



Investigating cyberspace security and safety engineering in rail transport network systems and subsystems (case study: Italian regional railways)

Mehran Khalaj¹ | Daud Jafari² | Pejman Salehi³

Abstract

Studying the history of cyber attacks on computer networks and rail transportation systems shows the vulnerability of these systems and related subsystems against the possible threats of intruders and attackers. In recent years, various implementation methods and guidelines have been designed and documented to improve the security level of railway systems against the risks in cyberspace. The large number and wide variety in the scope of these documents shows the importance and necessity of safety and security against the current increasing and complex attacks in the cyber fields. In this regard, the market of new technologies and innovative industrial services in this field shows a considerable growth. However, the risks of information exchange space in the computer networks of the rail transport industry are still considered one of the most important challenges in this field. Therefore, in this study, in addition to presenting a conceptual model, an attempt has been made to identify environmental threats and gain awareness about the vulnerability of rail transportation systems against cyber attacks, using a case example that includes the violation of the safety structures of critical facilities in the rail transportation industry. In this study, it has tried to investigate the existing vulnerabilities in the railway industry through the RAMS risk analysis model. Therefore, for the case study of the current research, an attack tree was used, which can provide the possibility of analyzing security and safety risks using systemic approaches in the rail network in an integrated manner. Some findings of the current research show that security risks in the rail network have the same importance as safety risks, and therefore, coherent integration between cyber security and rail transportation safety can increase the effectiveness of security measures in the rail network.

Keywords: Cyber security, safety engineering, rail transportation, resilience, penetration, RAMS analysis.

1. Corresponding Author: Associate Professor, Faculty of Industrial Engineering, Islamic Azad University, Parand Branch, Iran.
pejmansalehi.metro@gmail.com
2. Department of Educational Industrial Engineering, Faculty of Industrial Engineering, Azad University, Parand branch.
3. Faculty of Industrial Engineering, Islamic Azad University, Parand branch.



بررسی امنیت فضای سایبری و مهندسی ایمنی در سیستم ها و زیرسیستم های شبکه حمل و نقل ریلی (مطالعه موردی: راه آهن منطقه ای ایتالیا)

مهران خلج^۱ | داود جعفری^۲ | پژمان صالحی^۳

چکیده

مطالعه پیشینه حملات سایبری به شبکه های رایانه ای و سامانه های حمل و نقل ریلی، آسیب پذیری این سیستم ها و زیرسیستم های مرتبط را در مقابل تهدیدهای احتمالی نفوذگران و مهاجمان نشان می دهد. طی سال های اخیر روش های اجرایی و دستورالعمل های متنوعی برای ارتقای سطح امنیت سامانه های ریلی در برابر ریسک های موجود در فضای مجازی طراحی و مستندسازی شده است. تعدد فراوان و تنوع وسیع در دامنه شمول این اسناد، اهمیت و ضرورت ایمنی و امنیت را در برابر حملات فزاینده و پیچیده کنونی حوزه های سایبری نشان می دهد. در این راستا بازار فن آوری های جدید و خدمات نوآورانه صنعتی در این حوزه، رشد قابل ملاحظه ای را نشان می دهد. باین حال مخاطرات فضای تبادل اطلاعات در شبکه های رایانه ای صنعت حمل و نقل ریلی همچنان یکی از مهم ترین چالش های این حوزه محسوب می شود. لذا در این مطالعه ضمن ارائه یک مدل مفهومی کوشیده شده است به منظور شناسایی تهدیدهای محیطی و کسب آگاهی در خصوص نقاط آسیب پذیری سیستم های حمل و نقل ریلی در برابر حملات سایبری از یک نمونه موردی که شامل نقض ساختارهای ایمنی تسهیلات حیاتی در صنعت حمل و نقل ریلی است، استفاده شود. در این مطالعه کوشیده است آسیب پذیری های موجود در صنعت ریلی از طریق مدل تحلیل ریسک RAMS^۴ بررسی نماید. از این رو برای مطالعه موردی تحقیق حاضر از یک درخت حمله استفاده شده که می تواند امکان تحلیل ریسک های امنیتی و ایمنی را با استفاده از رهیافت های سیستمی در شبکه ریلی به صورت یکپارچه فراهم نماید. برخی یافته های تحقیق حاضر نشان می دهد که مخاطرات امنیتی در شبکه ریلی دارای اهمیتی برابر با ریسک های ایمنی است و لذا یکپارچگی منسجم میان امنیت سایبری و ایمنی حمل و نقل ریلی می تواند اثرگذاری اقدامات تأمینی را در شبکه ریلی افزایش می دهد.

کلیدواژه ها: امنیت سایبری، مهندسی ایمنی، حمل و نقل ریلی، تاب آوری، نفوذ گری، تحلیل RAMS

۱. نویسنده مسئول: دانشیار دانشکده مهندسی صنایع، دانشگاه آزاد اسلامی واحد پرند، ایران.
pejmansalehi.metro@gmail.com

۲. دانشیار دانشکده مهندسی صنایع، دانشگاه آزاد اسلامی واحد پرند، ایران.

۳. دکتری مهندسی صنایع، دانشگاه آزاد اسلامی واحد پرند، ایران.

۴. قابلیت اطمینان (Reliability)؛ قابلیت دسترسی (Availability)؛ قابلیت تعمیر و تعویض (Maintainability)؛

ایمنی (Safety)

مقدمه و بیان مسئله

در ادبیات صنعت حمل‌ونقل ریلی، سامانه‌های نرم‌افزاری و سخت‌افزاری بهره‌برداری و عملیاتی از نظر ساختاری و کارکردی دارای وجوه تمایز متعددی هستند (آمبروس^۱ و همکاران، ۲۰۱۸). سامانه‌های بهره‌برداری اصطلاحاً به بخش‌هایی اطلاق می‌گردد که مستقیماً با مسافران در ارتباط بوده و خدمات جابجای شهری و بین‌شهری را به ایشان عرضه می‌کنند. از سوی دیگر سامانه‌های عملیاتی به‌طور مستقیم، عملکرد ایمن تسهیلات و تجهیزات ثابت و متحرک در شبکه ریلی را تضمین می‌نمایند. به‌این ترتیب از آنجایی که سامانه‌های فن‌آوری اطلاعات و ارتباطات برای ارسال و دریافت داده‌ها در سیستم‌ها و زیرسیستم‌های کنترلی ناوگان قطارها و تجهیزات کنار خط مورد استفاده قرار می‌گیرند لذا امنیت فضای تبادل اطلاعات در محیط تعاملی ماشین و کاربران مراکز ناوبری عملیات و کنترل کننده‌های سایبرنتیک با عنوان «مهندسی حفاظت اطلاعات و نرم‌افزارهای ریلی» در نظر گرفته می‌شود (زلوسکی^۲ و همکاران، ۲۰۱۹). از سوی دیگر فرآیند امنیت سایبری به‌عنوان «مهندسی حفاظت از عملکرد ایمن سامانه‌های کنترلی قطار» در نظر گرفته می‌شود که می‌تواند امنیت سایبری شبکه ریلی را از طریق دسترس‌پذیری، یکپارچگی و محرمانگی برآورده نماید (باریل^۳ و همکاران، ۲۰۱۶). استقرار الگوی عمومی RAMS در شبکه‌های ریلی، چارچوب تحصیل قابلیت اطمینان تجهیزات و سامانه‌ها، نگهداری و تعمیر پذیری تسهیلات و ایمنی زیرسیستم‌های کنترل قطار را تضمین می‌نماید (یامپولسکی^۴، ۲۰۱۷). امنیت سایبری در صنعت حمل‌ونقل ریلی یک مسئله پیچیده و چندوجهی است که لازم است آلترناتیوهای مرتبط با آن توأم با رویکردهای ایمنی ارائه گردد. استانداردهای امنیت سایبری که توسط اتحادیه بین‌المللی راه‌آهن‌ها^۵ و اتحادیه اروپا ارائه شده است یکپارچگی کارکردهای ایمنی و امنیت سایبری را ترویج می‌نماید (بارنا^۶، ۲۰۲۲). درهم تنیدگی ایمنی و امنیت در صنعت حمل و نقل ریلی، همانندی ضرورت و اهمیت این دو مؤلفه را در کنترل سیر و حرکت قطارها نشان

