

TOMSAC - روش مدیریت تعادل بین ایمنی خودرویی و امنیت سایبری

شارا شاهوردیان

۴۰۲۱۵۷۴۱۰۰۲۰۹۹

کیانا ساسانیان

۴۰۲۱۵۷۴۱۰۰۲۰۹۹

علیرضا سلطانی نشان

۴۰۲۱۵۷۴۱۰۰۲۰۹۹

محمد خورشیدی روزبهرانی

۴۰۲۱۵۷۴۱۰۰۲۰۱۳

محمد سعید هاشمی طاهری

۴۰۲۱۵۷۴۱۰۰۲۰۹۹

چکیده

وابستگی‌های متقابل ایمنی و امنیت برای محققان چندین دهه مورد توجه بوده است. با این حال، در عمل، به دلایل مختلفی از جمله عدم درک کافی و تمایل به تغییر رویه‌های فعلی، توجه لازم به آن‌ها نمی‌شود. این تحقیق با هدف پیشبرد وضعیت هنر در این زمینه با توسعه یک روش عملی، آسان برای انطباق و استفاده برای مدیریت وابستگی‌ها و تعادل‌ها در طول دوره توسعه سیستم‌های سایبر-فیزیکی انجام شده است. این روش به نام TOMSAC که مخفف مدیریت تعادل بین ایمنی و امنیت سایبری است، نامیده شده است.

۱ مقدمه

یک بررسی جامع از روش‌های مهندسی مشترک برای ایمنی و امنیت سایبری در سراسر حوزه سایبر-فیزیکی توسط Kavallieratos و همکاران (۲۰۲۰) ارائه شده است. این مقاله یک بررسی جامع از ۶۸ روش مهندسی مشترک ایمنی و امنیت سایبری ارائه می‌دهد و به مسائل باز و چالش‌های پژوهشی مرتبط می‌پردازد. این ۶۸ روش به دو دسته "یکپارچه" (یعنی دو فرآیند جداگانه مرتبط ایمنی و امنیت) و "ترکیبی" (یعنی یک فرآیند یکپارچه که هم ایمنی و هم امنیت را ترکیب می‌کند) تقسیم می‌شوند. ۳۷ روش از روش‌های بررسی‌شده یکپارچه هستند و ۳۱ روش ترکیبی. بیشتر روش‌های بررسی‌شده مدل‌محور هستند (۵۲ از ۶۸) و برای یک حوزه کاربردی واحد توسعه یافته‌اند (۴۵). تنها ۲۰ روش با استانداردهای مربوطه اطلاعاتی دارند و جالب این است که اکثر روش‌های بررسی‌شده (۴۹) به مسئله حل تضاد نمی‌پردازند. تنها ۲۸ روش شامل تکنیک‌هایی برای ارتباط نتایج با ذینفعان هستند، در حالی که اکثریت (۴۱) توسط هیچ ابزار یا جعبه‌ابزاری پشتیبانی نمی‌شوند. در مجموع، این نتایج نشان می‌دهد که حوزه مهندسی مشترک امنیت سایبری و ایمنی هنوز بالغ نشده است.

Eames و Moffett (۱۹۹۹) بیان می‌کنند که روش‌هایی که تلاش می‌کنند تحلیل‌های ایمنی و امنیتی را یکپارچه کنند، معایبی دارند و نتیجه‌گیری می‌کنند که "در اکثر موارد تلاش برای یکپارچه‌سازی تحلیل‌های ریسک ایمنی و امنیت نامناسب است." در مورد 'ادغام'، آن‌ها نتیجه می‌گیرند که "ارزش ادغام ایمنی و امنیت در هماهنگ‌سازی تکنیک‌های هر حوزه است." این روش (ادغام) اجازه می‌دهد تا تکنیک‌های تخصصی هر دو حوزه ایمنی و امنیت بدون تغییر باقی بمانند و نیاز به آموزش مجدد تخصص‌های ویژه نباشد.

پروژه AQUAS (Pomante و همکاران، ۲۰۱۹) با هدف بررسی وابستگی‌های متقابل ایمنی، امنیت و عملکرد در زمینه افزایش پیچیدگی ناشی از اتصال دنیای باز و دنیای تعبیه شده آغاز شد. آن‌ها این کار را در پنج حوزه مختلف (مدیریت ترافیک هوایی، دستگاه‌های پزشکی، واگن‌های ریلی، درایو صنعتی و معماری‌های چند هسته‌ای فضایی) انجام دادند.

