ارزیابی ریسک سیستم سیگنالینگ با استفاده از رویکرد تجزیه و تحلیل مخاطرات سیستم های پیچیده ریلی

نجمه بلبل امیری[۱]، محمدعلی صندید زاده [۲]

[۱]دانشجوی مقطع کارشناسی ارشد رشته مهندسی ایمنی در راه آهن، دانشگاه علم و صنعت ایران، Najmeh.amiri@gmail.com

[۲]عضو هیئت علمی دانشکده مهندسی راه آهن دانشگاه علم و صنعت ایران

چکیده

سیستم های بحرانی می بایست در مقابل نیازمندی های ایمنی به منظور عملکرد کارا و بلادرنگ، معتبر شوند. به عبارتی هدف یافتن نیازمندی های کمی و کیفی ایمنی برای سیستم می باشد. کمیته های بین المللی نظیر CENELEC استانداردهایی جهت تعریف چرخه زندگی یک سیستم و تکنیک های مورد استفاده در تمامی فازهای فرایند توسعه سیستم تعریف کرده است. با توجه به آن، یک رویکرد دقیق به منظور پوشش تمامی جنبه های یک سیستم پیچیده از بعد توسعه ایمنی مورد نیاز است.

مقا له فوق، ابتدا رویکرد شناسایی و آنالیز مخاطرات یک سیتم را شرح می دهد. با توجه به رویکرد، تمامی اجزای ساختاری و کارکردی سیستم و تعاملات موجود، شناسایی و ارزیابی می شود. سپس سناریوهای ممکن مخاطرات شناسایی می گردد که پس از تجزیه تحلیل در یک سری جلسات، در یک log به همراه mitigations (شاخص های کاهش) ثبت می گردد. در واقع شاخص ها به عنوان نیازمندی های جدید سیستم تعریف می شوند.

سپس یک چهارچوب کلی برای ارزیابی ریسک ارائه می شود، که شامل فعالیت های فوق می باشد: تعریف سیستم، شناسایی مخاطره، تعریف معیار قابل پذیرش ریسک، آنالیز پیامد و خسارات و در خاتمه ارزیابی ریسک. سیستم مزبور کل نگر است و از دید تکنولوژیکی تمامی فاکتورهای انسانی و کارکردی را نیز پوشش می دهد.

در خاتمه چند مطالعه موردی در زمینه سیستم سیگنالینگ، با استفاده از رویکرد فوق ارائه شده است.

کلمات کلیدی: سیستم سیگنالینگ، تجزیه و تحلیل مخاطرات، ارزیابی ریسک، معیار قابل تحمل ریسک، نیازمندی های ایمنی

مقدمه

ایمنی یک پیش نیاز است. مدیریت ایمنی و توسعه تکنیک هایی به منظور پیش بینی عملکرد ایمن سیستم های ریلی، یک ابزار سیستمی محسوب می شود.

سیستم سیگنالینگ، به عنوان کنترل کننده فاصله بین قطارها، سرعت قطار و مسیر در یک ایستگاه، نقش عمده ای در ایمنی و پایداری سرویس های ریلی بر عهده دارد. سیستم فوق الذکر از زیر سیستم هایی تشکیل شده است که هریک با توجه به آمار حوادث ریلی گذشته، با شاخص ها بهینه شده اند. اگرچه زیر سیستم ها به منظور تضمین ایمنی و سایر نیازمندی های مربوطه بهینه شده اند، اما سیستم سیگنالینگ لزوما در زمینه قابلیت اطمینان، دسترس پذیری، نگهداشت و ایمنی یا به طورکلی RAMS[۱] بهینه نشده است. بنابراین به منظور برآورد نیازمندیهای کل سیستم، روشی مبتنی بر آنالیز نیازمندی ها ارائه می گردد.

استانداردهای ایمنی برای سیستم سیگنالینگ توسط ECELEC[۲] کمیته اروپایی طبقه بندی اصطلاحات و قواعد فنی الکتریکی به شرح زیر ایجاد شده است[۱]:

EN50126: تعیین مشخصه های قابلیت اطمینان، دسترس پذیری، نگهداشت و ایمنی.

EN50128: نرم افزار برای سیستم های حفاظت و کنترل ریلی

EN50129: سیستم های الکترونیک مربوط به مصارف ایمنی برای سیگنالینگ

EN50159: ارتباطات ایمنی در سیستم مخابرات

با توجه به فرضیات استاندارد فوق، وجود پارامترهای کافی جهت جلوگیری از خطا (نظیر حفاظت در برابر خرابی های سیستماتیک) و شاخص های کنترل خرابی های تصادفی لازمه ایمنی سیستم می باشد. به عبارتی CENELEC در راستای یک تعریف ریسک محور از ایمنی می باشد.

CENELEC یک فرایند برای آنالیز مخاطرات و ریسک پیشنهاد کرده است که در استاندارد EN50129 بیان شده است.

ابتدا به رویکرد شناسایی مخاطرات سیستم پرداخته و سپس یک نمونه مطالعه موردی در زمینه فوق، ارائه می گردد.