1 - Ambrose
2- Zalewski
3- Bar-El
4- Yampolskiy
5 - UIC
6- Barna

می‌دهد (تالبی^۱، ۲۰۱۷). در این بین حفاظت فیزیکی به عنوان یکی از مؤلفه‌های تأثیرگذار بر امنیت سایبری، می‌تواند نخستین مرحله از یک نفوذ مخرب باشد لذا علاوه بر بُعد ایمنی لازم است حفاظت فیزیکی نیز به صورت یکپارچه با ایمنی و امنیت لحاظ گردد (فرگ^۲ و همکاران، ۲۰۱۸). به عنوان یک مورد عملی، پروژه ریل سایبری^۳ در اتحادیه اروپا به ارائه راهکردهایی برای ارتقای امنیت سایبری در سیستم‌های سیگنالی‌نگ شبکه ریلی با استفاده از شناسایی و ارزیابی ریسک‌های سایبری می‌پردازد و لزوم پیاده‌سازی مدل RAMS را توصیه می‌نماید. در این الگو با استفاده از سیستم‌های تشخیص نفوذ (IDS)، سامانه‌های مبتنی بر فن‌آوری اطلاعات و سایر زیرسیستم‌های عملیاتی نظیر پکیج‌های علائم و ارتباطات به صورت انعطاف‌پذیر پیاده‌سازی شده‌اند (شاکلا^۴، ۲۰۱۹). در این راستا توسعه فن‌آوری‌های مرتبط با امنیت سایبری در صنعت حمل‌ونقل ریلی نظیر استقرار سیستم‌های پیشرفته تشخیص نفوذ در سوئیچ‌ها و فایروال‌های شبکه ریلی برای حفاظت از سامانه‌های عملیاتی حمل‌ونقل ریلی به‌ویژه بخش‌های ناوبری، کنترل و سیگنالی‌نگ از آن جمله است. با این حال بهره‌بردارهای حمل‌ونقل ریلی در به‌کارگیری این سیستم‌ها با چالش مواجه هستند (لاکشمینارایانا^۵، ۲۰۱۹). برنامه‌های امنیتی کاربردی در صنعت حمل و نقل ریلی به سیستم‌های تعبیه‌شده‌ای اطلاق می‌شود که دارای ساختار محاسباتی بوده و با سازوکارهای ساخت‌یافته برای یک محیط پیچیده و کارکردی طراحی شده‌اند و می‌توانند رفتارهای عناصر فعال در شبکه ریلی را از طریق سامانه‌های ریلی پیش‌بینی و کنترل نمایند. سیستم‌های عملیاتی در صنعت حمل و نقل ریلی، به تعبیری زیرسیستم‌های الکترونیکی توسعه‌یافته‌ای هستند که در سامانه‌های کنترلی استقرار یافته و ارزیابی امنیتی سامانه‌ها را راهبری و سازمان‌دهی می‌کنند (کارای^۶، ۲۰۲۱). اختلاف میان سیستم‌های امنیتی در محیط فن‌آوری اطلاعات به تفاوت کاربری‌های عملیاتی این سامانه‌ها بازمی‌گردد لذا در وهله نخست لازم است مسائل مرتبط با امنیت فیزیکی در بخش سخت‌افزاری سامانه‌ها شناسایی گردد و سپس در صورت شناسایی نفوذ؛ ردگیری حمله و آثار مهاجمان انجام گیرد. علاوه بر این در چرخه حیات این قبیل برنامه‌ها، ارزیابی و به‌روزرسانی ساختارها می‌تواند به

1- Talebi

2- Ferrag

3 - CyberRil

4- Shukla

5- Lakshminarayana

6- Karay

شناسایی نقاط ضعف و آسیب‌پذیری‌های شبکه بر اساس اطلاعات به‌روز منتج شود (کومار و استولینگا^۱، ۲۰۲۰). وجود حفرهای امنیتی و آسیب‌پذیری‌های سیستم‌های اطلاعات مدیریتی در شبکه ریلی، زمینه‌ساز بروز نفوذ در سیستم‌های داخلی می‌گردد. این در حالی است که نقاط ضعف سامانه‌های مرتبط با خدمات مسافری می‌تواند موجبات بروز اختلال در روند بهره‌برداری از شبکه ریلی و ایجاد خسارت‌های گسترده برای ذی‌نفعان گردد. سیستم‌های طراحی‌شده در یک زیرساخت (پلتفرم) یکپارچه که با سایر شبکه‌های محلی در ارتباط است، اصطلاحاً یک ساختار شبه مجازی از عناصر سخت‌افزاری فیزیکی را به وجود می‌آورند که در صنایع تولیدی نظیر نفت و گاز مورد استفاده قرار می‌گیرد بنابراین نکته قابل توجه وجود مخاطرات و تهدیدهای سایبری برای این سیستم‌هاست، که گاه تبعات جبران‌ناپذیری را در پی دارد (شکری^۲ و همکاران، ۲۰۱۹). برخی از این خطاها دارای پیامدهای ایمنی است که در نتیجه سبب خرابی تجهیزات متحرک و سیستم‌های کنترل صنعتی می‌گردد در این میان یک رویکرد «سخت‌افزاری (فیزیکی) - سایبری» با شتابی مضاعف توسعه یافته و عوامل دیگر صنعت حمل و نقل ریلی را متأثر می‌سازد.

۲- پیشینه تحقیق

در یک مطالعه، پکیک^۳ (۲۰۲۱) با مرور تهدیدها و آسیب‌های مترتب بر سامانه‌های سخت‌افزاری و نرم‌افزاری در صنعت حمل و نقل ریلی، به طبقه‌بندی انواع حملات سایبری در شبکه ریلی پرداخته و یک چشم‌انداز کلی از تهدیدهای تأثیرگذار بر سامانه‌های کنترل خودکار تعبیه‌شده قطار و تجهیزات کنار خط آهن ارائه داد. نتیجه این تحقیق از طریق تجزیه و تحلیل ریسک‌های امنیتی به ارائه یک مدل برای استقرار و توسعه سیستم‌های امن و ایمن برای مقابله با نفوذگری منتهی شده است.

در مطالعه دیگری که توسط اُکا^۴ (۲۰۱۷) انجام شده است، محقق ضمن طبقه‌بندی انواع حملات فیزیکی و سایبری به پیشنهاد توصیه‌هایی برای تقویت کمی و کیفی زیرساخت‌ها به منظور ارتقای تاب‌آوری در برابر حملات سایبری پرداخته است. در مطالعه مزبور محقق ضمن تبیین

1- Kumar & Stoelinga

2- Shoukry

3- Rekik

4- Oka

سناریوهای مختلف حملات سایبری در شبکه ریلی؛ شیوه‌های شناسایی آسیب‌های نرم‌افزاری و سخت‌افزاری در ناوگان قطارها را بیان نموده است. تمرکز اصلی تحقیق مزبور مطالعه رفتارهای غیرخطی واحدهای برنامه‌پذیر الکترونیکی در سیستم‌های مدیریت و کنترل ترافیک قطارها و سایر زیرسیستم‌های مشابه است.

در مطالعه‌ای که توسط پاپ و بوتیان^۱ (۲۰۱۸) انجام شده است، محققان به بررسی نقش واحدهای کنترل الکترونیکی^۲ در وسایل نقلیه ریلی از طریق بررسی معماری توزیع شده پردازنده‌ها و به‌طور خاص میکروکنترلرهای سری TC1797 پرداخته و از طریق تحلیل نتایج شبیه‌سازی تحت شرایط خاص از قبیل تغییر جریان خروجی‌های برنامه از قبیل تزریق کدهای SQL مخرب و تأثیرات آن بر واحدهای کنترلی پرداخته‌اند. این مطالعه هرچند آسیب‌پذیری‌های ECUهای بازرگانی مورد استفاده در TCMS را تبیین نکرده اما در نتیجه‌گیری تحقیق ضمن تأیید یافته‌های مطالعه اسکینیر (۲۰۰۹) یک حمله فرضی را برای یک نمونه واحدهای کنترل الکترونیکی شبیه‌سازی نموده و بر اساس یافته‌های میدانی نتیجه گرفته است که مکانیسم‌های حفاظت از حافظه و پردازشگر در برابر حملات سایبری در واحدهای کنترل الکترونیکی‌های قطارهای مسافری از استحکام کافی برخوردار نیستند. پژوهش یادشده همچنین چگونگی مواجهه با آسیب‌پذیری‌های نرم‌افزاری را در میکروکنترلرهای قطار مورد آنالیز قرار داده و آورده است که پردازنده‌های قطار در برابر برخی حملات نظیر تزریق کدهای مخرب زبان جستجوی ساختار یافته^۳ دچار خطای سخت‌افزاری شده و باعث بروز مشکلاتی در ولتاژ و کلاک پالس پردازنده می‌شوند. نتایج مطالعه مزبور با بیانی دیگر توسط پونسارد^۴ و همکاران (۲۰۲۲) تأیید شده است.

