrates, security must be monitored continually to ensure security measures are performing as intended and the assessment process should be performed as needed.[2]

4) Development of resilience plan

In today's uncertain and turbulent markets, supply chain vulnerability has become an issue of significance for many companies. As supply chains become more complex as a result of global sourcing and the continued trend to 'leaning-down', supply chain risk increases. The challenge to business today is to manage and mitigate that risk through creating more resilient supply chains.[11]

Organizations across the globe are rapidly developing risk management and resilience programs to address uncertainty in achieving their objectives. To ensure resilience in the supply chain, organizations must engage in a comprehensive and systematic process of prevention, protection, preparedness, mitigation, response, continuity and recovery.

The survivability of organizations within a supply chain depends largely on the resilience of their suppliers and customers. As a result, incorporating resilience, and improving the resilience of an organization within the supply chain, must be focused both within the organization and externally on its suppliers and customers.[6]

Managing risks in the supply chain requires an understanding of the organization's environment as well as the context of the global environment of the entire supply chain. Each node of the organization's supply chain involves a set of risks and management processes of plan, source, make, deliver and return. All of these management processes should be included in an organization's overall resilience program. With this understanding, an organization will define to which level or tier in their supply chain to include in their resilience program.[6]

The management systems approach encourages organizations to analyze organizational and stakeholder requirements and define processes that contribute to success. A management system can provide the framework for continual improvement to increase the likelihood of enhancing security, preparedness, response, continuity, and resilience. It provides confidence to the organization and its customers that the organization is able to provide a safe and secure environment which fulfills organizational and stakeholder requirements.

An organization needs to identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the trans-

- Low likelihood should be used in cases where the security measures in place offer substantial resistance to the security incident occurring.

Step four: Security incident scoring: The security incident scoring chart given in Table 4 is an example that may be used to determine when countermeasures should be considered for specific security incidents.

Likelihood Classification / Consequence Classification	**High**	**Medium**	**Low**
High	Countermeasures	Countermeasures	Consider
Medium	Countermeasures	Countermeasure or Consider as appropriate	Document
Low	Consider	Document	Document

Table 4. Security incident scoring chart

Identification of countermeasures is required for security incidents that score high in both likelihood and consequences, as well as for those scoring at medium likelihood and high consequences. Other security incidents need not include countermeasures, unless they are considered advisable by evaluator.

Step five: Development of countermeasures: If the development of a countermeasure is required or considered advisable by the evaluator both the consequences and/or likelihood of the security threat scenario should be considered for mitigation. Reducing the likelihood of the security threat scenario succeeding or reducing the harm that can be caused by the security threat scenarios to a level in which additional countermeasures are no longer required is the objective. Countermeasures may come under the actions such as: Treat, Transfer and Terminate.

Step six: Implementation of countermeasures: New countermeasures represent a change to operational practices and need to be enacted in accordance with the organization's management system to ensure that adequate resources are available; the impact on other operations is managed and the change has the support of management.

Step seven: Evaluation of countermeasures: Each countermeasure should be assessed for effectiveness in lowering the likelihood or consequences (or a combination of them) until the security risk no longer requires that additional countermeasures be considered.

Step eight: Repetition of the process: After countermeasures have been developed and evaluated as effective continue the process for the next security threat scenario until the scenario list is depleted.

Assign a rating	Consequence
High	**Death & Injury -** loss of life on a certain scale **and/or** **Economic Impact -** major damage to a asset and/or infrastructure preventing further operations **and/or** **Environmental Impact -** complete destruction of multiple aspects of the ecosystem over a large area
Medium	**Death & Injury -** for example loss of life **and/or** **Economic Impact –** for example damage to asset and/or infrastructure requiring repairs **and/or** **Environmental Impact –** for example long term damage to a portion of the ecosystem
Low	**Death & Injury –** injuries but no loss of life **and/or** **Economic Impact -** minimal damage to a asset and/or infrastructure and systems **and/or** **Environmental Impact –** some environmental damage

Table 3. Classification of consequences

Care should be taken in establishing values of “high”, “medium” and “low” consequences. The use of excessively low threshold values may result in the requirement that countermeasures be considered for more security threat scenarios than are needed. However, using excessively high threshold values may omit countermeasures for security threat scenarios involving consequences that the organization or government under which it is operating cannot tolerate.

