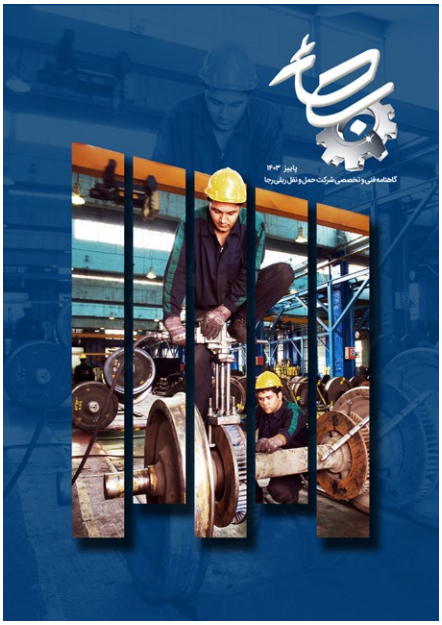
صنعت

گاهنامه فنی و تخصصی شرکت حمل و نقل ریلی رجا
سال شانزدهم - پاییز ۱۴۰۳ - شماره ۳۳

- پیام مدیرعامل: مدیریت و مهندسی دانش و اهمیت آن در سازمان
- مزایای باتری‌های LTO برای قطارهای هیدروژنی
- خطر، شناسایی خطر و تکنیک PHL

فهرست



نشریه فنی و تخصصی شرکت حمل و نقل ریلی رجا

شماره ۳۳ - پاییز ۱۴۰۳

شرکت حمل و نقل ریلی رجا
RAJA RAIL TRANSPORTATION CO

صاحب امتیاز: مدیریت مهندسی و پژوهش

شرکت حمل و نقل ریلی رجا

جانشین مدیر مسؤول و سردبیر: سید مجید افتخاری

شـــورای علـــمی: رضا واحدی، رویا السادات آشفته

مدیرداخلی، ویراستار و صفحه آرایی: ریحانه اردهالی

نشانی: تهران، خیابان شوش، ابتدای خیابان شهیـد رجایی

مدیریت مهندسی و پژوهش، کدپستی: ۱۳۱۳۱ - ۱۱۸۹۸

تلفن دفتر نشریه: ۵۵۱۲۴۵۴۰/ دورنگار: ۵۵۶۵۵۶۶۸

نشانی وب‌گاه: www.raja.ir

پست الکترونیک: engineering@raja.ir

گاهنامه رجا آماده دریافت مقالات، پیشنهادات و انتقـادات سازنده شما می‌باشد.

مدیریت و مهندسی دانش و اهمیت آن در سازمان

مدیریت دانش (Knowledge Management) فرآیند خلق، گردآوری، ذخیره، بازیابی، تسهیم و بکارگیری دانش و اطلاعات در یک سازمان تعریف می‌شود. با توجه به اینکه اطلاعات و دانایی در عصر حاضر حرف اول و آخر را می‌زند، اهمیت این حوزه از مدیریت روشن و بدیهی است. شاید بتوان گفت عنصر اصلی موفقیت در کسب و کارهای کنونی مدیریت دانش است.

در گذشته، صنعت راه‌آهن با سیستم‌های فنی و تکنولوژیکی ساده که تنها شامل تعداد کمی ورودی‌ها و خروجی‌های زیر سیستم‌ها و اجزای ساده می‌شد مواجه بود.

بنابراین، یک مدیر می‌توانست تقریباً به طور کامل آنها را درک و شرایط شکست و عواقب آن را پیش‌بینی کند. اما امروزه سیستم‌های فنی و فن‌آوری راه‌آهن پیچیده هستند و این پیچیدگی سیستم به طور مداوم در حال افزایش است و مدیران را وادار می‌کند تا درک بهتری از چگونگی رفتار سیستم و تأثیر آن بر کیفیت خدمات حمل و نقل ریلی داشته باشند. شایان ذکر است که بدون داشتن یک سیستم مدیریت دانش خوب طراحی شده و سازمان یافته و با توجه به عوامل مؤثر بر کیفیت خدمات راه‌آهن، حتی بهترین طرح‌ها و اهداف نیز می‌تواند بیهوده و بی‌نتیجه بماند.

در دسترس بودن نظام‌مند اطلاعات و اندوخته‌های علمی که تحت عنوان مدیریت دانش شناخته می‌شود روش جدید مدیریت را معرفی می‌کند که منطبق بر اصول علمی بنا نهاده شده است.

آنچه اکنون نیاز صنعت ریلی است، فرآیند مهندسی دانش در سه حوزه‌ی استخراج، تحلیل و مدل سازی دانش است که می‌تواند منجر به تولید یک پایگاه دانش ساختار یافته، مبتنی بر مدل‌های دانش شود. راهبرد خلق دانش تأکید بر نوآوری و آفرینش دانش جدید از طریق واحدهای تحقیق و توسعه دارد.

آنچه در مدیریت دانش اهمیت دارد، توجه به چرخه ی مدیریت دانش نگهداری و تعمیرات (نت) است که مواردی مانند: طرح‌ریزی فرآیند نت، گردآوری منابع و مراجع، اصلاح و به روزآوری دستورالعمل‌های نت، استانداردسازی آنها، طرح‌ریزی نت برنامه ریزی شده، ثبت اطلاعات در نرم افزار نت، به اشتراک گذاری آن و نیز اجرا، بهبود و ارتقای سیستم نت است.

حوادث ناشی از تجهیزات معیوب یا عدم توجه به نکات مهم ایمنی می‌تواند باعث زیان مالی و جانی در یک سازمان شود و این وظیفه‌ی نگهداری و تعمیرات است که تضمین کند این چنین اتفاقاتی در سازمان نیفتد. به علاوه، استفاده از تجاربی که از این حوادث به دست آمده، می‌تواند در کاهش خطرات ایمنی مؤثر باشد. نگهداری و تعمیرات در واقع یک عامل برای حصول عملکرد مناسب و کارآمد در سازمان محسوب می‌شود.

از آثار توقف‌های برنامه‌ریزی نشده قطعات و تجهیزات، از دست دادن زمان خروج واگن، بروز انفصالی های مکرر و عدم پشتیبانی و سرویس مناسب است.

انتشار گاهنامه تخصصی رجا می‌تواند یک قدم مثبت در جهت به اشتراک گذاشتن دانش و تجارب به دست آمده بین کارکنان شرکت و متخصصان صنعت ریلی باشد.

در این راستا مدیریت رجا از مکتوب کردن دانش و انتقال آن بین کارکنان حمایت می‌کند.

ناصر بختیاری
مدیرعامل

رونمایی پاناسونیک در نمایشگاه 2024 Inno Trans از یک سیستم درب پلتفرم کامل

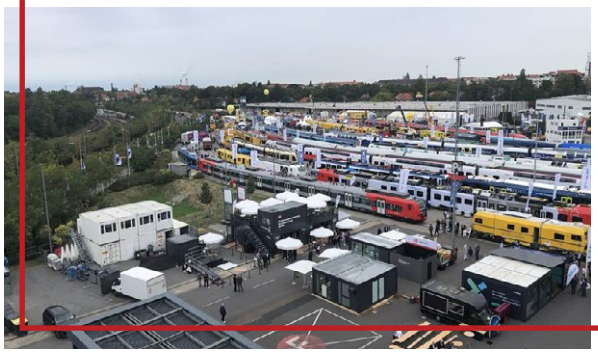
مترجم: مهدی نوری خانیوردو
ویراستار: سید هادی یوسفی

شرکت صنایع پاناسونیک برای اولین بار در اروپا سیستم درب پلتفرم کامل خود را به همراه پنل کنترل و یک سیستم تعمیر و نگهداری هوشمند به نمایش می‌گذارد.

طراحی این درب‌های نسل جدید به گونه‌ای است که به کمک سیستم سیگنالینگ [سیستم علائم الکتریکی] و اتصال به آن موجب کاهش مصرف انرژی می‌شود.

همچنین شرکت صنایع پاناسونیک یک سیستم هوشمند برای نگهداری و تعمیر کارآمد سیستم‌های درب پلت فرم را به نمایش گذاشته است.

خطاها را می‌توان در زمان واقعی وقوع خطا مکان‌یابی و گزارش کرد. توصیه‌هایی نیز برای نگهداری و تعمیر ارائه می‌شود و به پایگاه داده قطعات یدکی و سیستم مدیریت پرسنل تعمیر و نگهداری مخابره می‌شود. کارکنان تعمیر و نگهداری همچنین می‌توانند از عینک‌های AR و سایر دستگاه‌های هوشمند برای تجسم خطاها و دریافت مشاوره تخصصی برای عیب‌یابی از راه دور استفاده کنند.



کوپلینگ (اتصال) اتوماتیک راهروی بین دو قطار و ایجاد قطار اشتادلر (Stadler) جدید

مترجم: مهدی نوری خانیوردو
ویراستار: سید هادی یوسفی

این سیستم سال آینده در کانادا آزمایش خواهد شد. شرکت فن‌آوری راه‌آهن سبک آلمان Hobner، از اولین آزمایش‌های واقعی سیستم کوپلینگ خودکار این شرکت که در سال ۲۰۲۵ در کانادا انجام خواهد شد، رونمایی کرده است.

محصول AutoCouple [اتصال اتوماتیک] در اوایل سپتامبر قبل از عرضه رسمی آن در برلین طی این هفته تست میدانی می‌شود. متروی تورنتو میزبان این ابزار خواهد بود که با هدف استفاده‌ی کارآمدتر از ناوگان موجود و آسان و سریع‌تر کردن روند تغییر طول مؤثر قطارها (بسته به تقاضای مسافران) انجام می‌شود. این شرکت ادعا کرده است که زمان اتصال را می توان از ۳۰ دقیقه به پنج دقیقه کاهش داد. با سیستم کوپل اتوماتیک Hobner، رانندگان قطار می‌توانند با فشردن یک دکمه در یک فرآیند کاملا اتوماتیک، واگن‌ها را از قطار جدا یا به قطار اضافه کنند. در کل فرآیند کوپلینگ قطار باید به شبکه برق متصل بماند. به این ترتیب اپراتورهای حمل و نقل می‌توانند تا ۲۵ دقیقه در هر فرآیند کوپلینگ صرفه‌جویی وقت داشته باشند. به لطف دسترسی سریع‌تر به قطارها و صرفه جویی در هزینه‌های کارکنان، این سیستم ارزش افزوده واقعی ایجاد می‌کند.