در مطالعه دیگری پیکین^۵ (۲۰۲۱) به بررسی امنیت شبکه‌های ارتباطی برای انتقال داده‌ها میان وسایل نقلیه ریلی و بخش‌های کنترل ترافیک قطار در قالب توپولوژی (همبندی) CAN پرداخته است. در این مطالعه محقق ضمن تأکید بر ضعف‌های موجود در استانداردهای بین‌المللی و مرتبط در عدم تدقیق جامع ویژگی‌های درونی امنیت شبکه‌های رایانه‌ای ریلی، در نتایج مطالعه خود

1- Papp & Buttyan

2- ECU

3- SQL

4- Ponsard

5- Pekin

آورده است که گذرگاه انتقال داده در شبکه‌های CAN برای ارتباطات شبکه‌های ریلی از امنیت کافی برخوردار نیست زیرا در این همبندی اصول محرمانگی، یکپارچگی، دسترس‌پذیری و همچنین احراز اصالت تضمین نشده و انواع مختلف حملات نظیر جعل، شخص ثالث، ردگیری و غیره... پشتیبانی نمی‌شود. اهمیت این امر تا بدان جا است که در صناعی نظیر خودروسازی یا واگن سازی، برخی از تولیدکنندگان در سامانه‌های مبتنی بر سخت‌افزارهای توزیع شده برای فرستنده و گیرنده پیام در واحدهای کنترل صنعتی الکترونیکی به منظور ایجاد استحکام سامانه‌ها در برابر تهاجمات هکرها از سامانه‌های IPS و IDS برای تشخیص و مقابله با نفوذ و همچنین پروتکل‌های رمزنگاری استفاده می‌شود. با این وجود تعاملات شبکه‌ای و پیام‌های رمزنگاری شده در معرض تهدیدهای دیگری هستند از این رو با استفاده از تحلیل‌های قدرتمند یا سایر تکنیک‌های مکمل برای دریافت پیام رمز شده در مقصد سیستم‌های تعبیه شده در قطار و کنار خط آهن استفاده می‌شود.

نتایج یک مطالعه که توسط آمبروس و همکاران (۲۰۱۸) انجام شده، نشان می‌دهد که هدف برخی از تکنیک‌های حمله در شبکه ریلی، تهاجم به ارتباطات میان سنسورهای فیزیکی نصب شده در قطار و تجهیزات کنار خط آهن با واحدهای مختلف کنترل علائم و سیگنالینگ است. یافته‌های این مطالعه نشان می‌دهد که در این قبیل حملات مهاجمان از طریق تزریق داده‌های نادرست به پایگاه‌های اطلاعات، به دست‌کاری داده‌های صحیح و نرمال حسگرها پرداخته و مقادیر ولتاژ یا جریان را از طریق تداخل‌های الکترومغناطیسی تغییر می‌دهند.

نتایج مطالعه زلوسکی و همکاران (۲۰۱۹) نشان می‌دهد که برخی خبرگان امنیت فن‌آوری اطلاعات و ارتباطات ریلی، قطار را به عنوان یک مجموعه جامع از مراکز جمع‌آوری داده‌های حیاتی برای کنترل فرآیندهای حساس سیر و حرکت قطار در نظر می‌گیرند که می‌تواند توسط نفوذ گران فضای سایبری مورد حمله قرار گیرد. در مطالعه فوق‌الذکر محققان تجهیزات کلیدی قطار شامل را به چندین واحد الکترونیکی کنترل تسهیلات سیر و حرکت تقسیم کرده‌اند که بر روی قطار نصب بوده اما در فرایند سیر ایمن قطار نقش به سزایی دارد و هر یک دارای عملکرد وظیفه‌ای خاصی در کنترل قطار است. برخی از تجهیزات کلیدی از این قرار است: واحد کنترل

قطار (VCU^۱)، واحد کنترل درب‌های قطار (DCU^۲)، واحد کنترل سیستم ترمز قطار (BCU^۳) و واحد کنترل نیروی رانش قطار (TCU^۴). در بخشی از یافته‌های پژوهش مزبور آمده است که سیستم‌های یادشده، بر روی قطار نصب شده‌اند و رفتارهای حرکتی قطار را کنترل و در نتیجه ایمنی آن را در طول مسیر حرکت تضمین می‌نمایند. در همین راستا مطالعه (باریل و همکاران (۲۰۱۶) ضمن تأیید نتایج مطالعه قبلی با بررسی نقاط آسیب‌پذیری و ریسک‌های قطار آورده است که مقصد جذاب و صریح برخی نفوذ گران برای رخنه و حمله به سامانه‌های کنترل درب‌های قطار، سیستم کنترل الکتروموتورها و غیره ... است. در تحقیق یادشده محققان ضمن بیان آسیب‌های سیستم کنترل تراکشن قطار به آنالیز برخی حملات سایبری این بخش پرداخته‌اند. در یک مطالعه دیگر ری کیک و همکاران (۲۰۱۶) به ارزیابی و تحلیل آن دسته از حملات خارجی پرداخته‌اند که می‌تواند به صورت از راه دور و با استفاده از ابزارهای موجود در سیستم مدیریت کنترل ترافیک، ضمن نقض اصول مثلث امنیت (CIA) بر عملکرد سامانه‌های ارتباطی و ناوبری قطار متمرکز شده و رفتار نظام‌مند آن را مختل نماید. همچنین در مستندات استاندارد IEEE ISNCC (۲۰۱۹) ضمن تبیین ابعاد محرمانگی، یکپارچگی و دسترس‌پذیری در زیرسامانه‌های کنترلی قطار و مرکز فرمان، مراحل و تکنیک‌های ارزیابی نفوذ گری و حملات سایبری در این سامانه‌ها از طریق تست نفوذ و ارزیابی امنیتی تشریح شده است.

در مطالعه دیگری که توسط اوکا و همکاران (۲۰۱۹) انجام شده است، محققان ضمن تبیین ابعاد مرتبط با تهدیدها و ریسک‌های سیستم کنترل درب‌های قطار به برخی تبعات ناشی از حملات سایبری به این واحد کنترلی پرداخته و یکی از مهم‌ترین آثار تهاجم را بروز خطاهای پیکره‌بندی ذکر کرده‌اند. لازم به ذکر است که ارزیابی و تحلیل ریسک‌های امنیتی و ایمنی در شبکه ریلی با استفاده از ماتریس ارزیابی ریسک به روش FMEA (نظیر تساوی شدت ریسک در احتمال بروز) و به دست آوردن عدد تحلیل ریسک انجام می‌شود و در مورد ارزیابی‌های امنیتی ناشی از حملات سایبری در قطارها از طریق تکنیک‌های ارزیابی‌های امنیتی برای برآورد پتانسیل‌های احتمال بروز نفوذ استفاده می‌شود (تالبی، ۲۰۱۷). در برخی تحقیقات دیگر نظیر

-
- 1- vehicle control unit
 - 2- Doors control unit
 - 3 - Break control unit
 - 4 - Traction control unit

یامپولسکی (۲۰۱۷) و بارنا (۲۰۲۲) به تبعات ادامه سیر قطار پس از ارزیابی امنیتی و وجود ریسک های غیرقابل قبول اشاره نموده اند و در یافته های مطالعه خود آورده اند که برخی آسیب پذیری های شبکه ریلی ناشی از طراحی نایمن نرم افزارهای کنترلی قطار، عدم وجود حفاظت های مستحکم فیزیکی برای تجهیزات رایانه ای و ناآگاهی کارکنان شبکه ریلی نسبت به ماهیت مخاطرات امنیتی است و برخی از تبعات مهم تهاجمات سایبری نظیر شنود شخص ثالث، دستبرد، ویروسی شدن ناشی از بدافزار، انکار، ربایش جلسات ارتباطی میان تجهیزات و غیره ... را ذکر نموده و توصیه کرده اند که برای اتخاذ اقدامات مؤثر متقابل از سیستم های تشخیص نفوذ پیشرفته استفاده شود.

در تحقیق دیگری شاکلا (۲۰۱۹) به بررسی مخاطرات امنیتی مرتبط با سامانه رانش قطار پرداخته است. در مطالعه مزبور محقق ضمن ارزیابی ریسک های سایبری مرتبط با واحد کنترل الکتروموتورهای قطار، برخی تهدیدهای امنیتی مرتبط را ذکر نموده و در یک کار میدانی با اندازه گیری پارامترهای ترمز الکترو دینامیکی؛ در نتایج مطالعه خود آورده است که حملات سایبری در این حوزه می تواند در بستر میدان های الکترومغناطیسی مدارهای خط آهن، با استفاده از سیگنال های جعلی یا تروجان های سخت افزاری و نرم افزاری، سیگنال های الکتریکی را متأثر نموده و با نقض محدودیت های ایمنی مرتبط با ولتاژ، کارایی سیستم را دچار اختلال نماید.