یکی از مشارکت‌های کلیدی AQUAS ارتقا روش‌های ترکیبی برای استانداردها فراتر از وضعیت کنونی بود. این کار با تکامل مفهوم و عملی کردن پرونده‌های ایمنی اطلاع‌رسانی شده توسط امنیت انجام شد که تأثیر آن بر عملکرد در نظر گرفته شده بود. همچنین مفاهیم سیستم‌های سیستم‌ها نیز مورد بررسی قرار گرفت. مقاله AQUAS نزدیک‌ترین به روش ماست که به حوزه خودرویی محدود شده است.

در زمینه خودرویی، از سال ۲۰۱۳ Bloomfield و همکاران (۲۰۱۳) بر روی "ایمنی اطلاع‌رسانی شده توسط امنیت" بر اساس تأثیر امنیت بر پرونده‌های ایمنی ساختاری کار می‌کردند. آن‌ها به چالش‌های موجود در هم‌کاری ایمنی و امنیت، از جمله نیاز به یک هستی‌شناسی مشترک، تفاوت‌های اصول زیربنایی این حوزه‌ها، مدل‌های تهدید متفاوت و نیاز به یک رویکرد مشترک به استانداردهای ایمنی و امنیت اشاره می‌کنند. این

علاقه منجر به نگارش کد رفتار BSI PAS:11281 توسط Bloomfield Robin و دیگران از شرکت او شد تا "توصیه‌هایی برای مدیریت ریسک‌های امنیتی که ممکن است به مصالحه ایمنی در اکوسیستم خودروی متصل منجر شوند" ارائه دهد (مؤسسه استاندارد بریتانیا، ۲۰۱۸).

اخیراً، امنیت سایبری برای چندین دسته وسیله نقلیه از جمله خودروهای سواری، اتوبوس‌ها و کامیون‌ها به یک حوزه تحت نظارت تبدیل شده است. مقررات UN ۱۵۵ (UNECE، ۲۰۲۱a) و ۱۵۶ (UNECE، ۲۰۲۱b) به ترتیب الزامات امنیت سایبری و به‌روزرسانی نرم‌افزار را مشخص می‌کنند که تولیدکنندگان باید برای دریافت تایید نوع برای آن وسایل نقلیه در کشورهایی که مقررات را اجرا می‌کنند، رعایت کنند. به ویژه، اتحادیه اروپا UN R155 را به عنوان بخشی از مقررات ایمنی عمومی (GSRY) اجرا کرده است که نقش مهم امنیت سایبری در ایمنی کلی را بیشتر تأیید می‌کند. رعایت R155 همچنین به عنوان بخشی از دیگر مقررات UNECE از جمله R157 (UNECE، ۲۰۲۱c) در مورد تایید نوع سیستم‌های حفظ خط خودکار (ALKS) لازم است که نیاز به در نظر گرفتن "حملات سایبری که بر ایمنی خودرو تأثیر می‌گذارند" را دارد.

در آگوست ۲۰۲۱، استاندارد بین‌المللی جدید ISO/SAE 21434 "خودروهای جاده‌ای - مهندسی امنیت سایبری" (ISO/SAE، ۲۰۲۱a) منتشر شد تا از اجرای عملی UN R155 پشتیبانی کند. این سند توسط کارشناسان صنعت خودرویی شامل تولیدکنندگان خودرو، زنجیره تامین طبقه‌بندی‌شده، مشاوران امنیت سایبری و سازمان‌های دولتی توسعه یافت. اکنون در صنعت خودرویی به عنوان وضعیت هنر برای مهندسی امنیت سایبری به طور گسترده‌ای استفاده می‌شود، که راهنمایی در مورد اجرای یک سیستم مدیریت امنیت سایبری و انجام فعالیت‌های امنیت سایبری مورد نیاز برای رعایت UN R155 ارائه می‌دهد. ISO/SAE 21434 به صراحت از سازمان‌ها می‌خواهد که دیگر رشته‌های مهندسی که با امنیت سایبری در تعامل هستند، مانند ایمنی عملکردی، را شناسایی کنند و کانال‌های ارتباطی بین آن رشته‌ها را ایجاد کنند. علاوه بر این، استاندارد بین‌المللی ISO 26262 برای ایمنی عملکردی (ISO، ۲۰۱۸) شامل یک الزام متقابل برای شناسایی تعاملات و ایجاد کانال‌های ارتباطی بین ایمنی عملکردی و امنیت سایبری است. رابطه قوی به ویژه بین امنیت سایبری و ایمنی عملکردی در نحوه اشتراک‌گذاری عناصر مشترک از چارچوب‌های فرآیندی که این دو استاندارد تعریف می‌کنند، دیده می‌شود، برای مثال مراحل چرخه حیات هماهنگ و رویکرد مدیریت ریسک.