فن‌آوری جدید همچنین دخالت انسانی را کاهش داده و اتصال و جداسازی واگن‌های قطار را بسیار ایمن‌تر می‌کند. مدیرعامل این شرکت افزود: سیستم جدید بسیار قوی و بادوام است که در آینده می‌تواند انتقال نیرو را از یک واگن به واگن دیگر تسهیل کند.

الکساندر اشمیت، رئیس نوآوری و توسعه محصول در بخش حمل و نقل ریلی Hobner، در این باره گفت: «برای ما بسیار خوشحال کننده است که اولین نوآوری را ارائه و به اپراتورهای حمل و نقل ریلی در بخش مسافر این امکان داده می‌شود تا در برنامه‌ریزی و سازماندهی خود انعطاف پذیرتر و ایمن‌تر باشند».

«تیم ما در تلاش است تا یک نوآوری سفارشی برای مشتریان ایجاد کند که باعث صرفه جویی قابل توجهی در منابع شود».

مترجم: مهدی نوری خانیوردو
ویراستار: سید هادی یوسفی

مزایای باتری‌های LTO[1] برای قطارهای هیدروژنی

شرکت Saft باتری‌های اکسید تیتانیوم لیتیومی را برای باتری سوختی[2] و سیستم کشش وابسته به باتری، در هفت قطار هیدروژنی کششی چندگانه زیمنس Mobility Mireo Plus H عرضه می‌کند.

باتری‌ها عمدتاً در هنگام شتاب برای جبران محدودیت‌های قدرت سلول سوختی و در هنگام ترمز برای بازیابی انرژی جنبشی استفاده می‌شوند. به عبارت دیگر برای شارژ باتری در هنگام ترمز و کاهش سرعت استفاده می‌شود.

هنگامی که قطار در حال حرکت است، باتری‌ها بار را همگن کرده تا سلول‌های سوختی بتوانند با حداکثر کارایی عمل کنند.

در این راستا مدیرعامل سافت افزود: سافت یکی از معدود شرکت‌هایی است که علم شیمی خود را توسعه داده و این امکان را دارد که محصولات خود را با نیازهای خاص هر مشتری تنظیم کند.

سدریک دوکلوس، مدیر عامل سافت در ۲۷ سپتامبر اعلام کرد: «این پروژه معتبر برای قطارهای Mireo Plus H یک پیشرفت مهم برای این شرکت است. زیرا این اولین بار است که باتری‌های LTO در یک پروژه بزرگ ریلی تجاری حضور دارند.»

این قرارداد با زیمنس موبیلیتی نقطه اوج موفقیت برای یک پروژه توسعه بلند مدت است.

استفاده از این فناوری نوآورانه برای کاربردهای کششی، مزایای قابل توجهی دارد که از آن جمله می‌توان به بهبود ایمنی، افزایش قابلیت اطمینان، انتشار کمتر CO2، افزایش طول عمر و قدرت بیشتر اشاره کرد.

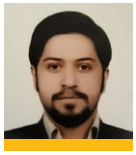
[1] باتری لیتیوم تیتانات یا اکسید لیتیوم تیتانیوم (LTO) نوعی باتری قابل شارژ است. مزیت آن این است که سریع‌تر از باتری‌های لیتیوم یونی شارژ می‌شود.

[2] fuel cell سلول سوختی: نوعی پیل گالوانی که در آن براثر اُکسید شدن سوخت مانند متانول، برق تولید می‌شود.

روش‌هـای تست عایقی و تحلـیل تست میگر در برنامه‌های تعمیراتی ژنراتـور سنکرون در قطارهـای خودکشـش

Insulation System Testing Techniques and Megger Test Analysis in Repair Programs for Synchronous Generator in Multiple-Unit Train

واژه نامه:
قطار پرسرعت ترنست و ریل باس
تسـت عایقـی- تسـت میگر
سیستم‌های تعمـیراتی
ژنراتور سنکرون



حسین فروتن
کارشناس اداره کل اعزام و خدمات راهبری
شرکت حمل ونقل ریلی رجا

چکیده

در این مقاله روش تست عایقی میگر در صنعت و تحلیل آن در برنامه‌های تعمیراتی ژنراتور سنکرون هیتزینگر در قطارهای پر سرعت ترنست ساخت شرکت زیمنس آلمان با کد مشخصه DH4 به مالکیت شرکت حمل ونقل ریلی رجا بررسی می‌شود. با توجه به ساختار موجود و طول عمر ژنراتورهای مورد مطالعه، تحلیل شرایط ژنراتور بسیار حائز اهمیت است زیرا در صورت انجام تعمیرات مناسب می‌توان نسبت به بهینه‌سازی عملکرد ژنراتور اقدام و از بروز قطع برق واگن قطار که مشکلات جدی بوجود می‌آورند جلوگیری نمود.

مقدمه

اتصالی در کابل‌های سیستم قدرت و نیز سیم پیچی‌های روتور و استاتور ژنراتور، قطع شدن برق آن را به دنبال دارد و این قطعی برق در قطارهای پرسرعت ترنست منجر به قطع سیستم تهویه و آسیب به سایر بارهای جریان متناوب از جمله شارژر باتری‌های کنترل می‌شود و این موضوع علاوه بر خسارت‌های مالی به مالک قطار باعث نارضایتی مسافران نیز می‌گردد.

بنابراین، بررسی وضعیت برنامه‌های تعمیراتی موجود و بهینه‌سازی روش‌ها می‌تواند به بهبود خدمت رسانی به مسافرین و پیشگیری از مشکلات سیر منجر گردد.

در این راستا، پس از بررسی شرایط تعمیرات موجود در برنامه‌های تعمیراتی T1 تا T7 ارائه شده توسط شرکت سازنده، می‌توان با اصلاح شرایط و احتمال اضافه کردن تست‌های عایقی غیر مخرب، مشکلات پیش آمده برای ژنراتور را کاهش داد و سیر مطمئنی را برای مسافران مهیا کرد.

بررسی روش آزمون عایقی میگر:

هادی‌ها، فضای بین دورها در سیم‌پیچی‌ها و نیز فضای مابین سیم‌پیچی‌ها و فازها در تجهیزات الکتریکی توسط یک یا چند نوع عایق الکتریکی پر می‌شود. جنس مواد عایقی بسته به کاربرد و نوع تجهیز می‌تواند گاز یا مایع یا جامد یا ترکیبی از مواد عایقی از جنس متفاوت باشد. جهت تعیین کیفیت و محاسبه طول عمر مفید باقیمانده سیستم‌های عایقی در تجهیزات الکتریکی استانداردهای بین‌المللی و ملی روش‌های گوناگونی را توصیه می‌کنند و به تبع آن دستگاه‌های اندازه‌گیری متنوعی برای پیاده‌سازی این روش‌ها در بازار وجود دارد. از جمله دستگاه‌های روتین می‌توان از دستگاه تست میگر نام برد. در ادامه کاربرد این روش معرفی می‌شود.

دستگاه میگر نوعی دستگاه تست عایق قابل حمل می‌باشد. دستگاه میگر برای اندازه‌گیری مقاومت عایقی در تجهیزات الکتریکی استفاده می‌شود و بخشی از برنامه بررسی وضعیت موجود سیستم عایقی می‌باشد.

شکل ۱ نمونه‌ای از دستگاه میگر را نشان می‌دهد.

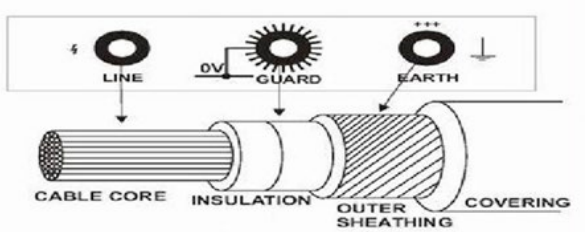
شکل ۱- نمونه‌ای از دستگاه میگر

این تجهیز بین دو نقطه عایقی ولتاژ DC بالایی اعمال می‌کند و براســاس قانون اهم مقاومت بین این دو نقطه را اندازه‌گیــری می‌کند. اندازه مقاومت بدست آمده نشان دهنده سطح عایق یا همان مقاومت عایقی است [۱].

این تست را می‌توان بر روی کابل و ژنراتور قطارهای ترنست اعمال کرد. در ادامه انجام این روش معرفی می‌شود.

مراحل انجام آزمون بر روی کابل:

دستگاه میگر مجهز به سه پایانه شامل پایانه ارت (E)، پایانه گارد (G) و پایانه لاین (L)، است. مطابق شکل ۲، برای اندازه‌گیری مقاومت عایقی یک کابل، باید انتهای لاین دستگاه میگر را به یکی از رساناها متصل کرده و انتهای ارت دستگاه را به سیمی که به دور غلاف کابل پیچیده شده است وصل کرد. متصل کردن پایانه گارد به اولین رسانا، هر دو رسانا را تقریبا در موقعیتی با پتانسیل برابر قرار می‌دهد.



شکل ۲- نحوه‌ی اتصال دستگاه میگر به یک کابل

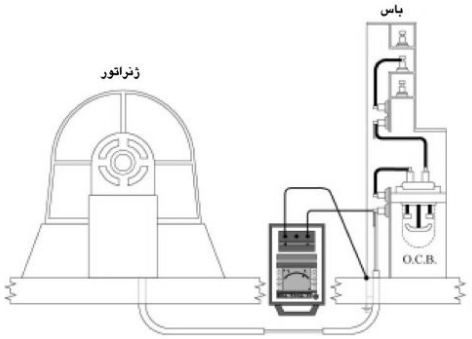
ابتدا باید مطمئن شد که دستگاه به درستی کار می‌کند. برای این کار، اول دستگاه روشن و پروب‌ها متصل می‌شوند. سپس کلید انتخاب ولتاژ در حالت حداقل ولتاژ قرار می‌گیرد و شاسی تزریق ولتاژ حدود ۱۰ ثانیه نگهداشته می‌شود.

دستگاه در این حالت باید مقاومت بی‌نهایت را نشان دهد. این آزمایش در حالت حداکثر ولتاژ دستگاه نیز تکرار می‌شود. سپس، دو پروب به یکدیگر متصل می‌شوند و شاسی تزریق ولتاژ برای مدت ۱۰ ثانیه نگه داشته می‌شود.