در یک تحقیق که توسط پانسردیتال^۱ و همکاران (۲۰۱۵) در خصوص امنیت سامانه های کنترل ترمز قطار انجام شده است، محققان ضمن ترسیم درخت حمله این سامانه کلیدی، از طریق شیوه های مرسوم و یکپارچه ی ارزیابی مهندسی امنیت و ایمنی صنعت ریلی نشان داده اند که چگونه کارکردهای وظیفه ای سیستم ترمز، می تواند در یک حمله خاص سایبری توسط نفوذ گران به مخاطره افتاده و راهکارهای متقابل تا چه اندازه از اثربخشی برخوردارند.

در یک جمع بندی اجمالی از پیشینه پژوهش مشاهده می شود که خلأ تحقیقاتی وسیعی در خصوص یکپارچگی امنیت فضای سایبری و مهندسی ایمنی وجود دارد که در صورت تحقق می تواند سبب ارتقای سطح استحکام سامانه های عملیاتی و مسافری در مقابل حملات نرم افزاری و

1- Ponsardetal

سخت‌افزاری سیستم‌ها و زیرسیستم‌های شبکه حمل‌ونقل ریلی گردد و از این منظر پژوهش حاضر می‌تواند یک کار جدید و تازه باشد.

۳- روش انجام پژوهش

همان‌گونه که پیش‌تر نیز گفته شد هدف از تحقیق حاضر در یک سطح مفهومی بررسی قابلیت اطمینان، دسترس‌پذیری و یکپارچگی سامانه‌های ایمنی شبکه ریلی است بنابراین روش انجام پژوهش حاضر مبتنی بر تحلیل ایمنی عملیات ریلی از طریق روش‌های کمی و شبیه‌سازی بوده و به پیشنهاد یک رهیافت مبتنی بر قابلیت اطمینان از طریق مدل‌سازی فرکانس و احتمال بروز سانحه با توجه به توپولوژی شبکه ریلی پرداخته است. از سوی دیگر با استفاده از روش‌های کمی به مطالعه امکان‌پذیری حفظ و نگهداشت شبکه ریلی در برابر حملات سایبری از منظر زمان بازیابی سیستم‌ها پرداخته شده و به‌منظور شناسایی ایستگاه‌ها و بخش‌های مهم ریلی از منظر امنیتی از رویکرد K -means استفاده شده است. به‌منظور بررسی اثربخشی خروجی‌های به دست آمده در این مدل، رفتارهای یک سیستم موردی در شرایط واقعی مورد آزمون قرار گرفته است. همچنین از یافته‌های مطالعه موردی به‌منظور مشخص نمودن کارآمدی مدل پیشنهادی در شناسایی ایستگاه‌ها و بخش‌های مهم شبکه ریلی با لحاظ کارایی و ظرفیت شبکه یاری گرفته می‌شود. همچنین در این مطالعه در نهایت شاخص‌هایی برای سنجش ایمنی شبکه راه‌آهن ارائه می‌گردد.

۳-۱- آنالیز توصیفی شبکه ریلی

سیستم ریلی یک شبکه گسترده است که با استفاده از گراف $G=(N,E)$ توصیف می‌شود. در این شبکه $n = N$ نشان‌دهنده ایستگاه‌ها و $e = E$ ناظر بر خطوط ریلی است که ایستگاه‌های مجاور i و j را به هم متصل می‌نماید.

۳-۲- تجزیه و تحلیل قابلیت اطمینان در شبکه ریلی

قابلیت اطمینان شبکه ریلی به عملیات سیر و حرکت قطارها با احتمال عددی وقوع صفر حادثه در زمان بهره‌برداری اطلاق می‌گردد. با توجه به نتایج به دست آمده از مطالعات پیشین می‌توان

احتمال بروز سانحه‌های عمدی (انسان‌ساز) یا غیرعمدی در شبکه ریلی را با توجه کران‌های بالا و پایین احتمال بروز سوانح که به صورت P_{ij}^{up} و P_{ij}^{down} نشان داده می‌شود میان ایستگاه‌های i و j را با استفاده از رابطه زیر به دست آورد:

$$P_{ij}^{up} = \frac{N_{ij}^{up}}{T}, P_{ij}^{down} = \frac{N_{ij}^{down}}{T} \quad \text{رابطه شماره (۱)}$$

در رابطه شماره یک N_{ij}^{up} و N_{ij}^{down} به ترتیب حدود بالا و پایین برای احتمال بروز وقایع برنامه‌ریزی شده در شبکه ریلی هستند و T یک مقدار آماری است که احتمال شکست شبکه ریلی در برابر حملات سایبری را نشان می‌دهد. این مسئله می‌تواند از طریق رابطه زیر توصیف شود:

$$P_{ij} = P_{ij}^{up} P_{ij}^{down} \quad \text{رابطه شماره (۲)}$$

در یک شبکه ریلی تعداد زیادی اعزام برای قطارها در نظر گرفته می‌شود. بنابراین فرض کنیم P_{ik} نشان‌دهنده احتمال بروز سوانح و حملات برنامه‌ریزی شده در مسیر k و ایستگاه ریلی i باشد در این صورت احتمال بروز نفوذ در سیستم‌های ایستگاه ریلی i به صورت رابطه شماره سه نشان داده می‌شود:

$$P_i = \prod_{k=1}^K P_i^k \quad \text{رابطه شماره (۳)}$$

بنابراین قابلیت اطمینان شبکه ریلی در برابر حملات سایبری با استفاده از رابطه شماره چهار به دست می‌آید:

$$R_G = \prod_{ij \in N} (1 - P_{ij}) \prod_{i \in N} (1 - P_i) \quad \text{رابطه شماره (۴)}$$

۳-۳- مدل مفهومی کارایی شبکه ریلی در برابر تهاجمات سایبری و فیزیکی

با در نظر گرفتن جریان ترافیک میان ایستگاه‌های شبکه ریلی، کارایی شبکه ریلی G را می‌توان با استفاده از رابطه شماره ۵ به صورت زیر محاسبه نمود:

$$E = \sum_{mn} \frac{u_{mn}}{d_{mn}} \quad \text{رابطه شماره (۵)}$$

در رابطه فوق u_{mn} تعداد قطارهای عبوری در مسافت میان ایستگاه m تا ایستگاه n را نشان می‌دهد و d_{mn} حداقل فاصله زمانی میان این دو ایستگاه است و E' نشان‌دهنده کارایی زمانی شبکه ریلی برای حالتی است که یک ایستگاه خاص در معرض تهاجم نفوذگران قرار بگیرید در این صورت میزان کارایی شبکه پس از بروز حادثه است که مقدار آن با استفاده از رابطه شماره ۶ به دست می‌آید:

$$\Delta E = \frac{E-E'}{E} \quad \text{رابطه شماره (۶)}$$

حال فرض کنیم X_j^i تعداد قطارهای عبوری بین ایستگاه‌های ریلی مجاور i و j باشد در این صورت چنانچه X_j نشانگر تعداد قطارهای ورودی از سایر ایستگاه‌ها به ایستگاه j باشد. در این صورت خواهیم داشت:

$$F_j^i = \frac{x_j^i}{X_j} \quad \text{رابطه شماره (۷)}$$

همچنین تعداد قطارهای ورودی به ایستگاه j با استفاده از رابطه زیر به دست می‌آید:

$$X_j = \sum_{i=1}^{N-1} F_j^i X_i + \sum_{s=1}^S x_j^s = \sum_{i=1}^{N-1} F_j^i X_i + U_j \quad \text{رابطه شماره (۸)}$$

برای به دست آوردن مجموع قطارهایی که به تمامی ایستگاه‌های شبکه ریلی اعزام می‌شوند می‌توان از رابطه شماره ۹ استفاده نمود:

$$X = F^{(-l)} X + U \quad \text{رابطه شماره (۹)}$$

حال چنانچه قطعه میان ایستگاه‌های U و V نتواند به هر علتی ظرفیت شبکه ریلی را پوشش دهد در این صورت می‌توان شبکه از رابطه زیر برای محاسبه ظرفیت جدید استفاده نمود:

$$X^{-(u,v)} = (1 - F^{(-i-(u,v))})^{-1} U \quad \text{رابطه شماره (۱۰)}$$

با لحاظ آنچه در فوق گفته شد ظرفیت شبکه ریلی پس از بروز حملات سایبری با استفاده از رابطه زیر به دست می‌آید:

$$\Delta C = \frac{\sum X - \sum X^{-(u,v)}}{\sum X} \quad \text{رابطه شماره (۱۱)}$$