فرایند شناسایی مخاطرات

[۱] Reliablity, Availability, Maintenance, Safety

[۲] European Committee for electro-technical standardization

فاز اول آنالیز مخاطرات، شامل سه فعالیت زیر می باشد[۲]:

۱. تقسیم بندی سیستم به ماژول ها
۲. انتخاب تکنیک شناخت مخاطرات برای هر ماژول
۳. شناسایی سناریوهای مخاطرات در هر workshop

در ادامه ماژول ها و تکنیک های شناخت مخاطرات مربوط به آن ها آورده شده است.

خروجی فرایند شناسایی مخاطرات, مجموعه ای از مخاطرات آشکار شده[۳] می باشد که در مرحله بعد، حالت[۴] مخاطرات، مطابق رویه ی منطبق با استاندارد CENELEC 50126، می بایست به بسته[۵] تغییر یابد.

ماژول۱: آنالیز عملکردی[۶]

در آنالیز عملکردی سطوح سیستم تنها از بعد ساختار عملکردی بررسی می گردد. مشخصه های عملکردی اسکن می گردد تا عملکردهایی که باید رد شود شناسایی گردد. فرایند شناسایی شامل دو مرحله می باشد:

۱. پس از انجام آنالیز مخاطرات یا PHA[۷]، وضوح و کاربرد مخاطرات شناسایی شده برای ماژول آنالیز عملکردی، بررسی می گردد. از طرفی سناریوی مخاطرات شناسایی شده و علل مربوطه نیز در دفتر ثبت گزارشات[۸] مربوط به مخاطرات ثبت می شود.

۲. فعالیت HAZOP: یک سری کلمات کلیدی به منظور شناسایی تمامیِ حالات خرابی سیستم، بکار می رود. کلکات کلیدی برای هر عملکرد سیستم تعریف می شود. مثالی از کلمات کلیدی در جدول ۱ آمده است :

جدول ۱: جدول کلمات کلیدی برای عملکرد سیستم

کلمه کلیدی	مفهوم
Not	هدف کارکردی حاصل نمی شود یا جنبه عملکردی سیستم قابل وصول نیست.
Less	یک کاهش کمی در هدف کارکردی سیستم ایجاد می شود.
More	یک افزایش کمی در هدف کارکردی سیستم ایجاد می شود.
Early	آغاز عملکرد سیستم، در زمان غلط یا خارج از سکانس است.
Late	مثل Early

ماژول ۲ : آنالیز تعامل سطوح مختلف سیستم با محیط

این ماژول تمامی علل محیطی که بر خرابی سطوح سیستم موثرند را در بر می گیرد. نظیر نگهداری مسیر و قطار، واسطه های خارج سیستم، بحران طبیعی...

به منظور شناسایی مخاطرات فاز فوق، با بهره گیری از یک رویکرد سیستماتیک، انحراف برخی سیستم ها از رفتار اسمی شان تعیین می شود. این انحراف که ناشی از تعامل سیستم با محیط اطراف می باشد، از طریق آنالیز دیاگرام اتصال داخلی[۹]، شناسایی و کد گذاری تعامل بین زیر سیستم ها و تعامل زیر سیستمها و محیط، براورد می شود.

ماژول ۳: معماری سیستم[۱۰]

در این مرحله سیستم به زیر سیستم ها و مجموعه تعاملات تقسیم می شود. شناسایی مخاطرات از دو بخش تشکیل شده است:

۱. شناسایی مخاطرات زیر سیستم ها
۲. شناسایی مخاطرات ناشی از تعاملات

۳,۱. شناسایی مخاطرات زیر سیستم ها

به طور کلی، رویکرد مورد بحث شناسایی مخاطرات سیستم، برای زیر سیستم ها هم قابل کاربرد است. بدین منظور تمامی مخاطرات در سطح سیستم می بایست مدنظر قرار گیرند و مخاطرات مزبور در محصول خروجی سیستم، بسته گردند. از طرفی شرایط ایمن که به منظور کاربری ایمن محصول می بایست مد نظر قرار گیرد، در سطوح زیر سیستم ها نیز، لحاظ می گردد.

۳,۲. شناسایی مخاطرات ناشی از تعاملات

در فرایند شناسایی مخاطرات، چندین نوع تعاملات مطرح است:

A: تعاملات بین زیر سیستم ها : از طریق آنالیز دیاگرام اتصال داخلی تعامل بین زیر سیستم ها شناسایی و کد گذاری می شود.

B: تعامل سیستم با محیط اطراف: از طریق آنالیز دیاگرام اتصال داخلی تعامل بین زیر سیستم و محیط شناسایی و کد گذاری می شود.

C: تمامی تعاملات درونی سیستم با عملیات نصب، پیکربندی، نگهداری و عملکرد نرمال.

فرایند شناسایی مخاطرات ناشی از تعاملات، بر اساس کلمات کلیدی موجود در CENELEC 50159 انجام می شود. کلمه کلیدی متناظرِ هر تعامل، در جدول ۲ آمده است. برای نمونه، اگر عبارت کلیدی REPETITION برای یک پروتکل ارتباطی بکار رود، تحقیقی پیرامون علل کلیه عوامل، نظیر دریافت پیام تکراری و تاثیرات ناشی از آن، نظیر آور رایت اطلاعات مهم، تاخیر در جزییات داده ها.. باید انجام گردد.