A “high” consequence classification may be considered as a consequence that would be unacceptable in all but low likelihood situations.

A “medium” classification of consequence may be considered as a consequence that would be inacceptable in a high likelihood situation.

A “low” classification of consequence may be considered as a consequence that is normally acceptable.

Step three: Classification of likelihood of security incidents: The status of physical and operational security measures in the supply chain as documented in the security performance review list and other documentation provided should be taken into account in classifying potential security incidents. Physical security measures include objects that impede or detect unauthorized access to a target. Operational security measures include people and procedures that impede or detect unauthorized access to a target. The likelihood of each security incident occurring at a particular asset should be classified as high, medium and low.

- High likelihood should be used when the security measures in place offer little resistance to the security incident occurring. If a numerical system is used in the assessment process, the numerical results should be converted into this qualitative system.

- Medium likelihood should be used when the security measures in place offer moderate resistance to the security incident occurring.

	Example security threat scenarios	Application example
1	Intrude and/or take control of an asset (including conveyances) within the supply chain	Damage/destroy the asset. Damage/destroy outside target using the asset or goods. Cause civil or economic disturbance. Take hostages/kill people.
2	Use the supply chain as a means of smuggling	Illegal weapons into or out of the country/economy. Terrorist into or out of the country/economy.
3	Information tampering	Locally or remotely gaining access to the supply chain's information/documentation systems for the purpose ofdisrupting operations or facilitating illegal activities.
4	Cargo Integrity	Tampering, sabotage and/or theft for the purpose of terrorism
5	Unauthorized	Use Conducting operations in the international supply chain to facilitate a terrorist incident (e.g. using the means of transport (as a weapon).
6	Others	

Table 2. Security threat scenarios to the supply chain

During the assessment consider the following:

1) Access control on premises of the organization in the supply chain, on the means of transportation, on information,...

2) Means of transportation (trucks, railway, barges, aircraft, ships, etc.), taking into account (normal operation, maintenance shops, changes due to e.g. break downs, change of means, conveyances while at rest, using means of transport as a weapon,…)

3) Handling (loading, manufacturing, storage, transfer, unloading, deconsolidation/ consolidation ...)

4) Transportation of goods by air, road, rail, nland waterway shipping, ocean shipping, ….

5) Intrusion detection/prevention applied to shipments.

6) During inspections, e.g. vehicle inspections.

7) Employees (level of competence, training and awareness; integrity, …)

8) Use of business partners.

9) Communication internal/external (information exchange; emergency situations,...)

10) Handling or processing of information about cargo or transport routes (data protection, data assurance ,…)

11) External information (legal, orders by authorities, industry practices, accidents and incidents, first response capability and response times,...)

Step two: Classification of consequences: An evaluation of consequences should consider potential loss of life and economic loss. The consequences of each security incident evaluated in the supply chain should be classified as high, medium, or low. An example is shown in Table 3. A numerical system may be used in the assessment process, as long as the numerical results are converted to a qualitative system.