زمان بازیابی شبکه ریلی بر اساس تعداد حملات ثبت شده با توجه به زمان شروع و پایان حمله که با t_s و t_e نشان داده می‌شود با استفاده از رابطه شماره ۱۲ به دست می‌آید:

$$M = 1 - \frac{t_r}{t_o} \quad \text{رابطه شماره (۱۲)}$$

۳-۵- تجزیه و تحلیل امنیت و ایمنی

ارزیابی امنیت و ایمنی شبکه ریلی با لحاظ ریسک بروز حمله و از دست رفتن قابلیت دسترس پذیری و نگهداری سیستم (M) و تبعات بروز حمله (S) از رابطه شماره ۱۳ محاسبه می‌شود:

$$S = (1 - R)\Delta A(1 - M) \quad \text{رابطه شماره (۱۳)}$$

در رابطه شماره ۱۳ S تبعات حمله را نشان می‌دهد و R نشان دهنده احتمال بروز نفوذ در شبکه ریلی است. حال چنانچه در حالت بروز حمله به شبکه ریلی قطعات مورد حمله قرار گرفته فرموله شوند مقدار ریسک را می‌توان از رابطه زیر محاسبه نمود:

$$EL_{ij} = p_{ij}\Delta E(1 - M), CL_{ij} = p_{ij}\Delta C(1 - M) \quad \text{رابطه شماره (۱۴)}$$

در رابطه شماره ۱۴ EL_{ij} نشان دهنده مقدار اتلافات شبکه پس از بروز تهاجم و CL_{ij} نشان دهنده اتلاف رخ داده در ظرفیت شبکه در اثر تهاجم نفوذگران است. بنابراین در خصوص عدد ریسک می‌توان از رابطه شماره ۱۵ استفاده نمود:

$$EL_i = p_{ij}\Delta E(1 - M), CL_i = p_{ij}\Delta C(1 - M) \quad \text{رابطه شماره (۱۵)}$$

در رابطه فوق EL_i نشان دهنده مقدار کارایی ازدست رفته شبکه در اثر تهاجم سایبری و CL_i نشان دهنده میزان ظرفیت ازدست رفته شبکه در اثر حملات رخ داده شده است. برای ارزیابی سطح امنیت و ایمنی قطعات ریلی و یا ایستگاه‌ها با توجه به افت کارایی شبکه ناشی از حملات سایبری

از روش K-means استفاده می‌شود. رویکرد K-means یک روش خوشه‌بندی است که می‌تواند داده‌ها را در کلاس‌های مختلف طبقه‌بندی نماید. بنابراین رویکرد K-means می‌تواند به یافتن بخش‌های بحرانی شبکه ریلی و ایستگاه‌ها از منظر امنیت و ایمنی کمک نماید.

۴- مطالعه موردی: بررسی حادثه حمله‌ی سایبری به راه‌آهن منطقه‌ای ایتالیا (۲۰۱۴)

در مورد کاوی این پژوهش ابعاد حمله سایبری به راه‌آهن منطقه‌ای ایتالیا در بخش‌هایی نظیر سامانه کنترل ترمز و سیستم ضد لغزش قطار (WSP^۱) و غیره ... مورد تحلیل قرار گرفته و از طریق بررسی سناریوهای احتمالی حملات سایبری به ارائه یک تحلیل یکپارچه از فضای تهاجم پرداخته شده است.

۴-۱- شرح کلیت سانحه

در راه‌آهن منطقه‌ای ایتالیا، قطاری که با سرعت ۸۰ کیلومتر بر ساعت در حال طی مسیر ریلی تعیین‌شده در جدول زمان‌بندی بود با تأخیری در حدود ۳۰ ثانیه در اعمال ترمز در چرخ‌ها، پس از ارسال پالس سیگنال ترمز‌گیری توسط راهبری قطار مواجه گردید. تحقیقات میدانی کمیسیون عالی سوانح ریلی ایتالیا نشان از بروز اختلال ارتباطی در واحد ضد لغزش چرخ‌ها در سیستم ترمز قطار داشت.

هرچند در پی اقدامات صورت گرفته توسط تیم نگهداری و تعمیرات به‌وسیله پیکره‌بندی مجدد دریاچه‌های WSP با استفاده از استاندارد مرتبط در اتحادیه بین‌المللی راه‌آهن‌ها (سند شماره UIC 541-05) و به‌روزرسانی نرم‌افزار واحد کنترل ترمز به رفع اختلال امکان‌پذیر گردید اما ردگیری سیستم حاکی از نفوذ گری گسترده در این ابزار حیاتی قطار بود.

دپارتمان واکنش اضطراری حملات سایبری راه‌آهن سرتاسری ایتالیا، پس از آنالیز داده‌های ضبط‌شده در بانک اطلاعاتی تشخیص خطاهای قطار، علت سانحه را عملکرد غیرعادی زیرسیستم WSP در سامانه ترمز اعلام نمود و در گزارش نهایی خود این‌گونه توضیح داد: "واحد کنترل WSP در آغاز فرایند ترمز‌گیری، سیگنال غلط دریافت نموده است که در نتیجه به‌عکس العمل

1- Wheel slide protection

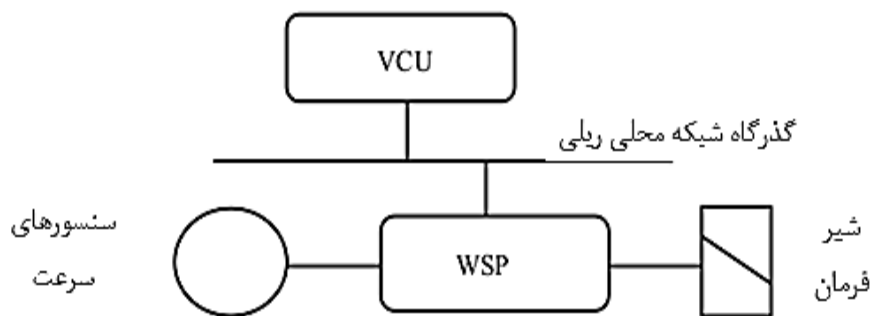
نادرست بخش اجرایی ترمز منتهی شده و این به دلیل پاک شدن داده‌های صحیح در بانک اطلاعاتی بوده و در ادامه، ایجاد اختلال در ارتباط بخش مقایسه کننده‌ی واحد کنترل WPS با مقادیر برنامه‌ریزی شده جدید و اشتباه که در حافظه دیتابیس جایگزین داده‌های درست و ذخیره شده در حافظه به عنوان مقادیر مبنا بوده است و همچنین عدم امکان به روزرسانی جداول متناسب با مختصات خط ریلی بوده که در نهایت به فرمان نادرست برای بخش اجرایی سیستم ترمز منجر شده است". لازم به توضیح است در وسایل نقلیه ریلی، سامانه WSP یک سیستم کنترلی محسوب می‌شود که بر اساس گشتاور قطار در سامانه سیستم ترمز از طریق تنظیم فشار هوا در سیلندرها، فرمان‌های الکتریکی متناسب را برای سوپاپ‌های تخلیه ارسال می‌نماید که ضمن حفظ چسبندگی میان چرخ و ریل، از قفل شدن چرخ‌ها در هنگام ترمزگیری جلوگیری نموده و در نتیجه از خرابی خط و صاف شدن چرخ پیشگیری می‌نماید. بنابراین WSP یک سیستم حیاتی برای ایمنی سیر و حرکت قطارها محسوب می‌شود که بروز اشکال یا خرابی آن می‌تواند اشکالات زیر را در شبکه ریلی ایجاد نماید:

نخست: گشتاور ناکافی نیروی ترمزی و عدم اعمال به هنگام آن که مسافت ترمزی را به صورت غیر نرمال افزایش می‌دهد.

دوم: نیروی گشتاور بیش از حد ترمزی که در نتیجه منجر به لغزش چرخ‌ها در امتداد ریل حرکتی شده که علاوه بر صاف شدن چرخ می‌تواند در موارد حاد باعث خروج قطار از خط شود (لاکشینارایانا، ۲۰۱۹).