در این حالت دستگاه باید مقاومت صفر را نشان دهد. در صورتی که هر دو آزمون با موفقیت انجام شود، دستگاه سالم و آماده بکار است. کابل‌ها نیز باید چک شوند و دو سر کابل تمیز و خشک باشند. بهتر است تست عایقی در هوای مرطوب انجام نشود. با استفاده از جدول مخصوص مقادیر مجاز مقاومت عایقی، ولتاژ مناسب برای تست کابل را تعیین می‌شود. در آخر، دستگاه به کابل متصل و شاسی ولتاژ ثابت نگهداشته می‌شود. اگر مقدار نشان داده شده در صفحه نمایشگر دستگاه در حدود ارقام جدول باشد، کابل مورد تست از عایق مناسبی برخوردار است [۲].

مراحل انجام آزمون بر روی ژنراتور:

شکل ۳ نحوه اتصال دستگاه مگر به ژنراتور را نشان می‌دهد. برای اندازه‌گیری مقاومت عایقی، همانند توضیحات ارائه شده در بخش آزمون کابل ابتدا از درستی عملکرد دستگاه اطمینان حاصل کرده و بعد انتهای لاین دستگاه میگر به یکی از هادی‌ها و انتهای ارت دستگاه به زمین وصــل می‌شود. در آخر، دستگاه به سر سیم‌پیچ متصل و شاسی ولتاژ ثابت نگهداشته می‌شود. بدین شـکل، مقاومت عایقی ژنراتور و کابل‌های خروجی تا کلید قطع کننـده انـدازه‌گیری می‌شود.



شکل۳- نحوه اتصال دستگاه میگر به یک ژنراتور

اگر مقدار نشان داده شده در صفحه نمایشگر دستگاه در حدود ارقام جدول ۱ باشد، سیم‌پیچ مورد تست از عایق مناسبی برخوردار است. با استفاده از جدول ۱ می‌توان مقادیر مجاز مقاومت عایقی و ولتاژ مناسب برای تست سیم‌پیچی‌های ژنراتور را تعیین کرد. این اعداد براساس دستورالعمل آزمون هر ژنراتور یا استاندارد می‌تواند متفاوت باشد.

جدول ۱- مقادیر مجاز مقاومت عایقی و ولتاژ مناسب برای تست سیم‌پیچی‌های ژنراتور

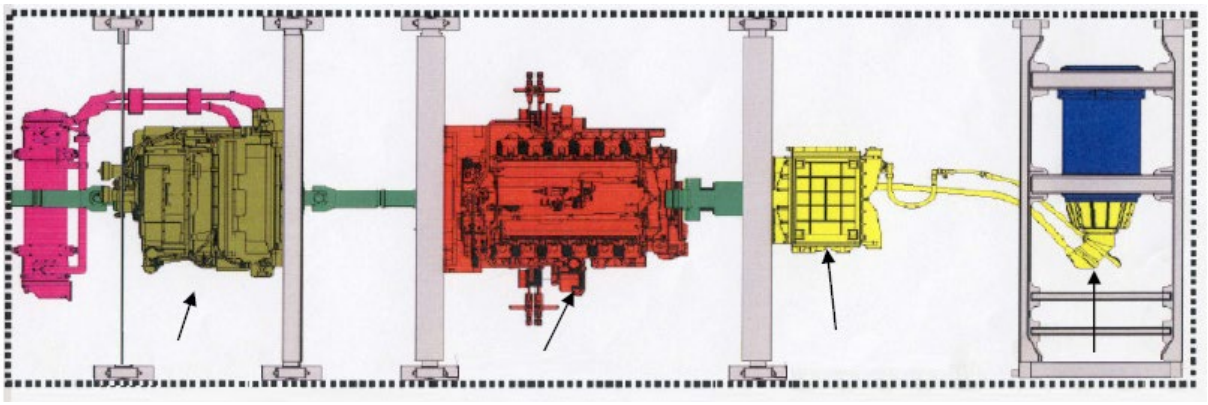
		1000 V	2500V
استاتور اصلی	U	5 MΩ	N.A.
	V	5 MΩ	N.A.
	W	5 MΩ	N.A.
روتور اصلی		5 MΩ	N.A.
روتور تحریک	U	5 MΩ	N.A.
	V	5 MΩ	N.A.
	W	5 MΩ	N.A.

آزمون میگر مقدار نسبی رطوبت در عایق، جریان نشتی بر روی سطوح، کثیف و یا مرطوب بودن، عیب سیم‌پیچی‌های رتور و استاتور را می‌تواند آشکار کند.

منبع تولید برق در قطارهای پر سرعت بین شهری ترنست

جهت تولید برق متناوب سه فاز از یک ژنراتور سنکرون با توان الکتریکی 75 kVA ساخت شرکت هیتزینگر که به صورت کوپل غیر مستقیم با موتور دیزل متصل است، استفاده شده است.
ژنراتور در نقشه‌های الکتریکال با کد (G11-34) مشخص می‌شود.

با چرخش روتور این ژنراتور سنکرون می‌توان از خروجی آن برق سه فاز متناوب 400 V با فرکانس 50 Hz و یک خط نول و یک خط ارتینگ دریافت نمود. شکل ۴ نحوه اتصال ژنراتور سنکرون را نشان می‌دهد.



شکل ۴- نحوه‌ی اتصال ژنراتور سنکرون

این ژنراتور ساخته شده توسط شرکت هیتزینگر با کد مشخصه 04R 4D SGS می‌باشد. در این ژنراتورها، یک جریان DC با کمک واحد تنظیم ولتاژ به سیم پیچی رتور اعمال می‌شود که میدان مغناطیسی روتور را ایجاد می‌کند. آنگاه روتور ژنراتور توسط پمپ هیدرولیک چرخانیده می‌شود و در نتیجه، میدان مغناطیسی دواری در داخل ماشین به وجود می‌آید. این میدان مغناطیسی دوار، ولتاژهای سه فاز در سیم پیچی استاتور ژنراتور القا می‌کند. کلمه سنکرون به این واقعیت دلالت دارد که فرکانس الکتریکی ماشین با سرعت چرخش مکانیکی محور (روتور)، قفل یا سنکرون می‌باشد [۳]. ژنراتورهای سنکرون قطارهای ترنست به صورت ماشین‌های بدون جاروبک میدان گردان طراحی شده‌اند و هسته‌های استاتور و روتور نیز از ورقه‌های فولاد مغناطیسی ورقه ورقه ساخته شده است. روتور بر روی محور اصلی قرار داشته و مجهز به سیم‌پیچی متعادل کننده برای بارهای نا متعادل و عملکرد موازی است. کلاف‌های سیم‌پیچی روتور به وسیله نوارهای عایق در مقابل نیروهای گرانشی محافظت شده است. عایق سیم‌پیچ‌ها از مواد رطوبت گیر ساخته شده تا در مقابل تغییرات حرارتی بالا مقاومت کنند[۴].

بر اساس دستورالعمل سازنده در هنگام نصب، مقاومت عایق‌ها باید چک شود. هنگام چک کردن دو سیم پیچ نسبت به هم یا یک سیم پیچ نسبت به زمین، باید مقاومت بیش از ۵ مگا اهم باشد. اگر مقاومت کمتر از این مقدار باشد باید سیم پیچی را کاملاً خشک کرد.

تحلیل برنامه‌های تعمیراتی ژنراتور و پیشنهادات

در بخش‌های قبل به بررسی آزمون میگر و بررسی ژنراتور برق قطارهای پرسرعت ترنست پرداخته شد. حال با استفاده از آن مطالب به تحلیل برنامه‌های تعمیراتی ژنراتور سنکرون هیتزینگر نصب شده بر روی قطارهای پرسرعت ترنست پرداخته و پیشنهادهایی ارائه می‌شوند.

براساس اطلاعات شرکت سازنده قطارهای پر سرعت ترنست با کد مشخصه DH4، سطوح تعمیراتی در 7 سطح شامل: T1, T2, T3, T4, T5, T6, T7 می‌باشد. هر یک از این سطوح بیانگر انجام فعالیت‌های مشخص برای تیم‌های تعمیراتی مختلف شامل مکانیک، برق، ترمز و تزئینات می‌باشد. زمان سر رسید هر یک از این سطوح به صورت ذیل است:

T1 : روزانه یا ۱,۹۰۰km یا ۲۲ نفر ساعت
T2 : هفتگی یا ۱۲,۵۰۰km یا ۱۵۴ نفر ساعت
T3 : ماهانه یا ۵۰,۰۰۰km یا ۶۱۶ نفر ساعت
T4 : هر دو ماه یکبار یا ۱۰۰,۰۰۰km یا ۱,۲۳۲ نفر ساعت
T5 : هر چهار ماه یکبار یا ۲۰۰,۰۰۰km یا ۲,۴۶۴ نفر ساعت
T6 : هر ساله یا ۶۰۰,۰۰۰km یا ۷,۳۲۹ نفر ساعت
T7 : هر دو سال یا ۱,۲۰۰,۰۰۰km یا ۱۴,۷۸۴ نفر ساعت

این روش تعمیراتی در بخش اول مدت زمان کلی سپری شده، بخش دوم کیلومتراژ کارکرد قطارکه به وسیله سیستم ثبت کیلومتر بر روی هر کلگی قطار استخراج میگردد و بخش سوم نفر ساعت انجام کار تیم تعمیراتی است طراحی شده است.

درخصوص روش برنامه‌ریزی T1 تا T7 این نکته مشهود است که درخصوص تجهیزات برقی بهتر است بجای استفاده از کیلومتراژ هر تجهیز از ساعت عملکرد هر تجهیز استفاده شود تا مجموع مدت زمان سیر قطار و مدت زمانی که تجهیز در خط پارک یا چال سرویس قرار دارد نیز لحاظ گردد. در این صورت تعمیرات جهت‌دار و بهینه‌تر خواهد شد.

جدول۲ فعالیت‌های تعمیراتی بر روی قطارهای ترنست ارائه شده توسط شرکت زیمنس آلمان را ارائه کرده است.
همانطور که در جدول۲ مشخص است، برای تعمیرات ژنراتور آزمون عایقی لحاظ نگردیده و تنها در دستورالعمل آن قید شده است که در زمان انجام مراحل نصب آزمون عایقی تحت استاندارد مشخص انجام شود و برای بخش باتری تنها در T7 یا هر دوسال یکبار آزمون عایقی الزام شده است.
با توجه به توضیحات ارائه شده در بخش‌های قبل، درخصوص اهمیت لزوم انجام آزمون مقاومت عایقی پیشنهاد می‌شود؛ این آزمون در برنامه تعمیراتی T4 یا هر دو ماه یکبار گنجانده و تیم تعمیراتی ملزم به انجام آن شود.