در حوزه خودرویی، اولین منطقه‌ای که تعادل ایمنی / امنیت سایبری مشهود شد، حوزه CAN bus بود. این باس برای ارتباط بین واحدهای کنترل الکترونیکی (ECU) طراحی شده بود. این باس بدون در نظر گرفتن امنیت و با قابلیت اطمینان بسیار بالا تعریف شد. Kleberger و همکاران (۲۰۱۱) یک مرور کلی از تهدیدات امنیتی درون خودرو و حفاظت‌های بالقوه با توجه به شبکه CAN ارائه می‌دهند.

اصالت یک نیاز امنیتی مهم برای سیستم‌های خودرویی است و بسیاری از راه‌حل‌های نرم‌افزاری یا سخت‌افزاری احراز هویت در Kleberger و همکاران (۲۰۱۱) بررسی شده‌اند. از این راه‌حل‌ها، کد احراز هویت پیام (MAC) تکنیک اصلی است. پهنای باند محدود و اندازه بار مفید پروتکل CAN به این معناست که این تکنیک‌ها باید سبک‌وزن باشند تا نیازهای دیگر طراحی را برآورده کنند. از آنجایی که CAN در درجه اول یک پروتکل طراحی شده برای ایمنی است، این را می‌توان به عنوان یک گام اولیه در تعادل بین نیازهای ایمنی و امنیت در نظر گرفت.

Lin و Yu (۲۰۱۶) مرور خوبی از تعادل‌های ایمنی و امنیت با بررسی TTEthernet (اترنت زمان‌مند) ارائه می‌دهند. این به عنوان یکی از رقبای جایگزین برای CAN bus دیده می‌شود، اگرچه نویسندگان از TTEthernet به عنوان یک رسانه ارتباطی بین خودروها، نه داخل آن‌ها، استفاده می‌کنند. آن‌ها به سه کاربرد نگاه می‌کنند: مدیریت کلید مخفی، تکرار و حذف فریم، و تقسیم‌بندی شبکه محلی مجازی (VLAN).

Li و Apvrille (۲۰۱۹) بر این اساس کار می‌کنند که یک فرد (یا یک تیم) مسئول طراحی اولیه سیستم است و بنابراین هماهنگ کردن نیازهای ایمنی، امنیت و عملکرد نسبتاً ساده است. TTool (Apvrille، ۲۰۰۸) (ابزار انتخابی آن‌ها) کل فرآیند مدل‌سازی و تایید را در یک جعبه ابزار واحد نگه می‌دارد که به طور همزمان برای نیازهای ایمنی، امنیت و عملکرد انجام می‌شود. Li و Apvrille (۲۰۱۹) اشاره می‌کنند که صحت تبدیل مدل برای ProVerif تا حدی ثابت شده است. آن‌ها همچنین اکتشاف فضای طراحی را در کار خود ارائه می‌دهند. اما با نگاه جداگانه به امنیت، ایمنی و عملکرد، به نظر می‌رسد که آن‌ها فرصت بهره‌برداری از وابستگی‌های متقابل بین این موارد را از دست می‌دهند. آن‌ها پیشنهاد می‌دهند که یکی از امنیت، ایمنی یا عملکرد به عنوان نیاز اصلی ابزار در نظر گرفته شود و راه‌هایی برای رسیدگی به عناصر غیرمطلوب از دو مورد دیگر ارائه کنند. این نشان می‌دهد که مقاله (اگرچه در مطالعه موردی از خودروها استفاده می‌کند) در حال حاضر در واقع بر بخش‌های کوچکتر CPS متمرکز است. کار ما در حال حاضر به شدت بر خودروها متمرکز است و ما به پرسش مقایسه روابط متقابل ایمنی و امنیت از دیدگاه آن‌ها می‌پردازیم.