در این راستا (بارنا، ۲۰۲۲) شرح جامعی از استانداردهای مرتبط با ایمنی سیر و حرکت از طریق WSP را ارائه نموده است. در این استاندارد شباهت‌های فراوانی میان سیستم WSP و سیستم ضد قفل خودروها (ABS) از نظر معماری و عملکردی ذکر شده است. لذا می‌توان تهدیدها و آسیب‌های مکانیکال مترتب بر ABS را به طور مشابه برای WSP نیز لحاظ نمود و این بدان معناست که سنسورهای WSP از همان فن‌آوری‌های ساختاری مشابه استفاده می‌کنند. در مطالعه انجام شده توسط زلوسکی و همکاران (۲۰۱۹) عکس‌العمل‌های سیستم در قبال تزریق کدهای مخرب به پایگاه اطلاعات این سامانه مورد بررسی قرار گرفته است. در مطالعه دیگری که توسط شکری و همکاران (۲۰۱۹) در خصوص این فن‌آوری انجام گرفته، محققان به توصیف

تکنیک‌های حمله به زیرسیستم WSP پرداخته و از نتایج آن برای تجزیه و تحلیل آسیب‌های احتمالی سامانه نرم‌افزاری WSP در صنعت حمل و نقل ریلی استفاده کرده‌اند. از نظر عملکردی واحد کنترل قطار (VCU) به عنوان یک مرجع اصلی، به اندازه‌گیری سرعت واگن‌های قطار می‌پردازد و اطلاعات به دست آمده را برای واحد کنترلر WSP ارسال می‌نماید. واحد کنترل WSP داده‌های گردآوری شده از سنسورهای سرعت هریک از محورهای بوژی قطار را با سرعت برنامه‌ریزی شده در ماژول مربوطه مورد مقایسه قرار داده و با استفاده از آن از طریق شیر تخلیه فشار هوای فشرده پشت سیلندر ترمز را تنظیم نموده و قدرت ترمزی را هماهنگ می‌سازد. در تصویر شماره یک، ضمن ترسیم معماری زیرسیستم WSP نصب شده در قطار حادثه راه آهن منطقه‌ای ایتالیا به تجزیه و تحلیل عملکرد سیستم پرداخته شده است.



تصویر شماره ۱) معماری ساختار WSP به بیان ساده

طبق معماری ترسیمی در تصویر شماره یک می‌توان توابعی عملکردی هر یک از بخش‌ها به شرح ادامه تبیین نمود:

➤ سنسورهای سرعت: بر اساس استانداردهای تولید قطار، سنسورهای سرعت که بر روی قطار نصب شده‌اند از نوع مغناطیسی است.

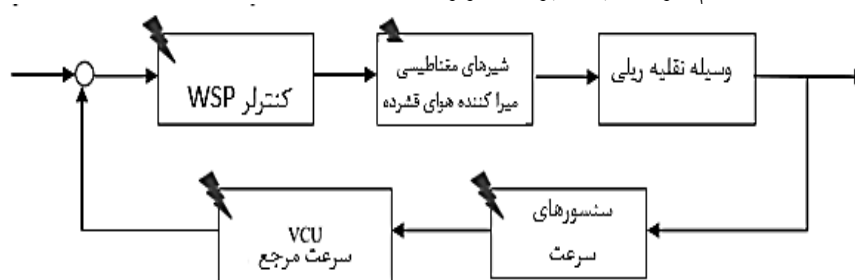
➤ VCU (واحد کنترل قطار): نقش کنترلر را در معماری WSP بر عهده داشته و لذا بر اساس معماری میکروکنترلر تعبیه شده در آن، می‌توان نوع کامپایلر مورد استفاده در نرم‌افزار تشکیل دهنده WSP را استنباط نمود.

➤ گذرگاه انتقال داده محلی قطار که به‌عنوان ابزار مخابراتی و ارتباطی در شبکه تجهیزات سخت‌افزاری قطار مورد استفاده قرار می‌گیرد.

بر اساس نتایج برخی مطالعات نظیر مطالعه کارای (۲۰۲۱) تجهیزات شبکه گذرگاه انتقال داده‌های قطار از چندین بُعد مختلف دارای نقاط آسیب‌پذیری است که از آن جمله می‌توان به موارد زیر اشاره نمود:

نخست: سطح و طیف حمله به سیستم WSP قطار؛ که در تصویر شماره دو بلوک دیاگرام ساده‌شده WSP برای شناسایی نقاط آسیب‌پذیری و تهاجم به WSP قطار ترسیم شده است. بر این اساس واحدهای مختلف WSP قطار برحسب شدت آسیب‌پذیری به شرح زیر است:

- ۱- واحد کنترلر سخت‌افزاری و نرم‌افزاری WSP قطار
- ۲- گذرگاه ارتباطی میان سنسورهای سرعت و واحد پردازش و مقایسه سرعت جاری با سرعت مرجع که در میان گزینه‌های متعدد تجهیزات قطار برای نفوذگران از جذابیت بالایی برخوردار می‌باشد زیرا مهاجمان می‌توانند از طریق تزریق کدهای مخرب به پایگاه داده به ثبت اختلاف غیرواقعی میان سرعت مرجع و سرعت واقعی قطار منجر شده و در نتیجه فرایند اعمال هوای فشرده برای ترمزگیری را دچار خطا نمایند.
- ۳- گذرگاه ارتباطی میان واحد کنترل WSP و شیرهای مغناطیسی تخلیه و تنظیم فشار باد سیلندر ترمزهای سیستم ترمز قطار
- ۴- کنترلر شیرهای مغناطیسی تخلیه هوای فشرده که از طریق تزریق داده‌های اشتباه می‌تواند زمینه تصمیم‌گیری اشتباه را برای کنترلر ایجاد نماید.



تصویر شماره ۲) WSP قطار به‌عنوان یک سیستم کنترل‌کننده

۵- بحث

امروزه حمل و نقل ریلی به یک شیوه محبوب برای جابجایی در شهرها بدل شده است. با این حال حملات سایبری می‌توانند عملیات معمول شبکه ریلی را دچار اختلال نمایند. بنابراین قابلیت اطمینان و دسترس‌پذیری شبکه ریلی از منظر کارکردی لازم است مورد تجزیه و تحلیل قرار گیرد تا میزان آسیب‌پذیری شبکه در برابر شکست‌های امنیتی در تسهیلات ریلی تعیین گردد. قابلیت اطمینان شبکه ریلی یک جنبه مهم است که می‌تواند از حملات سایبری متأثر گردد. در سانحه حمله سایبری به قطار منطقه‌ای ایتالیا با توجه به نتایج تحلیل بردار حمله، نفوذ گران از تکنیک‌های رسوخ به حفره‌های امنیتی، دو بخش کلیدی را مورد تهاجم قرار داده بودند که به شرح زیر بیان می‌شود:

نخست: حمله به واحد کنترل الکترونیکی WSP قطار با هدف تخریب حافظه داخلی از طریق تزریق کدهای غلط و بهره‌گیری از تکنیک نفوذگری سرریز بافر در WSP قطار

دوم: حمله نفوذ گران به گذرگاه انتقال داده و شبکه ارتباطی میان سنسورهای سرعت و واحد کنترل الکترونیکی WSP که از طریق تزریق اطلاعات نادرست، سبب ایجاد تفاوت غیر واقعی میان سرعت واقعی و سرعت مرجع در خط منطقه‌ای ایتالیا گردید و در نتیجه به رفتار غیر نرمال واحد کنترل WSP منجر شد. هرچند بر اساس اعلام شرکت سازنده قطار، بروز این رخداد از شرایط بسیار نادر در سامانه‌ی ترمز قطارها بوده، اما با این حال بر اساس گزارش دپارتمان امنیت و ایمنی وقوع این سانحه ناشی از درک نادرست شرکت سازنده از رفتار واقعی سامانه ترمز قطارها در مناطق بین‌شهری بوده است، هرچند بر اساس شواهد به‌دست آمده، تمامی اجزا و ارکان سیستم کنترل WSP در ناوگان قطارهای راه‌آهن ایتالیا با استانداردهای خاص تدوین شده توسط اتحادیه بین‌المللی راه‌آهن‌ها (UIC) انطباق داشته است، لیکن تنظیم نامناسب شیرهای مغناطیسی تخلیه هوای فشرده در سری‌های زمانی غلط بر اساس حمله سایبری، سبب عملکرد نادرست واحد کنترل در تنظیم WSP برای پیکره‌بندی صحیح خروجی سنسورهای سرعت قطار گردید. در این سانحه