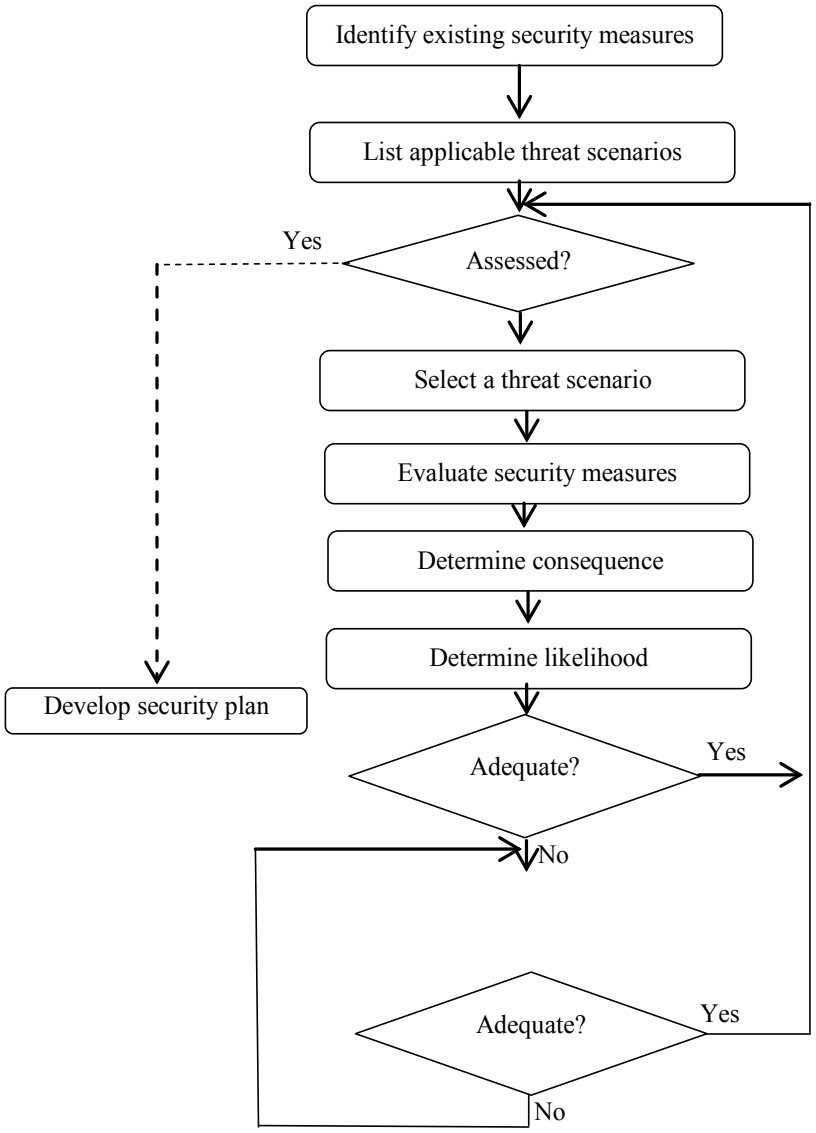


Figure 1. representation of a methodology for security risk assessment

Step one: Consideration of the security threat scenarios: The security assessment should consider as a minimum the security threat scenarios listed in Table2. The security assessment should also consider other scenarios identified by government authorities, supply chain management or the security professional conducting the assessment.

representatives and certain organizations responsible for the processing of the ship's port clearance request. [9]

ISO 20858 standard, addresses the execution of marine port facility security assessments, marine port facility security plans (including countermeasures) and the skills and knowledge required of the personnel involved. This Standard establishes a framework to assist marine port facilities in specifying the competence of personnel to conduct a marine port facility security assessment and to develop a security plan as required by the ISPS Code International Standard, conducting the marine port facility security assessment, and drafting/implementing a Port Facility Security Plan (PFSP).[10]

3) Methodology for security risk assessment

This section gives a methodology that recommended to be used by organizations in supply chains to make an assessment of the risk that their operations may suffer from security incidents, to determine the appropriate countermeasures, effective for the type and size of their supply chain operations. This methodology uses the following sequence that presented in figure 1.[2]

a) List all activities as covered in the Scope.

b) Identify security controls presently in place.

c) Identify security threat scenarios.

d) Determine consequences if the security threat scenario was completed.

e) What is the likelihood of this happening considering current security?

f) Are control security measures adequate?

g) If not develop additional security measures.

ISO/PAS 28002 document, is a management framework for action planning and decision making needed to anticipate, prevent if possible, and prepare for and respond to a disruptive incident (emergency, crisis, or disaster). The survivability of organizations within a supply chain depends largely on the resilience of their suppliers and customers. As a result, incorporating resilience, and improving the resilience of an organization within the supply chain, must be focused both within the organization and externally on its suppliers and customers. When this standard implemented within a management system, it enhances an organization's capacity to manage and survive the event, and take all appropriate actions to help ensure the organization's continued viability.[6]

ISO 28003 standard, is intended for use by bodies that carry out audit and certification of supply chain security management systems. This International Standard contains principles and requirements for bodies providing the audit and certification of supply chain security management systems according to management system specifications and standards such as ISO 28000. It defines the minimum requirements of a certification body and its associated auditors, recognizing the unique need for confidentiality when auditing and certifying/registering a client organization.[7]