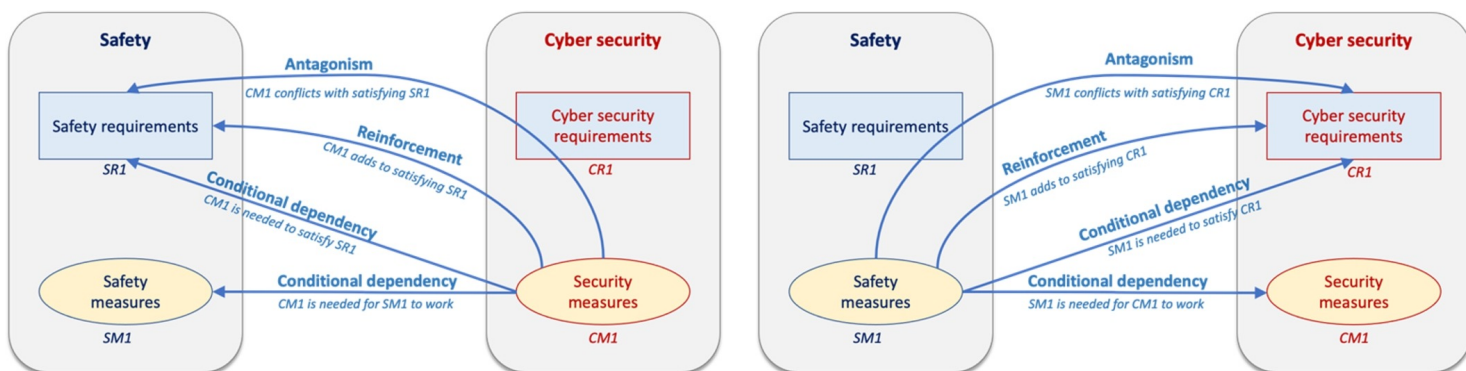
با نگاهی گسترده‌تر به فناوری‌های ارتباطی، در Huber و همکاران (۲۰۱۸) نویسندگان بررسی می‌کنند که چگونه سازمان‌های صنعت خودروسازی با چالش ادغام جنبه‌های ایمنی و امنیت در طول توسعه سیستم مقابله می‌کنند. نتیجه‌گیری کلی آن‌ها این است که در حال حاضر "کمبودهای قابل توجهی در ادغام هر دو حوزه وجود دارد." نویسندگان یک بررسی اکتشافی (محدود به اروپا) از ادغام جنبه‌های ایمنی و امنیت در طول توسعه سیستم در صنعت خودروسازی ارائه می‌دهند. چهار یافته کلیدی (KF) از این مطالعه به دست آمده است:

- اکثریت سازمان‌های (خودروسازی) به طور فعال وابستگی‌های متقابل بین نیازهای ایمنی و امنیت را در نظر نمی‌گیرند.