---

۳ Open
۴ Close
۵ European Committee for electro-technical standardization
۶ functional analysis
۷ preliminary hazard analysis
۸ Log
۹ Interconnection Diagram
۱۰ System Architecture

جدول ۲: کلمات کلیدی تعاملات سیستم

Repetition	یک پیام بیش از یک بار دریافت می گردد
Deletion	حذف یک پیام از جریان پیام های ارسالی
Insertion	یک پیام جدید در جریان پیام ها درج می گردد
Resequencing	یک پیام خارج از سکانس مورد نظر دریافت می گردد
Corruption	اطلاعات حاوی پیام بطور تصادفی یا بالعکس تغییر می کند
Delay	پیام ها با تاخیر دریافت می گردد.
Masquerade	یک پیام غیرمعتبر به منظور معتبر جلوه کردن طراحی شده است(یک پیام معتبر پیامی است که اطلاعات آن از منبع معتبر استخراج شده است)

[۱۱] لوگ و جلسات مربوط به مخاطرات

رویکرد آنالیز مخاطرات از یک سری جلسات تشکیل شده است که در آن یک تیم چندگانه با ارائه گستره وسیعی از تجارب، به منظور شناسایی مخاطرات و اقدامات احتیاطی ایمن و حفاظتی اجماع می کنند.

دو نوع از جلسات عبارتند از:

۱. جلسات شناسایی مخاطره[۱۲]

۲. جلسات مرور و بستن مخاطره[۱۳]

در نوع ۱، تمامی ماژول هایی که تشریح گردید، با استفاده از طوفان مغزی[۱۴] به منظور زیر و رو کردن کل سیستم، بررسی می گردد. مجموعه ای از سناریو های مخاطرات مد نظر قرار می گیرد و اگر قابل کاربرد در سیستم باشد در لوگ ثبت می گردد.

لوگ حاصله در خاتمه کار تیمی، در جلسه مرور و بستن مخاطره، بررسی می شود. در این جلسات پس از بررسی مخاطرات، قسمت های مختلف سیستم که نیازمند تغییر و توسعه می باشد و نیز اطلاعات مربوط به شاخص های کاهش، اقدامات لازم و منابع و مدارک رویه بستن مخاطرات تشریح می شود.

لوگ طی دوره تیمی فوق الذکر، یک سند قابل تغییر می باشد، بطوریکه هر زمان که اطلاعات جدید از سیستم و یا عناصر آن بدست آید، تغییرات مزبور اعمال می گردد. ساختار لوگ و تمامی حالات ممکن مخاطره، به ترتیب در جدول ۳ و۴ آورده شده است.

تغییر در حالت، نیازمند پذیرش گروه می باشد. مخاطراتی که لغو[۱۵] یا بسته شده اند، نیازمند کار بیشتر نیستند.

[۱۶] فرایند اقدامات لازم پس از شناسایی مخاطرات

هنگامیکه در رابطه با مخاطرات شناسایی شده، اطلاعات حاصله حاکی از حادثه آفرین بودن مخاطرات تشخیص داده شد، ضرورت اقدامات طی جلسات مطرح می شود. در این حالت، یک شخص مسئولیت تکمیل اقدامات را به عهده می گیرد و با سایر اعضای تیم پیرامونِ فرمت کار و اطلاعات پشتیبانی مربوطه به توافق می رسد (action form). یک موعد مقرر[۱۷] با توافق تیم در جلسات، مشخص می شود. اقدامات در لوگ تراک بندی می شود.

اقدامات بر دو نوع است:

۱. تغییر در طراحی، مجموعه ای از رویه ها یا دستورالعمل های عملیاتی

۲. فراهم آوردن مدارک کافی، مبنی بر اینکه طراحی، مجموعه ای از رویه ها یا دستورالعمل های عملیاتی، از کارایی لازم برخوردارند.

از طرفی اقذامات، به منظور ارزیابی جزیی تر ریسک نیز بکار می رود.

اقدامات مربوط به مخاطرات، به صورت فرم هایی در برگیرنده اطلاعات زیر به مسئول مربوطه ارسال می گردد:

مرجع مخاطره: یک شماره منحصر به فرد که در لوگ ثبت شده است.

منشا مخاطره: عنوان یاتوصیف مخاطره

حالت: سه حالت مجاز عبارتند از: جدید، مرور شده و غیرقابل قبول

توصیف مخاطره: علت و معلول مشروح در لوگ

پیشبرد کار از طریق اقدامات: یک روش مورد توافق گروه به منظور اجرا و اتمام اقدامات

شخص مسئول: این شخص تضمین می کند که اطلاعات مورد نیاز جهت تضمین اینکه شاخص های کاهنده مخاطرات تامین شده است، فراهم شده است.