جدول۲- فعالیت‌های تعمیراتی بر روی قطارهای ترنست

Row	Component	Task	T1	T2	T3	T4	T5	T6	T7	UMI
			daily	7 days	1 month	2 months	4 months	1 year	2 years	unscheduled
			1.900 km	12.500 km	50.000 km	100.000 km	200.000 km	600.000 km	1.200.000 km	unscheduled
			22 OH	154 OH	616 OH	1.232 OH	2.464 OH	7.392 OH	14.784 OH	
	66 Electrical Motors / Generators									
8	Generator	Check Terminal Screws for tight Seat					x			
9	Generator	Check Connecting Plug for tight Seat					x			
10	Generator	Check Air Exhaust Metal Sheet for Damage and Dirt					x			
12	Generator	Visual Check of Bearing Covers for protruding Grease					x			
14	Generator	Check mountiing Screws for secure Seat						x		
16	Generator	Replacement of Roller Bearing								every 30.000 OH
17	Generator	Replacement of Generator								if necessary
18	Generator	Replacement of Support of Distribution Box								every 4.800.000 km
	72 Batteries									
6	Battery	Measure and record individual voltages (capacity check) and acid density of the Cells.						x		
7	Battery	Cleaning the Batteries in dismounted state.						x		
8	Battery	Insulation Resistance Test						x		
9	Battery Container	Visual inspection						x		

نتیجه‌گیری

در این مقاله با بررسی روش‌های آزمون عایقی و استراتژی‌های تعمیراتی، روش‌های اصلاحی برای چک لیست تعمیراتی ارائه شد. با توجه به حساسیت بالای تعمیرات و نگهداری قطارهای مسافری می‌توان با انجام آزمون‌هایی همچون آزمون مقاومت عایقی سیر ایمن برای مسافران و کاهش هزینه‌های تعمیرات اساسی برای مالک را فراهم کرد.

مراجع

References

1- https://www.instrumart.com/assets/Megger-insulationtester.pdf ; 18.OCT.2017

2- http://www.gozuk.com/FORUM/HIPOT-V-S-MEGGER-TEST-481057.HTML ; 02.NOV.2017

۳- استیفن جی.چاپمن، ترجمه: ر.حق مرام، «اصول ماشین‌های الکتریکی»، انتشارات دانشگاه امام حسین، چاپ اول، اسفند ۱۳۷۶.

4- HITZINGER, 66.01 Generator, User Manual, RAILWAY SYNCHRONOUS ALTERNATOR SGS 4D 04R.

خطر، شناسایی خطر و تکنیک PHL

کیانوش منادی طبری
سمت: مدیر ایمنی

رسول صبوحی
سمت: رئیس گروه ایمنی سیر و حرکت

چکیده

در این مقاله ابتدا تعدادی از بنیادی‌ترین و مهم‌ترین مفاهیم یک نظام ایمنی را تعریف و در ادامه به بیان لزوم « فرآیند شناسایی خطر» می‌پردازیم. سپس به یکی از ساده‌ترین و در عین حال پرفایده‌ترین تکنیک‌های « شناسایی خطر»، به نام « فهرستِ اولیهٔ خطر» (reliminary Hazard List, PHL) را معرفی خواهیم کرد.

تعاریف

تعریف شماره۱: «خطر» (Hazard)
«خطر» عبارت است از شرایط اولیه، حالت، وضعیت و موقعیت اعم از بالقوه و بالفعل که قابلیت تبدیل شدن به آسیب جانی، آسیب به سیستم/ اموال و یا آسیب زیست محیطی را دارا باشد.

تعریف شماره ۲: «فرآیند شناسایی خطر»
(Hazard Identification Process)
عبارت است از فرآیند بازجویی و تفحص در تمام حوزه‌های تحت بررسی، به منظور کشف همهٔ خطرهایی که بطور ذاتی در آن حوزه‌ها وجود دارند. به بیان دیگر، «شناسایی خطر» یک فرآیند، برای ارزیابی هر موقعیت موردی یا هر رخداد ویژه‌ای، اعم از واقعی یا بالقوه، به منظور کشف «هر آنچه که توان بالقوهٔ آسیب رسانی(اعم از جانی/ مالی/زیست محیطی) را داشته باشد».

تعریف شماره ۳: « **ریسک**» (Risk)
اثر عدم قطعیت (بر اهداف)

تعریف شماره ۴: «**مدیریت ریسک**» (Risk Management)
فعالیت‌های هماهنگ برای هدایت و کنترل یک سازمان، از دیدگاه ریسک.

تعریف شماره ۵: «**چرخه‌ی عمر**» (Life Cyde, LC)
سیر تحولی که یک «سیستم»، «محصول»، «پروژه» یا هر «نهاد بشر ساخته» طی می‌کند، از زمانی که تنها یک « ایده یا تصور» است تا زمان «از کارافتادگی»

چرا «شناسایی خطر»؟

این یک پرسش اساسی است و در پاسخ به آن می‌گوییم، اصولاً هدف از توسعهٔ «دانش و ساختارهای ایمنی» آن است که *از بروز سوانح و حوادث ناگوار جلوگیری کرده و از پیامدهای جانی و مالی آنها، در امان باشیم.* از سوی دیگر، تجربه به ما ثابت کرده است که همیشه قبل از آن که حادثه و یا سانحه‌ای رخ دهد، چیزی بنام «خطر» (تعریف شمارهٔ۱) وجود داشته است، که در عمل، همین «خطر» است که، با کمک برخی عوامل دیگر، در نهایت به حادثه تبدیل می‌شود.

به بیان ساده‌تر: «خطر، مقدمهٔ همهٔ سوانح است».

پس می‌توان چنین نتیجه گرفت که منطقی‌ترین کار برای جلوگیری از بروز سوانح، عبارت است از اینکه:

پیش از هر اقدامی، نخست «خطر»ها را بیابیم، سپس آنها را کنترل کرده و مانع از تبدیل شدن آنها به حادثه/ سانحه شویم».

بخش نخست گزاره پیشین، که مشتمل بر «یافتن خطرها» است، در واقع بیان کننده‌ی «مأموریت فرآیند شناسایی خطر» بوده و نشان دهنده‌ی لزوم اجرای این فرآیند نیز هست.

لذا تا زمانی که خطرها را *نیابیم*، نمی‌توانیم آنها را کنترل و مانع از تبدیل شدن آنها به حادثه شویم.

در دانش امروز، بیش از یکصد تکنیک مختلف برای شناسایی خطرها توسعه یافته‌است که ما در این مقاله یکی از ساده‌ترین این تکنیک‌ها یعنی تکنیک «فهرست اولیه خطر» (Preliminary Hazard List, PHL) را معرفی خواهیم کرد.

تکنیک فهرست اولیهٔ خطر

(Preliminary Hazard List, PHL)

تکنیک «فهرست اولیهٔ خطر PHL»، تکنیکی است تحلیلی، برای شناسایی و فهرست کردن «خطر»ها و «رویدادهای نامطلوبی» که بطور بالقوه در یک سیستم وجود دارند.

این تکنیک بطور خاص برای مراحل اولیهٔ چرخهٔ عمر (Life Cycle, LC)، به خصوص در مراحل «طراحی مفهومی» یا «طراحی اولیه» توسعه یافته است.

لیکن می‌توان آن را در تمامی مراحل چرخهٔ عمر یک سیستم مورد استفاده قرار داد.

در واقع این تکنیک، نقطهٔ آغاز تمامی تحلیل‌های بعدی می‌باشد که در زمینهٔ خطر انجام خواهند شد.

تکنیک PHL وسیله‌ای است در دست مدیریت، تا به کمک آن بر روی حوزه‌های خطرناکی متمرکز شود که نیازمند تخصیص منابع بیشتری بوده و در نهایت بتوان خطر را حذف یا ریسک آن را تا حد قابل قبول کاهش داد (کنترل خطر).

همهٔ خطرهایی که در PHL مورد شناسایی قرارمی‌گیرند، توسط تکنیک‌های تحلیلیِ جزئی‌تری، در مراحل بعدی، از فرآیند «مدیریت ریسک» (تعریف شمارهٔ۴)، مورد تجزیه و تحلیل قرارخواهند گرفت.

مبانی نظری

روش PHL یک تکنیک تحلیلی ساده و مستقیم است که فهرستی از خطرهای شناخته‌شده و یا مشکوک را تدوین می‌کند.

این تحلیل می‌تواند در حد یک جلسه‌ی ساده «طوفان فکری(Brain Storming)» بوده و یا حتی می‌تواند شامل فرآیندهایی ساختار یافته‌تر شود. با این هدف که از شناسایی شدن تمام خطرها، اطمینان حاصل کنیم.

ساختار اجرای «تحلیل PHL»، می‌بایست شامل گروهی از مهندسین/تحلیلگران با تخصص‌های گوناگون باشد.

شکل شمارهٔ۱، فرایندِ پایه‌ایِ PHL را، به صورت جمع‌بندی شده نشان می‌دهد و همچنین ارتباطات مهم موجود در فرآیند را بطورخلاصه بیان می‌کند.