تجزیه و تحلیل واحد کنترل الکترونیکی WSP نشان داد که پیامدهای ناشی از عدم شناسایی ریسک‌ها و تهدیدهای بالقوه، ترکیبی از علل بروز خطا را به وجود آورد که در اثر آن زمینه مناسبی برای تهاجم نفوذ گران را به وجود آورد که سامانه‌ی ترمز قطار را دچار اختلال نمود. آموزه‌های این حادثه به پیشنهاد‌های جدید برای طبقه‌بندی حملات تأثیرگذار بر سیستم ترمز قطار منتهی گردید که می‌تواند در یکی از دسته‌های زیر قرار گرفته و یا ترکیبی از آن‌ها باشد:

- حملات فیزیکی که در آن مهاجمان معماری سیستم‌های کنترل قطار را با هدف طراحی دلخواه برای نفوذ از طریق نصب سیستم‌های مخرب تغییر می‌دهند.
- حملات غیرفعال از طریق کانال‌های جانبی قطار که در آن مهاجمان با مشاهده و شنود سیگنال‌های ارتباطات بیرونی سیستم و تجزیه و تحلیل توان دفاعی، زمان اجرای یک برنامه را بر اساس نشت مغناطیسی داده‌ها برای به دست آوردن کلیدهای رمزنگاری مورد استفاده قرار می‌دهند.
- حملات منطقی به شبکه‌های ارتباطی و نرم‌افزارهای نصب‌شده در قطار
- استفاده نفوذ گران از تکنیک درب‌های پشتی^۱ بر اساس بهره‌گیری از آسیب‌پذیری‌های نرم‌افزارهایی که پیش‌تر از طریق بدافزارها و کدهای مخرب در قطار نصب شده‌اند. به‌عنوان مثال استفاده از سرریز بافر که برای تغییر روند اجرای برنامه‌های سیر و حرکت قطارها از طریق گدهای مخرب به حافظه سخت‌افزار تزریق شده‌اند.
- استفاده از ضعف‌های موجود در رمزنگاری و پروتکل‌های مربوطه به‌منظور رمزگشایی از پیام‌های ارسال شده بر روی شبکه‌های مخابراتی قطارها و اجرای حملاتی نظیر جعل، تغییر، تزریق پیام، ایجاد ترافیک کاذب، MITM و غیره در سامانه سیر و حرکت قطارها

در حادثه قطار منطقه‌ای ایتالیا، داده‌های تغیر یافته که از طریق شبکه ارتباطی قطار برای تنظیم سرعت ارسال شدند دارای تبعاتی چندگانه بودند. حملات در این سانحه در یک سری زمانی

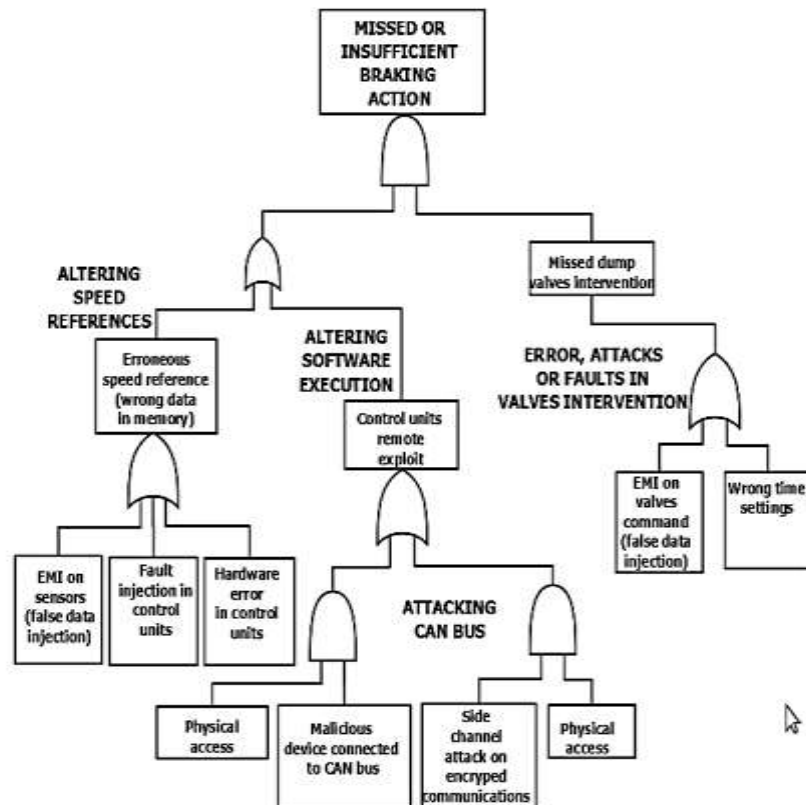
1- backdoor

متوالی و متناسب و بر اساس طرح قبلی با هم ترکیب شدند تا اهداف مدنظر مهاجمان برآورده شود. آثار این تهاجم نشان می‌دهد که خطاها می‌توانند که خود می‌توانند ناشی از خرابی تجهیزات و یا نقص فنی باشد و در زمره آسیب‌پذیری‌های شبکه ریلی به شمار می‌آیند. خطاهای سیستم توسط حملات فعال مورد استفاده قرار می‌گیرد و آسیب‌پذیری‌ها توسط تهدیدهای محیطی شبکه ریلی استفاده می‌شوند و این در حالی است که اشتباهات کاربران شبکه ریلی می‌تواند منشأ حملات فعال و بالفعل نمودن تهدیدها شود.

ملاحظات فوق در سانحه ریلی قطار منطقه‌ای فرانسه برای محققان دو دستاورد مهم به همراه داشت که عبارت بودند از نخست: اهمیت تحلیل کلی ریسک‌های سیستم و دوم: ضرورت یکپارچه‌سازی تجزیه و تحلیل خطاها و آسیب‌پذیری‌های سیستم

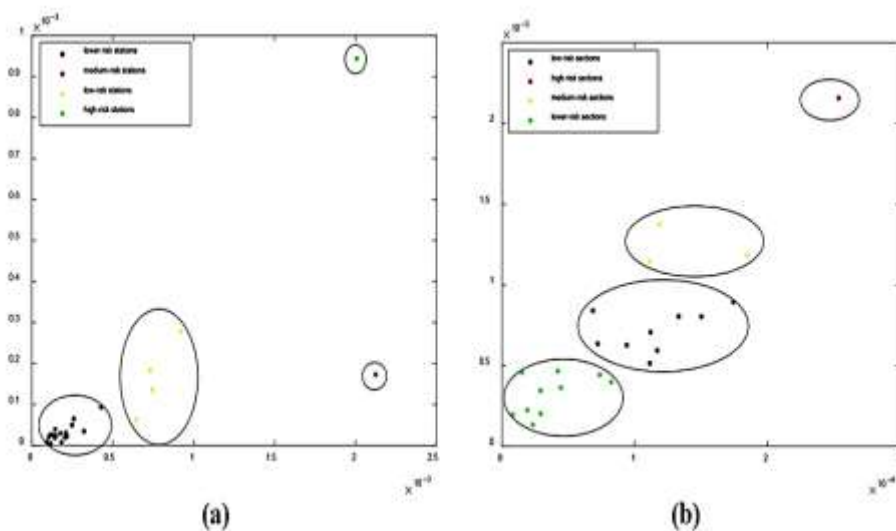
برای نیل به دستاوردهای فوق می‌توان از تکنیک توأمان درخت حمله و خطا استفاده نمود. بر اساس استانداردهای EN 50126 و IEC 61025 درخت تجزیه و تحلیل خطا و درخت حمله می‌توانند برای آنالیز شکست‌ها و شناسایی ریسک‌ها در شبکه ریلی مورد استفاده قرار گرفته و نشان‌دهنده تعامل و رابطه علی میان خرابی‌های سیستم، زیرسیستم‌ها و قطعات باشد که به‌طور مشابه در درخت حمله و خطا به‌عنوان یک تکنیک مؤثر شناسایی و نمایش حملات سایبری از طریق ساختارهای درختی، هم برای حملات مجزا به تجهیزات و یا کل وسیله نقلیه ریلی مورد استفاده قرار گرفته، و برای برآورد ریسک مخاطرات سایبری در ناوگان قطارها و زیرساخت‌های شبکه ریلی استفاده گردد.

با در نظر گرفتن جمیع جهات فوق می‌توان چنین اذعان نمود که برای مواجهه با حوادث مشابه، لازم است درخت حمله و درخت خطا به‌صورت یکپارچه برای تجزیه و تحلیل مخاطرات و شناسایی تهدیدها در شبکه ریلی مورد استفاده قرار گیرد که این خود ناظر بر مهندسی ایمنی و امنیت سایبری به‌صورت مشترک است که برای مورد مطالعه در تحقیق حاضر به‌صورت تصویر شماره سه نشان داده می‌شود.