موعد مقرر

پاسخ دهی اقدامات: شخص مسئول اطلاعات لازم و کافی جهت فراهم کردن مدارک پشتیبانی از بسته شدن مخاطرات، را تامین می کند.

تاریخ و امضا: از شخص مسئول

بررسی واکنش: مرورگر، جهت تعیین کار بیشتر یا تضمین کارایی اقدامات توضیح بیشتر می دهد.

شکل۱ فرایند مدیریت رویه مزبور را نشان می دهد.

---

[۱۱] hazard workshop & log

[۱۲] hazard identification workshop

[۱۳] hazard workshop & log

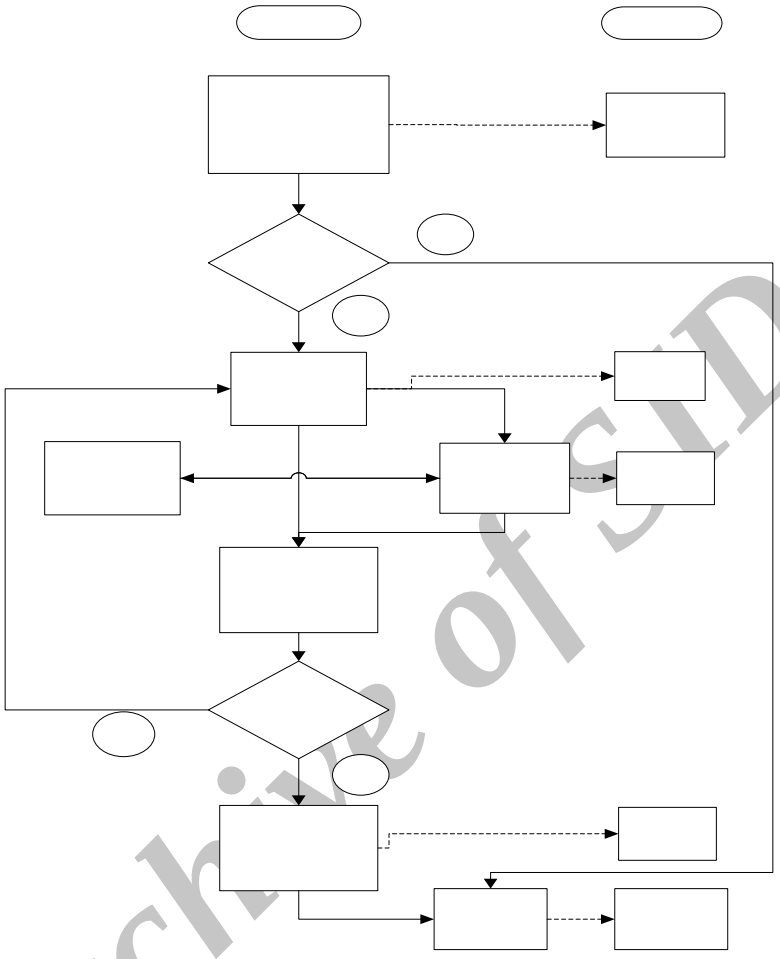
[۱۴] brainstorming

[۱۵] Cancel

[۱۶] Hazard action process

[۱۷] Due Date

شکل۱: فرایند مدیریت اقدامات



فرایند بسته شدن مخاطرات[۱۸]

بر لسلس فرایند فوق تغییر حالت مخاطره شناسایی شده به باز، بر اساس ارزیابی های زیر امکان پذیر است:

۱. بحرانی بودن مخاطرات
۲. کارایی شاخص های کاهندهِ پیشنهادی
۳. اثباتِ اینکه شاخص ها در سیستم نهایی به طور صحیح بکار بسته شده اند.

در رویکرد پیشنهادی، به منظور تعیین قابل قبول بودن سناریوی مخاطره، ارزیابی بحرانی بودن مخاطره براساس پیامد مخاطره، صورت می گیرد. اگرچه در حالت نرمال، برای این منظور، استفاده از نرخ تناوب و شدت اثر بکار می رود، اما استفاده از نظر کارشناسان ریسک مبنی بر مد نظر قراردادن مخاطره یا عدم آن، ارجح است.

پس از بکارگیری شاخص ها، یک ارزیابی مهندسی روی قابلیت کیفیتیِ آن، مبنی بر چگونگی ممانعت از وقوع مخاطره یا کاهش پیامد آن به یک سطح ایمن، انجام می شود. این ارزیابی بر دو نوع می باشد:

۱. **کیفی**: بر اساس تجربه شرکت کنندگان جلسات، شاخص از لحاظ قابلیت کاهش مخاطره مورد بررسی قرار می گیرد.
۲. **کمی**: یک ارزیابی کمی بر اساس روش FTA[۱۹] یا آنالیز درخت خطا، صورت می گیرد و احتمال وقوع هر رویداد تعیین می گردد.

به مجرد اینکه مخاطره پس از اجماع مثبت بود، حالت آن به رفع شده[۲۰] تغییر می یابد.

[۱۸] Hazard closure process

[۱۹] Fault tree analysis

[۲۰] Resolved

یک شاخص، یک نیازمندی ایمنی برای سیستم محسوب می شود. بنابراین آنالیز مخاطرات ضرورت بکارگیری نیازمندی های جدیدی را برای سیستم فراهم می کند.