شکل ۱- فرآیند پایه‌ای PHL

این فرآیند با هدف شناسایی خطرها، متشکل است از *تلفیق «اطلاعات طراحی» با «اطلاعات خطرهای شناخته شده»*.
در این تکنیک، «عناصر خطرناک شناسایی شده» و «درس‌های فراگرفته شده از رویدادهای نامطلوب پیشین»، با «طراحی سیستم» مقایسه می‌شود تا بفهمیم که آیا ایده‌ی مورد استفاده در طراحی، باعث تسهیل در بروز هیچکدام از این عناصر خطرناک می‌شود یا خیر؟
برای اجرای تحلیل PHL، تحلیل‌گر می‌بایست دو دانش را در اختیار داشته باشد: *یکی دانش طراحی و دیگری دانش خطر*. منظور از «دانش طراحی» این است که تحلیل‌گر می‌بایست درک پایه‌ای از طراحی سیستم داشته، که شامل فهرستی از *اجزای بزرگ سیستم* خواهد بود.
«دانش خطر» نیز به معنی آن است که تحلیلگر، درک پایه‌ای از خطرها، مثلث خطر، منابع خطر، اجزا خطر و خطرهای موجود در سیستم‌های مشابه، را دارا باشد. دانش خطر در ابتدا از موارد زیر بدست می‌آیند:

۱. چک‌لیست‌های خطر
۲. گزارش‌های مربوط به رویدادهای نامطلوب پیشین یا سوانح
۳. سیستم‌های ردیابی خطر (در صورت وجود)
۴. درس‌هایی که از سیستم‌ها و تجهیزات کاملاً مشابه و یا اندکی مشابه، فراگرفته‌ایم
۵. تحلیل‌ها و ارزیابی‌های ایمنی
۶. جزوات راهنمای تجهیزات
۷. اطلاعات مربوط به خطرهای حوزهٔ سلامتی
۸. مستندات آزمون‌های انجام شده
۹. جلسات طوفان فکری با حضور کارشناسان/ مهندسان با تخصص‌های مختلف

شکل ۲- چرخهٔ عمر (نمایش «چرخهٔ V شکل»)

تحلیل‌گر به هنگام اجرای PHL، دانش و اطلاعات طراحی را، با چک لیست‌های خطر مقایسه می‌کند. این امر باعث می‌شود که وی، نزد خود به تجسمی از خطرهای محتمل دست یابد.
به عنوان مثال اگر تحلیل‌گر ببیند بنا به طراحیِ سیستم، از افشانهٔ (جت) سوخت استفاده خواهد شد، آنگاه افشانهٔ سوخت را با چک لیست خطر مقایسه کرده و درچک لیست خطر، به وضوح مشاهده خواهد کرد که افشانهٔ سوخت، یک عنصرخطرناک است و همچنین در خواهد یافت که برای بسیاری از منابعِ تولیدِ جرقه، که هرکدام خطرهای متفاوتی ایجاد می‌کنند، انفجار/ آتش‌سوزیِ افشانهٔ سوخت، یک «رویداد نامطلوب بالقوه» محسوب می‌گردد.
ذکر این موضوع ضروری است که کاربرد تکنیک PHL، فقط به مراحل اولیه طراحی منحصر نمی‌شود و می‌توان از آن در تمام مراحل «چرخهٔ عمر»، اعم از آنچه که در شکل نمایش داده شده، می‌توان بهره جست:
خروجی اولیهٔ PHL، فهرستی از خطرهاست. همچنین لازم و مفید است که برخی اطلاعات اضافه مانند «عوامل ریشه‌ای اصلی خطر» (مثلا بروز شکست -Failure- در سخت‌افزار، خطای نرم‌افزاری، خطای انسانی و مانند آنها) و هرگونه «عوامل بحرانی ایمنی» (مانند عملکردهای بحرانیِ ایمنی، سخت‌افزارهای بحرانی ایمنی و مانند آنها)، که برای تحلیل‌های بعدی مفید باشند، جمع‌آوری و ثبت گردند.

روش‌شناسی

جدول شمارهٔ ۱، مراحل پایه‌ای PHL را فهرست و تشریح کرده و همچنین ارتباطات مهمی که بین آنهاست را بطور خلاصه بیان می‌نماید. در طول این فرآیند از یک کاربرگ استفاده می‌شود. اگر فرآیند PHL را در مراحل اولیه چرخهٔ عمر مورد استفاده قرار بدهیم آنگاه این فرآیند، با به دست آوردن «اطلاعات طراحی» آغاز می‌شود که شامل «ایدهٔ طراحی»، «ایدهٔ بهره‌برداری»، «شناسایی اجزا بزرگی که برای استفاده در سیستم درنظرگرفته شده‌اند»، «کارکردهای عمدهٔ سیستم» و «عملکردهای نرم‌افزاری» است. منابع این اطلاعات می‌توانند مواردی مانند: «شرح وظایف»، «مشخصات طراحی»،

«طرح‌ها»، «نقشه‌ها» یا «شماتیک‌ها» باشند.
همچنین برای آنکه بتوان سیستم را بهتر درک، تحلیل و مدل‌سازی کرد، می‌توان از داده‌های اضافی در خصوص «یکپارچگی طراحی» بهره گرفت.
«داده‌های یکپارچگی طراحی» (Design Integration Data) معمولاً شامل «بلاک دیاگرام‌های عملکردی» (Functional Block Diagrams)، «فهرست کاربردی تجهیزات» («ساختار ریزشکست کار WBS»، «بلاک دیاگرام‌های قابلیت اطمینان» و «ایدهٔ بهره‌برداری») است. اگر «داده‌های یکپارچگی طراحی» موجود نباشند، در اینصورت به منظور اجرای تحلیل PHL، ممکن است تحلیل‌گر مجبور شود از فرض‌هایی برای پیشبرد کار بهره بگیرد که البته همهٔ این فرض‌ها باید مستند و ثبت شوند.
گام بعدی در PHL عبارت است از تهیه چک‌لیست‌های خطر. چک‌لیست‌خطر، عبارت است از فهرست عمومی بخش‌هایی که با عنوان «خطرناک» شناخته شده‌اند و یا به صورت بالقوه می‌توانند طراحی و یا موقعیت خطرناکی را ایجاد کنند. لذا چک لیست خطر را نباید کامل و شامل همه چیز انگاشت.
چک لیست‌های خطر کمک می‌کنند تا تحلیل‌گر، منابع خطرناک بالقوه را، از دل درس‌های آموخته شدهٔ قبلی، شناسایی کند. چک‌لیست‌ها به طور معمول شامل موارد زیر هستند:

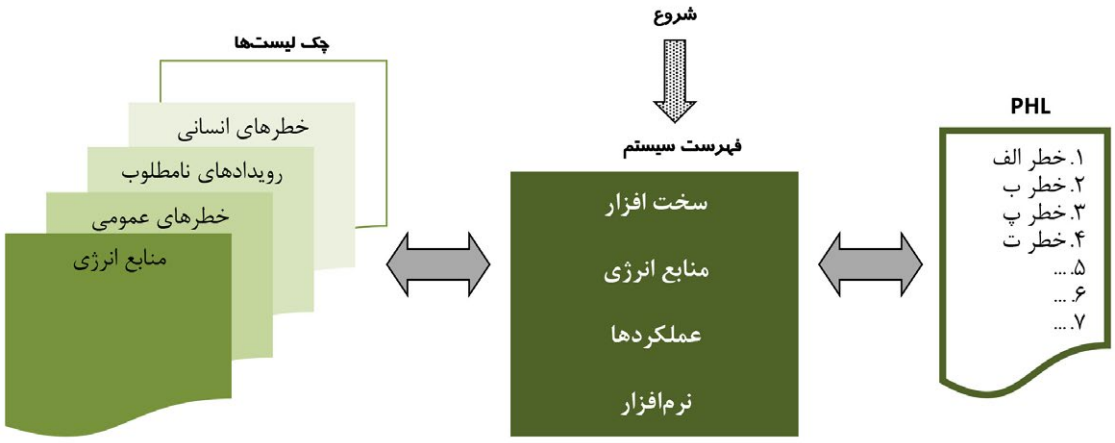
۱. منابع انرژی
۲. عملکردهای خطرناک
۳. بهره‌برداری‌های خطرناک
۴. اجزای خطرناک
۵. مواد خطرناک
۶. درس‌های فراگرفته شده از سیستم‌های مشابه
۷. رویدادهای نامطلوب
۸. حالات (بروز) شکست (Failure) و ملاحظات مربوط به وضعیت شکست هنگامی که همهٔ داده‌ها در اختیار بودند، تحلیل‌گر می‌تواند کارش را آغاز کند. تحلیل PHL، شامل در کنار هم قراردادن و قضاوت کردن بین «اطلاعات طراحی» و «یکپارچگی»، با «چک لیست خطر» است. اگر در طراحی سیستم از یک «جزو خطرناک شناخته شده»، «عملکرد خطرناک شناخته شده»، «بهره‌برداری خطرناک شناخته شده» و مانند آن، استفاده شده باشد، پس خطر بالقوه‌ای نیز وجود خواهد داشت. این خطر بالقوه در فرم تحلیل، ثبت شده و سپس به کمک اطلاعات طراحی که موجود است، مورد ارزیابی بیشتر قرارمی‌گیرد. چک لیست‌ها همچنین به فرآیند «طوفان فکری» کمک می‌کنند تا خطرهای احتمالی که در اثر «طراحی‌های خاص و منحصر به فرد» وارد سیستم می شوند، مورد شناسایی قرار بگیرند.

جدول ۱ - مراحل پایه‌ای برای PHL

مراحل	وظیفه	توضیـــح
	سیستم را تعریف کنید	دامنهٔ کاربرد و محدوده سیستم را تعریف کنید. ماموریت، مراحل ماموریت، و محیط ماموریت را تعریف کنید. بهره‌برداری و طراحی سیستم، مبانی بهره‌برداری، اجزا بزرگ سیستم را به درستی درک کنید.
	طرح‌ریزی برای PHL	اهداف، تعاریف، کاربرگ‌ها، برنامه کاری و فرآیند PHL را ایجاد کنید. عناصر و عملکردهایی که باید مورد تحلیل قرارگیرند را شناسایی کنید.
	تیم‌تان را انتخاب کنید	تمامی اعضای گروهی که می‌بایست در PHL شرکت کنند را انتخاب کنید و مسؤولیت‌ها را مشخص نمایید. از تخصص‌های مختلف در تیم استفاده کنید (مثلاً طراحی، آزمون، ساخت و ...)
	داده‌ها را بدست آورید	تمام داده‌های طراحی، بهره‌برداری و فرآیند در سیستم، زیرسیستم‌ها، و عملکردهایی که برای تحلیل مورد نیازند (به عنوان مثال فهرست تجهیزات، نمودارهای عملکردی، مبانی عملکردی و مانند آنها) را بدست‌آورید. چک لیست‌های خطر، درس‌های فراگرفته شده (از رویدادهای گذشته) و سایر داده‌های مربوط به خطر که مرتبط با سیستم باشند، را تهیه نمایید.
	PHL را اجرا کنید	الف) فهرست اجزای سخت‌افزاری و عملکردهای سیستم را تدوین کنید. ب) سخت‌افزارهای مربوط به سیستم مفهومی را مورد ارزیابی قرارداده، آن را با چک لیست خطر مقایسه کنید. پ) عملکردهای بهره‌برداری سیستم را مورد ارزیابی قرارداده، آنها را با چک لیست خطر مقایسه‌کنید. ت) منابع انرژی مورد استفاده در سیستم را مورد شناسایی و ارزیابی قرارداده، آنها را با چک لیست خطرهای مربوط به انرژی مقایسه کنید. ث) عملکردهای نرم‌افزاری سیستم را مورد ارزیابی قرارداده، آنها را با چک لیست خطر مقایسه‌کنید. ج) وضعیت‌های ممکن (بروز) شکست (Failure) را مورد ارزیابی قرار دهید.
	فهرست خطر را بنا نهید	فهرست «خطرهای شناسایی شده» و «خطرهای مشکوک» در سیستم و رویدادهای نامطلوب بالقوه سیستم را تهیه نمایید. « عملکردهای بحرانی از دیدگاه ایمنی» و نیز «رویدادهای نامطلوب سطح بالا» را در صورت امکان، از اطلاعات موجود، مورد شناسایی قراردهید.
	اقدامات اصلاحی پیشنهاد دهید	«خطوط راهنمای ایمنی» و «روش‌های ایمنی در طراحی» که باعث حذف و یا کاهش اثرات خطرها می‌گردد را پیشنهاد دهید.
	PHL را مستند کنید	کل فرایند PHL و کاربرگ‌های PHL را در یک «گزارش PHL»، مستند کنید. نتیجه‌گیری‌ها و پیشنهادها، را منظم کنید.