Certification of supply chain security management systems is a third party conformity assessment activity. Bodies performing this activity are therefore third party conformity assessment bodies, named certification body/bodies. Certification of supply chain security management systems of an organization is one means of providing assurance that the organization has implemented a system for supply chain security management in line with its policy. Certification of supply chain security management systems will be delivered by certification bodies accredited by a recognized body, such as IAF members.[7]

ISO 28004 documents, including parts 1-4, provides generic advice on the application of ISO 28000:2007. It explains the underlying principles of ISO 28000 and describes the intent, typical inputs, processes and typical outputs, for each requirement of ISO 28000. This is to aid the understanding and implementation of ISO 28000. [8]

ISO/PAS 28005 Documents, including parts 1-2, provides necessary guidance information related to electronic port clearance (EPC), such as message transmission requirements, business scenarios, message structures and software requirements and technical specifications that facilitate efficient exchange of electronic information between ships and shore for coastal transit or port calls. They contains the definition of core data elements for use in electronic port clearance (EPC) messages and defines XML message structures for transmission or information between a ship or its

There are several reasons why an organization should use these standards. Some of the key benefits include:

- Prove your advanced approach to transport security
- Integrated enterprise resilience and Greater compliance processes
- The implementation of an efficient Security Management System
- Pool available transport security standards in one unified management system
- Systematized management practices
- Enhanced credibility, trust and brand recognition
- Improved partner, customer and stakeholder confidence and assurance
- Optimize your processes and ensure that the supply chain remains free of disruptions
- Aligned terminology and conceptual usage
- Improved supply chain performance and Reduced regulation costs
- Benchmarking against internationally recognizable criteria
- Present yourself as a professional partner to customers, authorities, and investors
- Competitive advantage and market differentiation

ISO 28000 standard, has been developed in response to demand from industry for a security management standard. Its ultimate objective is to improve the security of supply chains. It is a high-level management standard that enables an organization to establish an overall supply chain security management system. It requires the organization to assess the security environment in which it operates and to determine if adequate security measures are in place and if other regulatory requirements already exist with which the organization complies. [1]

ISO 28001 standard, has been developed to allow an individual organization in the supply chain to apply its requirements in conformance with the organization's particular business model and its role and function in the international supply chain. This international standard provides an option for organizations to establish and document reasonable levels of security within supply chains and their components. It will enable such organizations to make better risk-based decisions concerning the security in those supply chains. The use of this International Standard will help an organization to establish adequate levels of security within those part(s) of an supply chain which it controls. It is also a basis for determining or validating the level of existing security within such organizations' supply chain(s) by internal or external auditors. [2]

2) Supply chain security management system standards

The recent concerns have led to the development of multiple initiatives and potential solutions to enhance security and resilience in international supply chains without affecting efficiency. [3]

One of these solutions is developing a collection of standards that include requirements, specifications, guidelines and methodologies for achieving to security and resilience with most cost-effective and reliable measures that will be introduced, in brief.

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies. The work of preparing International Standards is normally carried out through ISO technical committees. Collection of ISO 28000 standards was prepared by Technical Committee ISO/TC 8, Ships and marine technology, in collaboration with other relevant technical committees responsible for specific nodes of the supply chain. Therefore ISO solved our problems about security management systems for the supply chain with following standards:[5]

	Standard No.	Title
1	ISO 28000: 2007	Specification for security management systems for the supply chain
2	ISO 28001: 2007	Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans- Requirements and guidance
3	ISO 28002: 2011	Security management systems for the supply chain- Development of resilience in the supply chain- Requirements with guidance for use
4	ISO 28003: 2007	Security management systems for the supply chain- Requirements for bodies providing audit and certification of supply chain security management systems
5	ISO 28004-1:2007	Security management systems for the supply chain- Guidelines for the implementation of ISO 28000- Part 1: General principles
6	ISO/PAS 28004-2:2012	Security management systems for the supply chain- Guidelines for the implementation of ISO 28000- Part 2: Guidelines for adopting ISO 28000 for use in medium and small seaport operations
7	ISO/PAS 28004-3: 2012	Security management systems for the supply chain- Guidelines for the implementation of ISO 28000- Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports)
8	ISO/PAS 28004-4: 2012	Security management systems for the supply chain- Guidelines for the implementation of ISO 28000- Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective
9	ISO/PAS 28005-1:2012	Ships and marine technology- Electronic port clearance (EPC)- Part 1: Message structures- Implementation of a maritime single window system
10	ISO 28005-2:2011	Security management systems for the supply chain - Electronic port clearance (EPC) - Part 2: Core data elements
11	ISO 20858: 2007	Ships and marine technology- Maritime port facility security assessments and security plan development