وقتی تمامی مدارک گردآوری شد، لوگ بسته می شود.

مثالی از لوگ

رویکرد پیشنهادی فوق الذکر، برای سیستم های مختلف با سطوح مختلف پیچیدگی بکار می رود. نظیر:

۱. محصولات سخت افزاری با نرم افزار ساده مثل سوزن یا مدار راه.
۲. محصولات سخت افزاری با نرم افزار پیچیده مثل بالیس یا تجهیزات on-board.
۳. سیستم مرکب از محصولات مختلف و پروتکل های ارتباطی مثل واحد اینترلاکینگ مرکزی و on-board.
۴. سیستم های کامل مرکب از چندین زیر سیستم مثل سیستم حفاظت کنترل اتوماتیک و سیستم اینترلاکینگ ایستگاه مترو
۵. ارزیابی ایمنی از قوانین و رویه ها مثل رویه های نگهداری و تعمیرات

در ادامه کاربرد رویکرد فوق برای سیستم کنترل/فرمان قطار ERTMS/ETCS آورده شده است. در سیستم نوین، سیستم سنتی سیگنالینگ با مخابرات رادیویی شبکه GSM-R جایگزین شده است. زیر سیستم RBC[۲۱] از سیستم جدید، اطلاعات را از فیلد جمع آوری و پیام GSM را به زیر سیستم کنترل اتوماتیک قطار یا ATC ارسال می کند. سه جزء سیستم فوق الذکر عبارتند از:

۱. RBC
۲. سیستم GSM-R (MSC[۲۲]، BSC[۲۳])
۳. قطار

پس از شناسایی و آنالیز مخاطرات بر اساس روش PHA ، از کارشناسان سایر زمینه ها، ۱۵ جلسه به منظور پوشش تمامی مخاطرات احتمالی سیستم برقرار شد که ماحصل آن یک لوگ بیش از ۳۰۰ مخاطره به شرح زیر می باشد :

۱. مخاطرات لغو شده، زیرا جزء مخاطرات بحرانی نبوده اند. مثل تاخیر در حرکت.
۲. مخاطراتی که پس از شناسایی و مستند سازی شاخص های کاهنده، بسته می شوند. به عنوان مثالی برای این دسته شاخص ها می توان به رویه ها (برای عملکرد، نگهداری و تعمیرات..)، تغییر در مشخصه ها (مثلا مشخصه جدید پروتکل ها، مقادیر متفاوت پارامترها..) یا نیازمندی های SIL[۲۴] برای زیر سیستم و اجزا اشاره کرد.
۳. مخاطرات باز که نقطه بحرانی سیستم می باشد و می توان به عملکرد انسانی اشاره کرد که رویه های خاصی می بایست بهبود یابند و ارزیابی شوند.

بدین ترتیب، انواع مخاطرات شناسایی گردید تا در صورت لزوم، در مرحله بعد اقدامات اصلاحی تعیین و انجام گردد.

در ادامه یک رویکرد کلی برای ارزیابی ریسک مطرح می شود که رویکرد فوق برای مطالعات موردی مختلف، با پیروی از یک فرایند مشابه اما تحت شرایط مختلف، بکار بسته شده است[۳] [۴].

اپراتور بانفوذ سیستم ریلی، وظیفه آنالیز ریسک را بعهده دارد که شامل فعالیت های زیر می باشد:

۱. تعریف سیستم(عملکرد، مرز سیستم، تعامل..)
۲. تعریف نیازمندی های سیستم ریلی
۳. شناسایی مخاطرات وابسته به سیستم
۴. استنتاج نرخ قابل پذیرش ریسک[۲۵]
۵. اطمینان از اینکه ریسک حاصله، با توجه به معیار قابل پذیرش، قابل تحمل است.

تعریف سیستم، نیازمندی های آن و همچنین مخاطرات وابسته در بالا تشریح گردید. در ادامه به شاخص های پذیرش ریسک به طور مختصر اشاره می گردد تا سطح تحمل ریسک سیستم تعیین گردد.

معیار پذیرش ریسک

وظیفه عمدهٔ معیار فوق پاسخ به پرسش "چطور ایمنی، به قدر کافی ایمن است؟" می باشد. البته تاکنون جواب قابل قبول جهانی برای پرسش فوق یافت نشده است.

CENELEC EN50126 سه معیار پیشنهاد می کند:

۱. ALARP[۲۶]
۲. GAME[۲۷]
۳. MEM[۲۸]

ALARP ریسک را به سه زیرشاخه تقسیم می کند:

غیرقابل پذیرش: ریسک بالا و غیر قابل تحمل می باشد. مثل از کار افتادگی سیستم.

قابل پذیرش: ریسک پایین و بدون هیچ پرسشی قابل پذیرش است.

بینا بین: می بایست نشان داد که کاهش بیشتر ریسک نشدنی است. در اینجا یک مقدار برای مرگ و میر پیش گیری شده، در آنالیز سود- هزینه حاصل می شود.