خروجی‌های فرایند PHL عبارتند از: «خطرهای شناسایی شده»، «حوزه‌های مربوط به ریشهٔ خطرها (در صورت امکان)»، «اثرات ناشی از رویدادهای نامطلوب» و «عوامل بحرانی ایمنی» (در صورت وجود).

روش‌شناسی کلی PHL را در شکل شمارهٔ ۳ ملاحظه می‌فرمایید. در این روش، فهرستی از سیستم ایجاد می‌شود که (این فهرست) عناصر(ویژه) و برنامه‌ریزی شده‌ای را در خود دارد که در بخش‌های سخت‌افزاری، منابع انرژی، عملکردها و نرم‌افزاری قراردارند. سپس بخشی که در فهرست سیستم وجود دارد، با بخش‌های موجود در چک‌لیست‌های گوناگون ایمنی، مقایسه می‌شود. مواردی که در هر دو فهرست با هم منطبق باشند، کاندیدهایی برای خطرهای بالقوه هستند، که در ادامه و در فهرست اولیهٔ خطر PHL، با هم ترکیب خواهند شد.



شکل ۳- روش شناسی PHL

کاربرگ

همانطور که گفتیم، برای اجرای PHL از یک کاربرگ استفاده می‌شود. کاربرگ باعث می‌شود که تحلیل، با دقت بیشتری انجام شده و فرآیند مستند گردد. قالب و هیأت کاربرگ مورد استفاده در تحلیل، از اهمیت ویژه‌ای برخوردار نیست و معمولاً به شکل یک کاربرگ ستون‌بندی شده، می‌باشد. اطلاعات پایه‌ای زیر را باید بتوان از کاربرگ PHL بدست‌آورد:

۱. خطرهای واقعی و مشکوک

۲. رویدادهای نامطلوبِ سطح بالا

۳. پیشنهادها (مانند الزامات / خطوط راهنمای ایمنی که می‌توانند مورد استفاده قرارگیرند)

نمونه‌هایی از کاربرگ PHL در جدول شمارهٔ ۲ آمده است.

جدول ۲ - دو نمونه از کاربرگ PHL

تحلیل PHL				
نوع عنصر سیستم:				
شماره	بخش سیستم	شرح خطر	اثرات خطر	توضیحات

فهرست مقدماتی خطر (PHL)							
ردیف	نوع خطر	دسته خطر	واحد مسئول کنترل خطر	تاریخ ثبت خطر	کد خطر	شرح خطر	پیامدهای خطر

ستون‌های کاربرگ PHL را به صورت زیر تعریف می‌کنیم:

نـوع عنصر سیستم
نـوع خطر / دسته خطر

در این ستون، بیان می‌کنیم که بخشی از سیستم که مورد تحلیل قرارگرفته است از چه نوعی است مانند سخت‌افزار سیستم، عملکرد سیستم، نرم‌افزار سیستم، منابع انرژی و مانند آن.
به عنوان مثال در یک سازمان، ابتدا «نوع عنصر سیستم»، به دسته‌های «سخت‌افزاری»، «نرم‌افزاری»، «منابع انرژی»، و «عملکردها» تقسیم شده است، سپس خطرها از طریق آزمون‌های دقیق به هر کدام از دسته‌های فهرست شده، نسبت داده می‌شوند. به عنوان مثال اگر «مواد منفجره»، را یک سخت‌افزاری در نظر بگیریم، می‌توان آن را تحت عنوانِ «سخت‌افزار» و همچنین مجدد تحت عنوان «منابع انرژی» فهرست کنیم.
این کار ممکن است منجر به مستندسازی یک خطر، در دو جای مختلف خواهد بود، اما باعث می‌شود خطرهای مرتبط با مواد منفجره شناسایی شوند.

شمارهٔ خطر/کدخطر

در این ستون به منظور مراجعات بعدی، شماره‌ای (و یا یک کد) برای خطر تعیین می‌کنیم.

بـخش سیستم

این ستون، در واقع زیرمجموعهٔ «نوع عنصر سیستم» است که در آن بخش‌های اصلی سیستم را بررسی و در دسته‌هایی معین قرارمی‌دهیم.

شـرح خطـر

در این ستون، یک خطر خاص و منحصر به فرد مورد شناسایی قرارمی‌گیرد. باید به یاد داشته باشیم که این خطر، در واقع به عنوان یکی از خروجی‌های آن بخش از سیستم که در حال بررسی آن هستیم، به شمار می‌آید. (به یاد داشته باشید همه خطرهای بالقوه را، مستند کنید حتی اگر در آینده و در تحلیل دیگری ثابت گردد که درکاربردی که در حال بررسی آن هستیم، خطرناک نیست)

اثـرات خطر
پـیامدهای خطر

در این ستون، پیامد ناشی از خطر شناسایی شده را مشخص می‌کنیم. این پیامد، می‌بایست در قالب عناوینی که مرتبط با بهره‌برداری سیستم هستند بیان شوند مانند «عدم بهره‌برداری از سیستم»، «مرگ»، «جراحت»، «تخریب» و مانند آنها. عموماً اثر یک خطر ، یک «رویدادِ نامطلوب» است.

تـوضیحات

در این ستون هرگونه اطلاعات مهم، حدس و گمان، پیشنهادها و مانند آن که می‌توانند از تجزیه و تحلیل بدست آمده باشند، بیان شود. به عنوان مثال «عملکردهای بحرانی ایمنی»، «رویدادهای نامطلوب سطح بالا» و یا «خطوط راهنمای طراحی» نیز ممکن است در اینجا مورد اشاره قرارگیرند.

چک لیست خطر

چک‌لیست‌ها یک مرجع عمومی هستند، برای آنکه خطرها به‌آسانی مورد شناسایی قرارگیرند. از آنجایی که در واقع یک چک‌لیست منفرد، هرگز کافی نخواهد بود، لذا ضروریست تا چک‌لیست‌های متفاوتی تدوین و بکارگرفته شوند. بکارگیری چک‌لیست‌های متعدد، شاید منجر به دوباره‌کاری گردند اما عناصر خطرناک را بهتر پوشش می‌دهند. بخاطر داشته باشید که هرگز یک چک‌لیست کامل و نهایی وجود ندارد بلکه چک‌لیست، صرفاً یک سازوکار یا یک تسریع‌کننده برای تشخیص خطرها می‌باشد.

نکات راهنما

نکاتی که در زیر بیان می‌شوند در واقع خطوط راهنمایی هستند که در هنگام تکمیل کاربرگ PHL، می‌بایست مد نظر قرارگیرند:
۱. به یاد داشته باشید که هدف از PHL، صرفاً «شناسایی خطرها/ رویدادهای نامطلوب سیستم» است و نه ارائه راهکار برای «کنترل خطر».
۲. بهترین رویکرد آن است که با بررسی بخش‌های «سخت‌افزاری سیستم»، «عملکردهای سیستم» و «منابع انرژی سیستم»، آغاز کنید.
۳. از چک‌لیست‌های خطر و درس‌های فراگرفته شده (از رویدادهای گذشته) برای شناسایی خطرها استفاده کنید.
۴. نحوهٔ نگارش یک خطر، باید قابل درک باشد، اما لازم نیست که خطر، به صورت جزئی تشریح گردد (یعنی خطر ذکر شده در PHL، لزوما نباید هر سه عنصر مثلث خطر یعنی: «عنصر خطرناک»، «ساز و کار فعال کننده حادثه» و «گروه هدف/تهدید» را در برگیرد)

مزیت‌ها و اشکالات

اشکال قابل ملاحظه‌ای بر این تکنیک وارد نیست، اما مزیت‌های PHL عبارتند از:
۱. تحلیل PHL به راحتی و به سرعت انجام می‌شود.
۲. به منظور استفاده از تکنیک PHL، نیاز به تخصص قابل ملاحظه نیست.
۳. برای دستیابی به نتایج معنی‌دار، نیازی به صرف هزینه زیاد نمی‌باشد.
۴. فرآیند PHL به شدت بر روی «خطر» متمرکز است.
۵. تحلیل PHL بر مکان‌هایی که ریسک خطرهای اصلی و رویدادهای نامطلوب سیستم در آنهاست، اشاره دارد.

اشتباهات رایج

در زیر فهرستی از اشتباهات رایج که در هنگام هدایت فرآیند PHL ممکن است بروز کند ارائه می‌شود:

۱. فهرست نکردن تمامی خطرهای مرتبط یا قابل ملاحظه بسیار مهم است که تمامی خطرهای محتمل و یا مشکوک را فهرست کرده که هیچ‌کدام از نگرانی‌های بالقوه را، از حیطه تحلیل خارج نکنیم.

۲. عدم توفیق در مستندسازی خطرهایی که شناسایی شده‌اند، اما آنها را چندان مهم در نظر نگرفته‌ایم. PHL سند تاریخی است که تمامی حوزه‌های شناسایی خطر را که مورد توجه قرارگرفته‌اند را در برمی‌گیرد.