- مشکلات رایج مربوط به پیچیدگی، مدیریت تغییر ردیابی و در دسترس بودن منابع، ادغام امنیت را پیچیده می‌کنند.
 - اهداف هر دو حوزه امنیت و ایمنی در چندین سازمان گسترده می‌شوند.
 - درک نسبتاً یکنواخت و آگاهی عمومی در سازمان‌ها در مورد تفاوت‌های اساسی بین حوزه‌های ایمنی و امنیت وجود دارد.
- نتیجه‌گیری از این یافته‌های کلیدی نیاز به یک مدل جامع است که اسناد و مدارک را یکپارچه کند تا پیچیدگی را کاهش داده و مدیریت تغییرات موثر را تسهیل کند.
- چهار نوع تعامل بین ایمنی و امنیت توسط Piètre-Cambacédès (۲۰۱۰) (به زبان فرانسوی) معرفی شده و سپس توسط Kriaa و همکاران (۲۰۱۵) منتشر شده است. این تعاملات شامل موارد زیر هستند:
- وابستگی شرطی: برآورده شدن نیازهای ایمنی یک شرط برای امنیت است یا برعکس.
 - تقویت متقابل: نیازها یا اقدامات ایمنی امنیت را افزایش می‌دهند یا برعکس.
 - تقابل: نیازها یا اقدامات ایمنی و امنیتی با یکدیگر در تضاد هستند.
 - استقلال: هیچ تعاملی وجود ندارد.
- Kolb و همکاران (۲۰۲۱) استدلال می‌کنند که تعاریف دقیق‌تری از ایمنی و امنیت سایبری لازم است، که شامل موارد زیر باشد:
- جهت‌گیری: آیا ایمنی و امنیت یک‌طرفه هستند یا دوطرفه و از کدام جهت جریان دارند؟
 - شدت: برای یک هم‌تحلیل کمی، شدت این تعاملات باید در نظر گرفته شود.
 - ماهیت تعامل: برای هر یک از تعاملات ممکن، از تأثیر تا وابستگی یا تقابل، در نظر گرفتن تأثیر مثبت یا منفی چنین تعاملی اساسی است. علاوه بر این، وابستگی‌های شرطی سوالی را در مورد اینکه چه کسی مسئول اقدامات است هنگامی که ایمنی و امنیت به شدت وابسته هستند، مطرح می‌کند.
- Kolb و همکاران (۲۰۲۱) تحلیل مقایسه‌ای از ۱۴ روش برای هم‌تحلیل مدل‌محور ایمنی و امنیت انجام دادند. یافته‌ها/چالش‌های کلیدی شامل موارد زیر است:
- بیشتر روش‌ها درخت‌های حمله و درخت‌های خطا را ترکیب می‌کنند.
 - هیچ ساختار جدیدی برای ثبت تعاملات ایمنی-امنیت معرفی نشده است. در عوض، ساختارهای موجود برای مدل‌سازی ایمنی و امنیت با هم ترکیب شده‌اند.
 - تعاملات ایمنی و امنیت هنوز به طور کامل درک نشده‌اند.
 - هیچ معیار جدیدی برای کمی کردن تعاملات ایمنی-امنیت پیشنهاد نشده است.
 - هیچ مطالعه موردی بزرگ در مورد هم‌تحلیل ایمنی/امنیت انجام نشده است.
- هدف کلی تحقیقات ما ادامه رسیدگی به این چالش‌ها است.

۲ امنیت و وابستگی متقابل امنیت سایبری

شکل ۱ و شکل ۲ وابستگی‌های متقابل بین اقدامات و نیازهای ایمنی و امنیت سایبری را نشان می‌دهند. شکل ۱ تأثیر اقدامات ایمنی بر امنیت سایبری را نشان می‌دهد، در حالی که شکل ۲ تأثیر اقدامات امنیت سایبری بر ایمنی را نمایش می‌دهد. سه نوع رابطه که در Piètre-Cambacédès (۲۰۱۰) و Kriaa و همکاران (۲۰۱۵) تعریف شده‌اند، در شکل ۱ و شکل ۲ به تصویر کشیده شده‌اند: تقابل، تقویت، و وابستگی شرطی.



شکل ۲: تاثیر اقدامات امنیت سایبری بر ایمنی

شکل ۱: تاثیر اقدامات ایمنی بر امنیت سایبری

| Relationship type | I. Interactions between safety requirements or measures and security requirements or measures | | | II. Interactions between safety failures and security attacks | |
|-------------------|--|---|---|---|--|
| | (a) <u>Conditional dependency</u> fulfilment of safety requirements is a condition for security, or vice versa | (b) <u>Reinforcement</u> safety requirements or measures increase security, or vice-versa | (c) <u>Antagonism</u> safety and security requirements or measures conflict with each other | (d) <u>Enabling</u> safety failure enables security attack, or vice versa | (e) <u>Blocking</u> safety failure blocks security attack, or vice versa |
| Factors | | | | | |
| Direction | Safety -> Security Security -> Safety | Safety -> Security Security -> Safety | Safety -> Security Security -> Safety | Safety -> Security Security -> Safety | Safety -> Security Security -> Safety |
| Intensity | If requirement is not fulfilled, how strong is the effect? | How big is the increase? | How strong is the conflict? | What is the probability? | What is the probability? |
| Methods/ Models | Interdependency identification; Trade-off analysis | Interdependency identification; Trade-off analysis | Interdependency identification; Trade-off analysis | Interdependency identification; Trade-off analysis | Interdependency identification; Trade-off analysis |