روش ALARP بدلیل هزینه بالای پیشگیری از مرگ و میر، در بسیاری از کشورهای اروپایی غیرقابل پذیرش است.

---

[۲۱] Radio block centre
[۲۲] Mobile Switching centre
[۲۳] Base Station centre
[۲۴] Safety integrity level
[۲۵] Hazard tolerability criteria
[۲۶] As low as reasonably practible
[۲۷] Globalment as moins equvalant
[۲۸] minimum endogenous mortality

GAME یعنی تمامی سیستم های جدید حمل و نقل می بایست یک سطح از ریسک را پیشنهاد کنند که حداقل به خوبی سطح پیشنهاد شده از هریک از سیستم های معادل موجود می باشد.
MEM یعنی به هر سیستم ریلی نباید اجازه داده شود که ریسک مرگ و میر سالیانه بیش از ۵-۱۰ باشد. بر اساس آمار موجود در اروپای غربی، در هر گروه سنی از جمعیت سالانه حدود ۲/۱۰۰۰ مردم می میرند که این ثابت به عنوان MEM شناخته شده است.
MEM تاکنون برای سیستم سیگنالینگ ریلی بکار گرفته نشده است و تنها برای مطالعات تحقیقاتی می باشد.

رویکرد سنتی

به طور کلی تکنیک ارزیابی ریسک با سنجش دو بعد و ترکیب خروجی، یک سطح کلی از ریسک ارائه می دهد. این دو بعد عبارتند از:

۱. احتمال اینکه یک مخاطره منجر به حادثه گردد؟
۲. در صورت وقوع یک سانحه، شدت اثر پیامد آن چقدر است؟

ارزیابی ریسک به سه قسم کیفی، شبه کیفی و کمی انجام می گیرد که بسته به نوع سیستم و میزان اهمیت، نوع آن تعیین می شود.

روش کیفی سریع است اما عموما جزییات ناکافی به منظور پشتیبانی از ارزیابی فراهم می کند. در عوض نتایج حاصل از کمی جزیی و کامل اند. اگرچه محدودیت در دسترس بودن داده ها موجود است. همچنین در روش شبه کیفی، یک مقدار عددی نسبی به مخاطره تخصیص می یابد.

عمومی ترین رویکرد ارزیابی ریسک، ماتریس ارزیابی ریسک می باشد که به صورت یک مثال در CENELEC EN50126 بکار گرفته شده است و توسط MIL-STD-882D، مادر تمامی استانداردهای ایمنی، توصیه شده است. این دو استاندارد در واژه متفاوت، اما در رویکرد مشابه اند.

مدل ماتریسی ارزیابی ریسک یک ابزار غربالگر کیفی مبتنی بر دانش تلقی می شود که به رده بندی احتمال و پیامدهای محتمل درطی اجرای عملیات می پردازد در واقع یک ابزار تصمیم سازی برای مدیران می باشد.
سطح ریسک می تواند قابل پذیرش، غیر قابل پذیرش و یا قابل پدیرش مطابق دستور باشد (جدول ۳)

جدول ۳: ماتریس ارزیابی ریسک

تناوب وقوع یک رویداد مخاطره آمیز	**Risk Level**			
Frequent	۱۰	۶	۳	۱
Probable	۱۴	۹	۵	۲
Occasional	۱۸	۱۳	۸	۴
Remote	۲۱	۱۷	۱۲	۷
Imporable	۲۳	۲۰	۱۶	۱۱
Incredible	۲۴	۲۲	۱۹	۱۵
	Insignificant	Marginal	Critical	catastrophic
	شدت اثر وقوع یک مخاطره			

با این حال، ماتریس فوق معایبی به شرح زیر دارد:

۱. اصول کلی برای ایجاد یک ماتریس ارزیابی ریسک منتشر نشده است.
۲. بدلیل عدم وجود یک معیار جهانی قابل پذیرش ریسک، یک ماتریس ریسک منحصر به فرد وجود ندارد و بنابراین ماتریس برای هر کاربرد جدید می بایست سازگار شود.
۳. معمولا دسته بندی احتمال وقوع به طور واضح برای یک قطار در طول چرخه زندگی آن، تعریف نشده است.
۴. بدلیل تمایل به اغراق در شدت اثر ریسک، ریسک بالاتر از معمول براورد می شود.

در ادامه چندین مطالعه موردی در زمینه سیگنالینگ آورده شده است. این موارد جنبه پژوهشی داشته و صرفاً به منظور تشریح رویکرد های تجزیه تحلیل مخاطرات سیستم و ارزیابی ریسک، در قالب مثال آورده شده است. لازم به ذکر است که این پژوهش مقدمه فعالیت های وسیع تری در این مقوله می باشد، که بدلیل محدودیت های مقاله، به آینده موکول می گردد. امید است که مشابه ارزیابی های فوق، بر روی سیستم های ریلی موجود در کشور ، تکمیل و نتایج حاصله در پژوهش های آتی مورد استفاده قرار گیرد.