۳. بکار نگرفتن یک رویکرد ساختاریافته. همیشه از یک کاربرگ استفاده کنید و تمامی تجهیزات، منابع انرژی، عملکردها و مانند آن را لحاظ کنید.

۴. عدم جمع‌آوری و بهره‌برداری از چک‌لیست‌های منابع خطر

۵. عدم جستجو برای یافتنِ سیستم‌ها و تجهیزات مشابه، تا بتوان از درس‌های قابل استفادهٔ آنها بهره برد.

۶. عدم ایجاد یک فهرست صحیح از سخت‌افزار، علمکردها، و مراحل مأموریت.

۷. فرض بر این گذاشته شود که خواننده، توصیف‌های خطر را، از عباراتی کوتاه، که انباشته است از اصطلاحات منحصربفرد و مخففها (Abbreviations) و سرنام‌ها (Acronyms)، می‌تواند درک کند. به بیان دیگر توصیف خطر نباید بیش از اندازه مختصر و همچنین انباشته از عبارات و واژگان نامفهوم باشد.

خلاصه

مطالب ذکر شده را می‌توان در موضوعات زیر خلاصه کرد:

۱. هدف اولیهٔ تحلیل PHL عبارتست از شناسایی خطرها و رویدادهای نامطلوب که در «طرح مفهومی» یک سیستم وجود دارند اما این روش را برای شناسایی خطر در سایر موارد و سایر مراحل چرخهٔ عمرِ سیستم هم، می‌توان به کار برد.

۲. فرآیند PHL، اطلاعات مربوط به خطرها را مهیا کرده و به عنوان نقطهٔ آغازی برای فرایند تحلیلی‌تر و عمیق‌تری بنام «تحلیل اولیه خطر» یا PHA-Preliminary Hazard Analysis) است.

۳. تحلیل PHL به عنوان یک یاری‌گر در فرآیند تصمیم‌سازی در حوزه‌های ایمنی و طراحی و در مراحل اولیهٔ توسعه بوده و اطلاعاتی را مهیا می‌کند که بر اساس آنها می‌توان دریافت که منابع طراحی در مرحلهٔ توسعه را، در کجا می‌توان صرف کرد.

۴. استفاده از یک نمودار جریان کار عملیاتی و یک فهرست از تجهیزات قراردادی، به طور قابل ملاحظه‌ای به فرآیند PHL کمک کرده و آن را ساده می‌کند.

۵. در هنگام اجرای PHL، «چک لیست‌های خطر» مورد استفاده قرار می‌گیرند. گرچه که یک چک لیست خطر را نباید یک فهرست کامل و نهایی به شمار آورد بلکه فقط کاتالوگی برای تحریک ایده‌سازی در موضوع خطر است.

۶. در هنگام حدس زدن خطرها هیچگونه فکر، ایده و یا حتی نگرانی را نادیده نگیرید.

همچنین مهم است که علاوه بر شناسایی خطرهای واقعی، نشان دهید که به برخی از خطرها مشکوک بوده و یا آنها را در نظر گرفته‌اید، حتی اگر بعدها مشخص شود که آن خطرها بنا به دلایل طراحی، غیرممکن بوده‌اند. این کار به عنوان شاهدی خواهد بود بر این امر که در این پروژه، «همهٔ خطرها را مد نظر قرارداده‌ایم».

۷. یک توصیف کامل و معتبر و با معنا از خطر بنگارید که برای دیگران قابل درک باشد و نه فقط برای تحلیلگر. چنین فرض نکنید که خوانندهٔ توصیفِ خطر، می‌تواند خطر را از طریق یک جمله مختصر و مخفف درک کند، که انباشته از اصطلاحات خاص آن پروژه است.

۸. در هر مورد که مقدور بود، عناصر سه‌گانه‌ی تشکیل دهند، هر خطر (مثلث خطر) را شناسایی کنید که عبارتند از:

- عنصر خطرناک (منبع)
- سازوکار فعال کنندهٔ حادثه (سازوکار)
- گروه هدف/تهدید (خروجی)

۹. معمولا هرگاه یک خطر مورد شناسایی واقع شده و توصیف می‌شود، متن نگاشته شده برای توصیف خطر، هر سه عنصر تشکیل دهندهٔ خطر (مثلث خطر) را شامل شده و مورد شناسایی قرار می‌دهد. گرچه در PHL، یک توصیف کامل از خطر ارائه نمی‌شود که این امر به خاطر ماهیت مقدماتی تحلیل بوده و همچنین به این خاطر که خطرها در مرحلهٔ بعد توسط تکنیکِ PHA مورد بررسی و توصیف کامل قرار خواهند گرفت.

منابع:

1. Ericson II, C.A., Hazard Analysis Techniques for System Safety, Wiley-Interscience, 2005.

۲. کیانوش منادی طبری، علیرضا نوری، نظام شناسایی خطرها رویکردی کارآمد برای یافتن و کنترل خطرها، همایش بین‌المللی حمل و نقل ریلی،۱۳۸۶.

۳. کیانوش منادی طبری، جزوه آموزشی ایمنی و شناسایی خطر، مرکز آموزش شرکت رجا.

4. Layton, D., System Safety: Including DOD Standards, Weber Systems, Inc., 1989.

5. Roland, H., E. and B. Moriarty, System Safety Engineering and Management, 2nd ed., Willey New York, 1990.

6. MIL-STD882-e, 11May 2012, SYSTEM SAFETY.

7. Vincoli, J.W., Basic Guide to System Safety, 3rd ed., John Wiley & Sons, 2014.

8. BS EN 1:2017-50126 Railway Applications - The Specification and Demonstration of Reliability, Availability,Maintainability and Safety (RAMS).

9. ISO 31000:2018 Risk management-Guidlines.

تهدیدات امنیت سایبری در حمل و نقل ریلی

سید علی مصطفوی
معاون اداره کل توسعه سرمایه‌های انسانی

بابک آذرباد
رئیس اداره روابط کار و جبران خدمات

محمد چگنی
کارشناس مسئول اداره روابط کار و جبران خدمات

بررسی عمیق حملات مهم و استراتژی های کاهش

چکیده

همانطور که سیستم های حمل و نقل ریلی به طور فزاینده دیجیتالی می‌شوند، با افزایش کارایی عملیاتی و خطرات امنیت سایبری بالا مواجه می‌شوند. این شمشیر دو لبه پیشرفت‌هایی را در ایمنی و ارائه‌ی خدمات به ارمغان می‌آورد و در عین حال زیرساخت‌های حیاتی را در معرض حملات سایبری مخرب قرار می دهد. پیامدهای این حملات سایبری می‌تواند شدید باشد، از اختلالات عملیاتی و خسارات مالی گرفته تا امنیت و اعتماد عمومی.

هدف این مقاله مروری بررسی برخی از مهم‌ترین حملات سایبری بر سیستم‌های حمل‌ونقل ریلی، تحلیل علل، اثرات و اقدامات متقابل اجرا شده برای جلوگیری از تکرار آن است. با درک این حوادث و چشم‌انداز در حال تحول تهدیدات امنیت سایبری، نیاز به پیشرفت‌های مستمر و قوی در اقدامات امنیت سایبری برای محافظت از سیستم‌های حمل و نقل ریلی در برابر حملات آینده تأکید می کنیم.

مقدمه

سیستم‌های حمل و نقل ریلی برای زیرساخت‌های اقتصادی و اجتماعی جامعه مدرن حیاتی هستند. با ظهور فناوری‌های دیجیتال، این سیستم‌ها شاهد پیشرفت‌های چشمگیری در عملیات، ایمنی و خدمات به مسافران بوده‌اند. حملات سایبری به سیستم‌های ریلی می‌تواند منجر به اختلالات خدماتی، زیان‌های مالی و خطرات احتمالی ایمنی شود. این مقاله به بررسی حملات سایبری عمده به سیستم‌های حمل و نقل ریلی، تأثیرات آنها و استراتژی‌های مورد استفاده برای مقابله با این تهدیدات می‌پردازد.

حملات سایبری قابل توجه به سیستم‌های ریلی

اهمیت هدف و فقدان نسبی رویکردهای موجود برای امنیت راه‌آهن، بسیاری از نویسندگان را وادار کرده است تا تحلیل‌هایی را برای انواع مختلف حملات و کاهش احتمالی آن‌ها در جامعه دانشگاهی پیشنهاد کنند. در این پژوهش فهرست مختصری از این وقایع به شرح ذیل ارائه می‌دهیم.

- در سال ۲۰۰۳ یک ویروس کامپیوتری، دفتر مرکزی حمل و نقل CSX در فلوریدا را از کار انداخت و بر سیگنال دهی هزاران کیلومتر خط راه آهن تأثیر گذاشت. از این حادثه به عنوان واقعه «سوبیگ» نیز یاد شده است[۱].
- در سال ۲۰۰۸ یک نوجوان لهستانی به سیستم تراموا نفوذ کرد و منجر به خروج از ریل و مصدومیت چندین نفر شد. این حادثه ضعف سیستم‌های ریلی حتی در برابر حملات با تکنولوژی پایین را نشان داد و نیاز به تدابیر امنیتی قوی‌تر را برجسته کرد[۲].
- در سال ۲۰۱۵، یک حمله سایبری به Deutsche Bahn، شرکت راه‌آهن ملی آلمان، رخ داد. این حمله شامل باج‌افزاری بود که خدمات مختلفی از جمله صدور بلیت و نمایش اطلاعات را مختل کرد.
این حادثه نشان داد که حملات سایبری می‌تواند باعث اختلالات عملیاتی قابل توجه و زیان‌های مالی شود[۳].
- در سال ۲۰۱۶، بدافزار BlackEnergy & KillDisk سیستم‌های یک شرکت راه‌آهن برجسته اوکراین را آلوده کردند. در دسامبر ۲۰۱۵ حمله سایبری شبکه برق اوکراین نیز با استفاده از همان بدافزارها مورد حمله قرار گرفت[۴].
- یک حمله قابل توجه دیگر در سال ۲۰۱۶ رخ داد زمانی که سازمان حمل و نقل شهری سانفرانسیسکو (SFMTA) مورد حمله باج‌افزاری قرار گرفت.
مهاجمان برای بازگشایی سیستم‌های سازمان تقاضای باج کردند، اما SFMTA از پرداخت خودداری کرد. اگر چه این حمله بر عملیات قطار تأثیری نداشت، اما موجب ناراحتی قابل توجه مسافران و هزینه‌های مالی برای سازمان شد[۵].
- در سال ۲۰۱۷، اداره حمل و نقل سوئد هدف یک حمله DDoS به سیستم های فناوری اطلاعات که بر ترافیک راه آهن نظارت می کنند، قرار گرفت. روز بعد دو حمله DDoS به اپراتور حمل و نقل عمومی V¨asttrafik ضربه زد[۶].
- در سال ۲۰۱۸، اپراتور دانمارکی DSB مورد حمله DDoS قرار گرفت و خرید بلیط را غیرممکن کرد. سیستم‌های پست داخلی و تلفن مورد استفاده کارکنان DSB نیز تحت تأثیر قرار گرفتند[۷].
- در سال ۲۰۲۰، یک حمله باج افزار سازمان (Soci,e de transport de Montreal (STM را مورد حمله و ۶۲۴ سرور حساس عملیاتی را در معرض خطر قرار داد. این قطع همچنین STM را برای بیش از یک هفته تحت تاثیر قرار داد. [۸,۹]
- در سال ۲۰۲۰، یک حمله باج افزار به OmniTRAX انجام شد. این اولین مورد فاش شده عمومی از یک حمله باج‌افزاری به اصطلاح دوطرفه علیه اپراتور راه‌آهن باری ایالات متحده بود[۱۰].