شکل ۳: امنیت و وابستگی متقابل امنیتی

علاوه بر وابستگی‌های متقابل بین نیازها و اقدامات ایمنی و امنیت سایبری، ممکن است وابستگی‌هایی بین سطوح خرابی و حمله نیز وجود داشته باشد. به عنوان مثال، یک خرابی ایمنی می‌تواند به فعال‌سازی یک حمله امنیتی کمک کند، یا برعکس. علاوه بر این، یک خرابی ایمنی می‌تواند یک حمله امنیتی را مسدود کند، یا برعکس. بنابراین، دو نوع رابطه جدید می‌توان تعریف کرد: "فعال‌سازی" و "مسدودسازی". ما طبقه‌بندی اولیه وابستگی‌های متقابل ایمنی و امنیت، که توسط Kolb و همکاران (۲۰۲۱) پیشنهاد شده بود، را گسترش داده و روابط "فعال‌سازی" و "مسدودسازی" را اضافه کرده‌ایم، همان‌طور که در شکل ۳ نشان داده شده است.

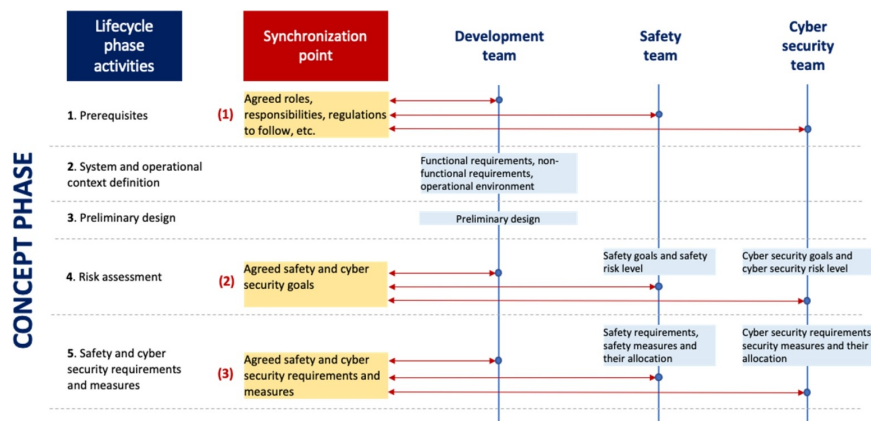
علاوه بر انواع روابط، شکل ۳ شامل عوامل مختلفی است که برای تمامی انواع روابط مرتبط هستند، مانند:

• جهت - دو جهت وجود دارد، یا از ایمنی به امنیت (تأثیر ایمنی بر امنیت) یا برعکس

• شدت - اندازه‌گیری شدت وابستگی متقابل.

• روش‌ها/مدل‌ها - روش‌ها و مدل‌های مختلف برای تسهیل تحلیل وابستگی‌های متقابل

هدف کار ما ارائه روشی است که به بررسی رابطه بین ایمنی و امنیت سایبری در هر مرحله از چرخه حیات سیستم سایبر فیزیکی (CPS) بپردازد و تعامل بین آن‌ها را برجسته کند.



شکل ۴: فعالیت های فاز مفهومی و نقاط هماهنگ سازی بین تیم های توسعه، ایمنی و امنیت سایبری.

۳ مروری بر روش‌شناسی

شکل ۵ چارچوب روش‌شناسی TOMSAC را نشان می‌دهد که شامل موارد زیر است:

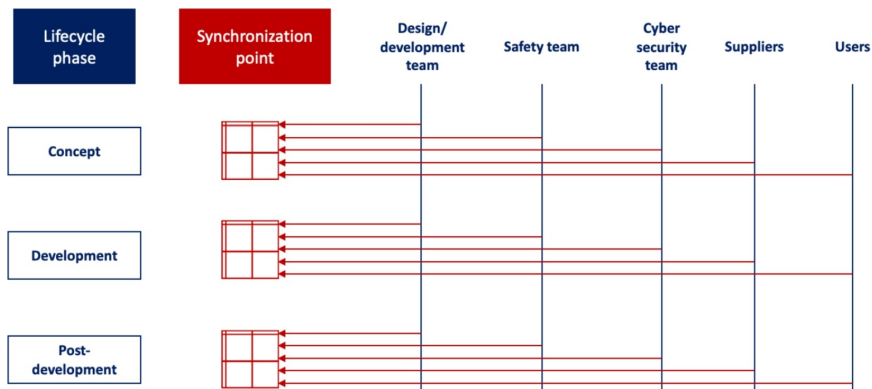
- مراحل چرخه حیات CPS
- تیم‌های درگیر در فرآیند توسعه، مانند تیم‌های طراحی/توسعه، ایمنی و امنیت سایبری، تأمین‌کنندگان و کاربران؛
- نقاط هماهنگی در مراحل مختلف چرخه حیات برای تیم‌ها به منظور هماهنگ کردن محصولات کاری خود و انجام مبادلات، در صورت لزوم.
- تیم‌های متعددی در توسعه CPS درگیر هستند، مانند توسعه‌دهندگان، تیم ایمنی، تیم امنیت سایبری و غیره، که هر کدام استانداردهای خود را دنبال می‌کنند، فرآیندهای مختلفی دارند، محصولات کاری مختلفی توسعه می‌دهند و حتی به زبان‌های مختلفی صحبت می‌کنند یا از اصطلاحات مشابه برای معانی مختلف استفاده می‌کنند، که این امر باعث می‌شود درک کامل یکدیگر و یکپارچه‌سازی نتایج کارشان دشوار باشد. هدف روش‌شناسی TOMSAC فراهم کردن یک چارچوب یکپارچه برای این تیم‌ها است تا ارتباط و هماهنگی کارهایشان را تسهیل کند.

۴ روش‌شناسی TOMSAC برای حوزه خودرو

بخش خودرو، به‌ویژه وسایل نقلیه جاده‌ای خودکار، حوزه اصلی تخصص ما است. بنابراین، ابتدا روش‌شناسی TOMSAC را برای این بخش سفارشی می‌کنیم. مراحل چرخه حیات بر این اساس به فعالیت‌های ISO ۲۶۲۶۲ (ISO، ۲۰۱۸) و ISO/SAE ۲۱۴۳۴ (ISO/SAE، ۲۰۲۱a) تنظیم می‌شوند. ISO ۲۶۲۶۲ استاندارد ایمنی عملکردی وسایل نقلیه جاده‌ای و ISO/SAE ۲۱۴۳۴ استاندارد امنیت سایبری است. هر دو استاندارد ISO ۲۶۲۶۲ و ISO/SAE ۲۱۴۳۴ نیاز به شناسایی رشته‌های مرتبط و ایجاد و نگهداری کانال‌های ارتباطی بین آن‌ها را دارند. ISO ۲۶۲۶۲ به‌طور صریح به امنیت سایبری اشاره می‌کند و به‌طور مشابه، ISO/SAE ۲۱۴۳۴ ایمنی عملکردی را به‌عنوان رشته‌های مرتبط شناسایی می‌کند. زیر بخش‌های زیر به توصیف کاربرد روش‌شناسی TOMSAC در مراحل توسعه مفهوم و محصول خودرو می‌پردازند.

۱.۴ مدیریت مبادلات در مرحله مفهوم

شکل ۴ یک نمای کلی از روش‌شناسی TOMSAC را که در مرحله توسعه مفهوم خودرو به کار گرفته شده است، شامل می‌شود. در این مرحله، تولیدکنندگان تجهیزات اصلی خودرو (OEM ها) یا تیم‌های درگیر، مسئولیت‌ها را به اشتراک می‌گذارند و یک مدل مفهومی سیستم توسعه می‌دهند. به عنوان بخشی از مدل مفهومی سیستم، آن‌ها ارزیابی اولیه ریسک را انجام می‌دهند و با توافق بر روی نیازها و اقدامات ایمنی و امنیت سایبری مرتبط به پایان می‌رسانند. همان‌طور که در شکل ۴ می‌بینیم، سه تیم در این مرحله درگیر هستند: توسعه، ایمنی و امنیت سایبری. ما در این مرحله سه نقطه هم‌زمانی پیشنهاد می‌کنیم تا تیم‌ها محصولات کاری خود را هماهنگ کنند و هرگونه مبادله لازم را انجام دهند.