Table 1. supply chain Security management systems Related Standards

their related services. [1,2]

For many companies, the supply chain is their lifeblood and can commonly hold very high worth of cargo at any given time. With this much value passing through the hands of third parties, it is vital that cargo arrive at its destination safely and on-time. Security means “any resistance to intentional, unauthorized act(s) designed to cause harm or damage to, or by, especially in this paper the supply chain”.[1]Security concerns are an issue that has gained increased importance in supply chains. Supply chain security refers to efforts for enhancing the security of the supply chain. It combines traditional practices of supply chain management with the security requirements of the system, which are driven by threats.

Security, its demands and constraints, constitute obstacles (logical and physical barriers) in the flow of supply and distribution. These “barriers” created by a perceived increased need for security, or political reasons, reduce the reaction capacity and the physical and economical performance of the company. Integrating the security dimension into the logistics strategy, organization and operations has become a new challenge for supply chain management.

Security incidents against supply chains are threats to trade and the economic growth of trading nations. People, goods, infrastructure and equipment - including means of transport - need to be protected against security incidents and their potentially devastating effects. Such protection benefits the economy and society as a whole. Supply chains are highly dynamic and consist of many entities and business partners. [1]

Security management is defined as “systematic and coordinated activities and practices through which an organization optimally manages its risks and the associated potential threats and impacts there from”.[3]

For implementation of supply chain security management system, organizations should develop a supply chain security process, Therefore they need to conduct a security risk assessment that documents the vulnerabilities of the supply chain to defined security threat scenarios. This paper presents a methodology for security risk assessment and development of countermeasures.

Resilience is defined as “the ability to react to unexpected disruption and restore normal supply network operations”. A secure supply chain is not necessarily a resilient supply chain , therefore supply chain networks should be designed network for suitable levels of both security and resilience.[4] To ensure resilience in the supply chain, organizations must engage in a comprehensive and systematic process of prevention, protection, preparedness, mitigation, response, continuity and recovery. This paper presents a process approach for resilience management in the supply chain.

Security risk assessment and resilience methodology for supply chain security management system (SCSMS)

Mostafa Tamtaji

تاریخ دریافت: ۹۱/۱۰/۲۵
تاریخ پذیرش: ۹۱/۱۲/۲۶

Abstract:

Security and resilience are supply chain management issues that have grown in importance, particularly in recent years. Implementation of supply chain security management system (SCSMS) based on comprehensive standards is a good way for insuring the managers that security and resilience process are under control.
Experience has shown that a good understanding of risk assessment and risk management and using an appropriate methodology for risk assessment and also developing an effective resilience plan are often critical to the successful implementation of SCSMS.
After presenting the concepts of supply chain, security management and resilience management ,This paper introduce available standards about supply chain security management, their benefits, applications and approaches.
Then a recommended methodology for security risk assessment will be described. In addition, an applicable plan for relicense management in the supply chain will be presented.
Finally, this paper suggest that during the implementation of SCSMS based on mentioned standards, organizations should pay special attention to challenges such as selecting adequate measures, risk assessment methodology and resilience management.

Keywords:

Supply chain, security management, security standards.

1) Introduction

Supply chain is defined as “linked set of resources and processes that -upon placement of a purchase order- begins with the sourcing of raw material and extends through the manufacturing, processing, handling and delivery of goods and related services to the purchaser (end user) across the modes of transport”. Supply chain may include vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers and other entities that lead to the end user or involved in the manufacturing, processing, handling and delivery of the goods and