تأثیرات حملات سایبری به سیستم‌های ریلی

پیامدهای حملات سایبری به سیستم‌های حمل و نقل ریلی می‌تواند شدید باشد. اختلالات عملیاتی می‌تواند منجر به زیان‌های مالی قابل توجهی شود، همان‌طور که در حمله به Deutsche Bahn مشاهده شد، جایی که باج‌افزار سیستم‌های صدور بلیت و نمایش اطلاعات مشتریان را مختل کرد و باعث سردرگمی و زیان مالی گسترده شد [۳]. علاوه بر این، ایمنی یک نگرانی عمده است همان‌طور که در حادثه لهستان مشاهده شد، جایی که دستکاری سیگنال‌های راه‌آهن منجر به خروج از ریل و مصدومیت شد [۲]. حملات سایبری می‌تواند اعتماد عمومی به ایمنی و قابلیت اطمینان خدمات ریلی را کاهش دهد.

در مورد حمله SFMTA، اگرچه عملیات قطار به‌طور مستقیم تحت تأثیر قرار نگرفت، اما نفوذ به اطلاعات حساس و ناراحتی‌ای که برای مسافران ایجاد شد، تأثیرات ماندگاری بر اعتبار سازمان داشت[۱۱]. تأثیر روانی بر مسافران و کارکنان می‌تواند قابل توجه باشد، که منجر به افزایش استرس و کاهش اعتماد به امنیت سیستم ریلی می‌شود.

استراتژی‌های کاهش حملات سایبری

برای حفاظت از سیستم‌های حمل و نقل ریلی در برابر تهدیدات سایبری، چندین استراتژی به کار گرفته شده است. یکی از رویکردهای کلیدی، پذیرش فناوری‌ها و شیوه‌های پیشرفته امنیت سایبری است. به عنوان مثال، سیستم‌های تشخیص نفوذ (IDS) و سیستم‌های جلوگیری

از نفوذ (IPS) برای نظارت بر ترافیک شبکه و شناسایی تهدیدات احتمالی به کار گرفته می‌شوند[۱۲]. علاوه بر این، ارزیابی‌ها و بازرسی‌های امنیتی منظم کمک می‌کنند تا نقاط ضعف شناسایی شوند و اطمینان حاصل شود که استانداردهای امنیتی رعایت می‌شوند. برنامه‌های آموزشی و آگاهی‌رسانی کارکنان نیز در کاهش ریسک‌های سایبری بسیار مهم هستند.

خطای انسانی اغلب عامل مهمی در موفقیت حملات سایبری است. بنابراین آموزش کارکنان در مورد بهترین شیوه‌های امنیت سایبری ضروری است[۱۳]. علاوه بر این، همکاری بین ذینفعان صنعت، از جمله سازمان‌های دولتی، شرکت‌های خصوصی و کارشناسان امنیت سایبری، برای به اشتراک‌گذاری اطلاعات و توسعه استراتژی‌های جامع امنیتی حیاتی است.

نقش فناوری در جلوگیری از حملات سایبری

فناوری‌های پیشرفته نقش مهمی در جلوگیری از حملات سایبری به سیستم‌های حمل و نقل ریلی ایفا می‌کنند. پیاده‌سازی ابزارهای نظارت در زمان واقعی می‌تواند به شناسایی ناهنجاری‌ها کمک کند. افزایش ناگهانی در ترافیک شبکه ممکن است نشان‌دهنده حمله سایبری باشند. به عنوان مثال، الگوریتم‌های یادگیری ماشین می‌توانند الگوها را تحلیل کرده و انحرافاتی را که نشان‌دهنده تهدیدات احتمالی باشند را شناسایی کنند[۱۲]. علاوه بر این، فناوری بلاک‌چین یک رویکرد امیدوارکننده برای افزایش امنیت سیستم‌های ریلی ارائه می‌دهد و یک دفتر غیرمتمرکز و تغییرناپذیر برای ردیابی سوابق نگهداری و دیگر داده‌های حیاتی فراهم می‌کند [۱۴].

مطالعات موردی و درس‌های آموخته شده

بررسی مطالعات موردی حملات سایبری به سیستم‌های ریلی بینش‌های ارزشمندی در مورد ماهیت این تهدیدات و اثربخشی استراتژی‌های کاهش ارائه می‌دهد. حمله لهستان در سال ۲۰۰۸ نشان داد که حفاظت از اجزای به ظاهر کم‌ریسک سیستم ریلی، مانند سیگنال‌های کنترلی ، بسیار مهم است [۲].

حمله باج‌افزاری Deutsche Bahn نیاز به برنامه‌های پشتیبان‌گیری و بازیابی قوی برای کاهش اختلالات و زیان‌های مالی را برجسته کرد [۳]. در همین حال، حادثه SFMTA ارزش امتناع از پرداخت باج و تمرکز بر بازیابی و تقویت امنیت پس از حمله را نشان داد [۵].

نتیجه‌گیری

دیجیتالی شدن روزافزون سیستم‌های حمل و نقل ریلی آنها را در معرض حملات سایبری قرار داده است. این بررسی اهمیت تدابیر امنیت سایبری قوی برای حفاظت از این زیرساخت‌های حیاتی را برجسته می‌کند. با بررسی حملات سایبری قابل توجه به سیستم‌های ریلی، می‌توانیم بهتر ماهیت این تهدیدات و استراتژی‌های مورد نیاز برای کاهش آنها را درک کنیم. پیشرفت‌های مستمر در شیوه‌ها و فناوری‌های امنیت سایبری برای حفاظت از سیستم‌های حمل و نقل ریلی در برابر تهدیدات سایبری نوظهور ضروری است.

مراجع

References

1- W. G. Temple, Y. Li, B. A. N. Tran, Y. Liu, and B. Chen, “Railway system failure scenario analysis,” in International Conference on Critical Information Infrastructures Security, pp. 213–225, Springer, 2016.

2- Kune, D. F., Kim, J., & Perrig, A. (2013). The Poland Rail System Attack: Implications for Critical Infrastructure Security. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (pp. 111-120). https://doi.org/10.1145/2508859.2516693

3- Rowe, D., Lunt, B., & Ekstrom, J. (2017). Cybersecurity Breaches in Rail Transportation: A Case Study of the Deutsche Bahn Attack. Journal of Transportation Security, 10(2-3), 95-105. https://doi.org/10.1007/s12198-017-0186-7

4- K. Wilhoit, “KillDisk and BlackEnergy go beyond energy sector,” Trend Micro, Feb. 11 2016. https: //www.trendmicro.com/en us/research/16/b/killdiskand- blackenergy-are-not-just-energy-sector-threats.html.

5- A. Thomas, “Germany’s Deutsche Bahn rail operator targeted in global cyberattack,” The Wall Street Journal, May 13 2007. https://www.wsj.com/articles/germanys-deutsche-bahn-railoperator- targeted-in-global-cyberattack-1494658493.

6- The Local, “Swedish transport agencies targeted in cyber attack,” The Local, Oct. ,12 2017. https: //www.thelocal.se/20171012/swedish-transport-agenciestargeted- in-cyber-attack.

7- Ritzau/The Local, “Cyber attack hits Danish rail network,”The Local, May 14 2018. https://www.thelocal.dk/20180514/cyber-attack-hits-danish-rail-network/amp.

8- CBC, “STM says it refused hackers’ $2.8M demand in ransomware attack,” Canadian Broadcasting Corporation News, Oct. 29 2020. https://www.cbc.ca/news/canada/ montreal/stm-refused-to-pay-2-8-million-ransomware-attack- 1.5782838.

9- L. Abrams, “Montreal’s STM public transport system hit by ransomware attack,” Bleeping Computer, Oct. 21 2020. https: //www.bleepingcomputer.com/news/security/montreals-stmpublic- transport-system-hit-by-ransomware-attack/.

10- N. Tabak, “Ransomware attack hits short line rail operator OmniTRAX,” FreightWaves, Jan. 9 2021. https://www.freightwaves.com/news/ransomware-attackhits- short-line-rail-operator-omnitrax.

11- Beek, C. (2016). Ransomware: The San Francisco Rail System Attack. Retrieved from https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-the-san-francisco-rail-system-attack/

12- Jia, X., Wang, P., & Zhou, H. (2018). Advanced Cybersecurity Technologies in Rail Transportation Systems. Journal of Transportation Safety & Security, 10(3), 301-315. https://doi.org/10.1080/19439962.2017.1411872

13- Cai, H., Ge, Y., & Gao, Q. (2020). Enhancing Cybersecurity in Rail Transportation: Employee Training and Awareness. International Journal of Rail Transportation, 8(1), 1-14. https://doi.org/10.1080/23248378.2019.1682592

14- Li, H., Peng, Y., & Zhang, J. (2019). Blockchain Technology for Enhancing Rail Transportation Security. Transportation Research Part C: Emerging Technologies, 103, 71-85. https://doi.org/10.1016/j.trc.2019.03.011