مطالعه موردی۱: تقاطع جاده و راه آهن

بدلیل فاجعه انگیز نبودن حوادث احتمالی در این بخش، ضرورت اتخاذ بالاترین سطح ایمنی احساس نمی شود. داده های این بخش، مربوط به خرابی بخش تقاطع اتوماتیک، مربوط به راه آهن آلمان می باشد.

با فرض H احتمال خرابی GX در هشدار به مردم و A احتمال تصادف اتومبیل و قطار، ریسک به صورت زیر محاسبه می شود:

A.H =کرانه ریسک قابل پذیرش

کاربرد فرایند ارزیابی مطالعه موردی فوق، در شکل ۱ نشان داده شده است. GAME به منظور تعیین سطح ریسک انتخاب شده است.

ماتریس ارزیابی ریسک به عنوان یک راه حل با فرض آنکه شدت اثر و تناوب وقوع، با توجه به داده ها معلوم است، در جدول۴ آورده شده است.

جدول ۴: ماتریس ارزیابی ریسک برای GX

تناوب وقوع یک رویداد مخاطره آمیز	**Risk Level**			
Frequent	imporable			intolerable

Probable	tolerable	intolerable		
Occasional		tolerable	intolerable	
Remote			tolerable	tolerable
Imporable				intolerable
Incredible	Tolerable			
	Insignificant	Marginal	Critical	catastrophic
	شدت اثر وقوع یک مخاطره			

مطالعه موردی۲: کنترل کم هزینه قطار

اخیرا راه آهن آلمان یک رویه نوین عملکرد رادیویی، تحت عنوان FFB را توسعه داده است. FFB یک روش سیگنالینگ می باشد و عمده عملکرد حفاظتی و نظارتی آن عبارتند از:

۱. تنظیم هدوی مناسب بین قطار و وسیله نقلیه جهت جلوگیری از تصادف
۲. کنترل سرعت
۳. حفاظت وسیله نقلیه در سوزن و تقاطع جاده-ریل
۴. FFB برخلاف سیستم سنتی اینترلاکینگ نیازمند سیگنال کنار خط، سیستم تشخیص کنار خط مثل مدار راه یا سیستم حفاظت قطار نمی باشد.

در ارزیابی مخاطرات آن، ۳۸ مخاطره در ۷ گروه تعیین گردید که عبارتند از:

تجاوز از سقف سرعت، تشخیص مسیر اشتباه، تخلف از محدوده FFB ، وجود مانع روی خط، وجود قطار دیگر در خط، حفاظت ناکافی از سوزن، حفاظت فرد و وسیله نقلیه در تقاطع.

ارزیابی ریسک که شامل فعالیت های زیر می باشد انجام گردید:

۱. آنالیز پیامد تمامی گروه مخاطرات شناسایی شده با استفاده از آنالیز درخت وقایع یا ETA.
۲. آنالیز آماری میزان خسارات[۲۹] برای تمامی پیامدهای شناسایی شده.
۳. آنالیز قابلیت اطمینان انسانی[۳۰] برای تمامی فعالیت های انسانی
۴. Casual analysis با استفاده از ETA برای ۳۸ مخاطره شناسایی شده با علل تکنیکی و انسانی

با مقایسه آنالیزهای فوق با ریسک هدف، نرخ مخاطره برای علل تکنیکی محاسبه شده و توزیع تخمینی ریسک برای علل ریشه ای به شرح زیر بدست آمد:

۱٪ به علت خرابی های تکنیکی
۲۲٪ به علت خرابی های عامل انسانی در شرایط نرمال عملکردی
۵۳٪ به علت خرابی های عامل انسانی در شرایط تنزیل کارکرد
۲۴٪ سایر

ارزیابی کمی ریسک

ارزیابی کمی ریسک یا QRA[۳۱]، یک پایه برای سرمایه گذاری در ایمنی می باشد و تصمیم گیری در تخصیص منابع به مخاطرات موجود و بهینه سازیِ بازگشت سرمایه را پشتیبانی می کند[۵].

اکثر تصمیم گیری ها به منظور بهبود ایمنی سیستم های سخت افزاری، نیازمند ارزیابی مطلق سطوح ریسک بجای ارزیابی نسبی می باشد و لذا برخی فرم های QRA توصیه می شود. به عبارتی، QRA با شناسایی مخاطراتی که سهم بیش تری در ریسک دارند و تعیین شاخص های کاهش در صورت لزوم، تصمیمات مربوط به ارتقاء ایمنی در صنعت ریلی را پشتیبانی می کند. از طرفی، QRA با ترکیب دو مورد زیر، ریسک را تعیین می کند:

۱. آنالیز تناوب وقوع: با استفاده از آنالیز درخت خطا و آنالیز وقایع، احتمال وقوع علل مخاطراتی که منجر به حادثه می شوند، بدست می آید.
۲. آنالیز پیامد: شدت اثر یک پیامد پس از وقوع یک حادثه بدست می آید، مثل تعداد مرگ و میر.

پس از محاسبه، در صورت تشخیص ضرورت اقدام اصلاحی و با توجه به ساختار ارزیابی ریسک، عللی که مشارکت بیش تری در ریسک دارند و همچنین شاخص های کاهش ریسک تعیین می شوند.