تصویر شماره ۳) یکپارچگی درخت حمله و درخت خطا برای ارتقای امنیت سایبری و ایمنی شبکه ریلی در مطالعه موردی راه‌آهن منطقه‌ای ایتالیا

درخت حمله به‌عنوان یک ابزار تحلیلی می‌تواند به‌منظور دستیابی به مسیر «خطا - حمله» مورد استفاده قرار گیرد. از طرفی تکنیک‌های تحلیلی لازم است در یک رویکرد یکپارچه و تشکیل‌شده از موارد ایمنی و امنیتی برای توسعه دستورالعمل‌ها و استانداردها مورد استفاده قرار گیرد. در این مطالعه نتایج تجزیه و تحلیل RAMS در تصویر شماره ۴ ترسیم شده است. در این شکل قسمت a از دست رفتن کارآمدی شبکه ریلی در اثر تهاجمات سایبری متناسب با کاهش ظرفیت شبکه را نشان می‌دهد در قسمت b از تصویر شماره ۴ ظرفیت ازدست‌رفته شبکه ریلی در اثر تهاجم سایبری به تصویر کشیده شده است.



تصویر شماره ۴) میزان کارایی و ظرفیت ازدست‌رفته شبکه ریلی در اثر حملات سایبری

نتیجه‌گیری

در این تحقیق پس از بررسی ابعاد مختلف ایمنی و امنیت در صنعت حمل‌ونقل ریلی، ضرورت همراستائی توأمان آن‌ها مورد بررسی قرار گرفت. در این پژوهش همچنین به‌عنوان یک مطالعه موردی سانحه حمله سایبری به قطار منطقه‌ای ایتالیا بررسی گردید. چنانکه در قسمت یافته‌های پژوهش بحث گردید، گراف حمله سایبری به قطار با نقایص ایمنی عملیات، یک فراگرد سازگار است. در مورد کاوی این تحقیق هرچند هر یک از بخش‌های زیرسیستم سامانه ضد لغزش چرخ‌ها (WSP) با الزامات و استانداردهای مدون در صنعت حمل‌ونقل ریلی انطباق دارند ولی بااین‌حال فقدان یک رویکرد یکپارچه برای ایمنی و امنیت سایبری، می‌تواند به نتایج غافلگیرکننده‌ای در شبکه ریلی منتهی گردد. از طرفی هنگامی که سخن از سیستم‌های عملیاتی در صنعت حمل‌ونقل ریلی می‌شود، امنیت سایبری علاوه بر موارد مرتبط با آسیب‌پذیری‌های نرم‌افزارهای کاربردی سیر و حرکت قطار، سامانه‌های خدمات مسافری و سیستم‌های اطلاعاتی ریلی را نیز در برمی‌گیرد زیرا نقاط ضعف، آسیب‌پذیری‌های نرم‌افزاری و تهدیدهای ناشی از

نشت سیگنال‌های الکترومغناطیسی می‌تواند به صورت مستقل یا وابسته هر یک از تجهیزات و یا مجموعه‌ای از اجزاء مرتبط در ترافیک سیر و حرکت قطارها را از طریق کدهای مخرب یا بدافزارهای نصب شده؛ به صورت حملات منفرد و یا ترکیبی از تکنیک‌های نفوذگری متأثر سازد. از این رو به عنوان یک نوآوری در این تحقیق، در بررسی سانحه نفوذ راه آهن منطقه‌ای ایتالیا؛ ریسک‌های ترکیبی (امنیتی و ایمنی) بر اساس درخت حمله برای سیستم‌ها و زیرسیستم‌های «فیزیکی-سایبری» شبکه ریلی آنالیز شدند. استفاده از این تکنیک برای تجزیه و تحلیل مدیریت اختلال و کنترل قطارها می‌تواند ابعاد متنوع و جدیدی را اضافه و مورد بررسی قرار دهد و از این راه بینش مناسبی را برای ارزیابی ریسک‌های امنیتی با لحاظ مهندسی ایمنی عملیات در شبکه حمل و نقل ریلی فراهم آورد.

فهرست منابع

- Ambrose, J.; Ragel, R.; Jayasinghe, D.; Li, T.; Parameswaran, S. (2018). Side channel attacks in embedded systems: A tale of hostilities and deterrence. 452-459.
- Bar-El, H.; Choukri, H.; Naccache, D.; Tunstall, L.; Whelan, L. (2016). "The Sorcerer's Apprentice Guide to Fault Attacks", in Proc. of IEEE, vol. 94, issue 2, pp:370-382.
- Barna, G. (2022).; Control system of wheel slide protection devices for rail vehicles meeting the requirements of European normative documents -CzasopismoTechniczne, MechanikaZeszyt 7-M/2022.
- Ferrag M. A.; Chekkai N.; Nafa M. (2018). - Securing Embedded Systems: Cyberattacks, Countermeasures and Challenges in Securing Cyber-Physical Systems - CRC Press.
- Lakshminarayana, S.; Teo, Z.; Tan, R.; Yau, D.K.Y.; Arboleya, P. (2019) "On False Data Injection Attacks Against Railway Traction Power Systems," 2019 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Toulouse, 2019, pp. 383-394.
- Karray, K.; Danger, J; Guilley, S; El Aabid, M. A. (2021). Attack tree construction: an application to the connected vehicle - Cyber-physical security education workshop - Paris, France — July 17-19, 2020 or Cyber-Physical Systems Security - Springer .
- Kumar, R.; Stoelinga, M. (2020). Quantitative Security and Safety Analysis with Attack-Fault Trees. 10.1109/HASE.2020.12.
- Rekik, M.; Gransart, C.; Berbineau, M. (2021). - Cyber-Physical Security Risk Assessment for Train Control and Monitoring Systems. SSV, 1st International Workshop on System Security and Vulnerability, IEEE CNS Conference on Communications and Network Security, May 2021.
- Pekin, China. SSV 2021, 1st International Workshop on System Security and Vulnerability, IEEE CNS Conference on Communications and Network Security, 9p, 2021.
- Rekik, M.; Gransart, C.; Berbineau, M. (2020) - Cyber-physical Threats and Vulnerabilities Analysis for Train Control and Monitoring Systems.
- IEEE ISNCC 2019, International Symposium on Networks, Computers and Communications, Jun 2019, Rome, Italy.
- IEEE ISNCC 2021, International Symposium on Networks, Computers and Communications, 6p, 2021.
- Oka, D.; Matsuki, T. (2017). A security assessment study and trial of Tricore-powered automotive ECU.
- Oka, D., Langenhof, L., Marie-Louise, M. & Waguri, N. & Matsuki, T. (2019). Investigation of How to Exploit Software Vulnerabilities on an Automotive Microcontroller and Corresponding Security Measures.
- Papp, D.; Ma, Z.; Buttyan, L. (2018) - Embedded Systems Security: Threats, Vulnerabilities, and Attack Taxonomy - 2015 Thirteenth Annual Conference on Privacy, Security and Trust (PST)
- Ponsard, C.; Massonet, P., Dallons, G. 2022- Co-engineering Security and Safety Requirements for Cyber-Physical Systems - The European Research Consortium for Informatics and Mathematics ERCIM News 106, Special theme: Cybersecurity.
- Schneier, B. - Attack Trees - Dr. Dobb's Journal, December 2009 - https://www.schneier.com/academic/archives/2009/12/attack_trees.html

- Shoukry, Y.; Paul Martin, P.; Paulo Tabuada, P. (2019). Srivastava, M - Non-invasive Spoofing Attacks for Anti-lock Braking Systems – International Workshop on Cryptographic Hardware and Embedded Systems, pp. 55-72.
- Shukla, S. (2019). - Embedded Security for Vehicles, ECU Hacking - Uppsala Universitet - Department of Information Technology.
- Talebi, S. (2017). A Security Evaluation and Internal Penetration Testing Of the CAN-bus - Chalmers University of Technology Department of Computer Science and Engineering - Göteborg, Sweden, October 2017.
- Yampolskiy, M.; Horvath, P.; Koutsoukos, X.D.; Xue, Y.; Sztipanovits, J. (2017)- Taxonomy for description of cross-domain attacks on CPS –HiCoNS'13 Proceedings of the 2nd ACM international conference on High confidence networked systems
- Zalewski, J.; Buckley, I.A.; Czejdo, B.; Drager, S.; Kornecki, A.J. (2019). Subramanian, N. A Framework for Measuring Security as a System Property.