مطالعه موردی۳: ارزیابی کمی ریسک سیگنالینگ یکی از خطوط مسیر

به عنوان مثالی از QRA، انجام فرایند ارزیابی کمی ریسک در مورد سیگنالینگ یک خط از مسیر می باشد که توسط ناحیه کنترل کننده زیرساختارهای انگلستان[۳۲] انجام شده است. ارزیابی فوق اطلاعاتی با عنایت به عملکرد ایمنی موجود در سطوح مختلف بهره برداری از خط فراهم می کند که نشان می دهد عملکرد ایمنی مورد انتظار خط در بعضی سطوح می بایست بهبود یابد.

با مرور ساختار FTA حاصله، مهم ترین عامل ریسک مرگ و میر، SPAD[۳۳] در تقاطع خطوط مسیر می باشد. بنابراین ارزیابی ریسک به منظور بهبود عملکرد ایمنی در گذرگاه همکف انجام گردید. برای این منظور، برای یک تقاطع معلوم موقعیت هایی برای مطالعات بیش تر و تمرکز بهبودها، مشخص می گردد. به عنوان مثال، یکی از زمینه های ارزیابی، ارزیابی ریسک مرگ و میر ناشی از تصادف یا خروج از خط قطار در تقاطع می باشد که در این حالت تقاطع در مرحله طراحی یا هرجا که تغییر ضرورت می یابد ارزیابی می شود. زمینه دیگر تفاوت در آرایش سیستم سیگنالینگ دو وسیله نقلیه می باشد(مثل کارکرد قطارهای سبک بر روی خطوط متعارف سنگین ریلی). ارزیابی ریسک با استفاده از تکنیک فاکتورهای انسانی، به منظور پیش بینی هر تغییری که در نرخ SPAD رخ می دهد انجام می شود و شاخص های کاهش ریسک مثل ATP تست

[۲۹] Statistical Loss analysis
[۳۰] Human reliability analysis
[۳۱] Quantitive risk assessment
[۳۲] UK infrastructure controller zone
[۳۳] Signal passed at danger

می شود. زمینه دیگر توسعه یک رویکرد به منظور اولویت بندی عملیات نگهداری برای واحدهاست که پیامد ناشی از به تعویق انداختن عملیات نگهداری، در قالب ایمنی و میزان خسارات مالی مورد بررسی قرار می گیرد. به عنوان مثال با تعویق تعمیر تهویه ی جعبه سیگنال، تاثیر آن روی ایمنی نامحتمل است، اگرچه هزینه تاخیر در سرویس را متحمل می شود. و برعکس، عدم جایگزینی سطوح ساییده شده ی ایستگاه بر ایمنی تاثیر گذار است، اگرچه تاثیر آن بر سرویس قطار بعید است.

بدین ترتیب تمامی پیامدهای ممکن تعیین می گردد و با توجه به آنالیز هزینه سر به سر، اقدام اصلاحی مناسب تعیین می گردد.

نتایج

همانگونه که ملاحظه گردید، در این مقاله رویکرد ارزیابی مخاطرات سیستم، تعیین نوع مخاطرات و اقدامات مربوطه، تعیین ریسک با استفاده از شاخص های پذیرش ریسک و ماتریس ریسک، دسته بندی ریسک سیستم به منظور رتبه بندی آن و بطورکلی ضرورت ایمنی سیستم های بحرانی، نظیر سیگنالینگ تشریح گردید. همچنین به منظور آشنایی با موارد مطروحه، مطالعات موردی موجود در هر مقوله، که ماحصل پژوهش موجود می باشد به صورت خلاصه بیان گردید. همانگونه که اشاره شد، این مطالعات تنها جنبه آشنایی داشته و مطالعات مشابه، بر روی مخاطرات سیستم ریلی کشور(سیستم سیگنالینگ)، جهت ارزیابی ریسک، با استفاده از رویکرد های فازی تجزیه تحلیل ریسک، توسط اینجانب در حال انجام است که امید است در آینده نتایج حاصله تکمیل و به تحریر درآید.

مراجع

[1]- Berband J., ''European Safety standards for railway signaling systems,'' Proc. 16th International system safety Conference, System safety society, 1998.

[2]- di Tommaso Pasquale, Esposito Rosaria, Marmo Pietro, Orazzo Antonio, Ansaldo Segnalamento Ferroviario S.p.A., ''Hazard analysis of distributed system,'' Proceedings of the 22nd International Symposium on Reliable Distributed Systems, 2003.

[3]- Jens Bernard, Siemens AG Transportation System, Bruinswick(Germany), ''Risk assessment in railroad signaling Experience Gained and Lessons Learned,'' Annual Reliablity and Maintainablity Symposium, 2002.

[4]- S-L. Kurz, B. Milius , ''Negligible risk for European Railway Risk Assessments,'' .

[5]- Richard J. Clarke, Arthur D. Little Ltd, '' Safety pre-requisitive or Just another business issue?'', Electric Railway in United group Conference, 27-30 March 1995.