شکل ۵: مراحل چرخه حیات، CPS، تیم‌های درگیر و نقاط همگام‌سازی/معادل.

| Goals | Risk level | Risk treatment | System assets | | |
|-----------------------------|------------|----------------|---------------|-----|----|
| | | | A1 | ... | An |
| Safety goals | | | | | |
| SG1 | | | | GA1 | O |
| ... | | | O | | |
| SGn | | | | | |
| Cyber security goals | | | | | |
| CG1 | | | O | GA2 | |
| ... | | | | | O |
| CGn | | | | | |

شکل ۶: فعالیت های فاز مفهومی و نقاط هماهنگ سازی بین تیم های توسعه، ایمنی و امنیت سایبری.

۱.۱.۴ نقطه هم‌زمانی (۱): توافق بر نقش‌ها، مسئولیت‌ها و مقررات

در این نقطه، باید یک جلسه بین همه تیم‌ها برگزار شود تا در مورد نحوه هماهنگی کارهایشان توافق کنند. توافق می‌تواند شامل تعریف نقش‌ها، مسئولیت‌ها، مقرراتی که آن‌ها دنبال می‌کنند، برنامه‌ها و غیره باشد.

۲.۱.۴ نقطه هم‌زمانی (۲): توافق بر اهداف ایمنی و امنیت سایبری

مفید است که در پایان ارزیابی ریسک یک نقطه هم‌زمانی داشته باشیم، زمانی که اهداف ایمنی و امنیت سایبری (نیازهای سطح بالا) تعریف می‌شوند و سطح ریسک مربوط به آن‌ها تعیین می‌شود. اهداف این نقطه هم‌زمانی دوگانه است:

۱. بررسی اینکه آیا همه دارایی‌های مهم سیستم (از دیدگاه توسعه‌دهندگان) محافظت می‌شوند - یعنی اطمینان حاصل کنیم که تیم‌های ایمنی و امنیت سایبری چیزی را از قلم نینداخته‌اند؛ و

۲. انجام یک تحلیل اولیه وابستگی متقابل بین ایمنی و امنیت با تحلیل روابط بین اهداف ایمنی و امنیت سایبری.

برای دستیابی به هدف اول، می‌توانیم از ماتریس‌های رابطه برای نقشه‌برداری اهداف ایمنی و امنیت سایبری به دارایی‌های سیستم استفاده کنیم، همان‌طور که در شکل ۶ نشان داده شده است. در شکل ۶، "O" نشان‌دهنده این است که هدف (ردیف) به حفاظت از دارایی (ستون) کمک می‌کند.

هر سه تیم باید بر اهداف ایمنی و امنیت سایبری، سطوح ریسک و گزینه‌های مدیریت ریسک (کاهش یا اجتناب، اشتراک‌گذاری، حفظ) برای هر دارایی، مطابق با استانداردهای ISO 26262 و ISO/SAE 21434 توافق کنند.

برای دستیابی به هدف دوم، می‌توانیم از ماتریس‌های رابطه GA1 و GG2 که به ترتیب در شکل ۷ و شکل ۸ نشان داده شده‌اند، استفاده کنیم. GG1 به تحلیل تأثیر اهداف امنیت سایبری بر اهداف ایمنی کمک می‌کند، در حالی که GG2 بر تأثیر اهداف ایمنی بر اهداف امنیت سایبری متمرکز است.

در شکل ۷، "O" نشان می‌دهد که هدف امنیت سایبری (ستون) به تحقق هدف ایمنی (ردیف) کمک می‌کند، در حالی که "X" به این معنی است که هدف امنیت سایبری (ستون) با هدف ایمنی (ردیف) در تضاد است.

| Goals (high-level requirements) | Cyber security goals | | | Safety risk level | Risk treatment |
|------------------------------------|----------------------|-----|-----|----------------------|-------------------|
| | CG1 | ... | CGn | | |
| Safety goals | O | | | | |
| SG1 | | GG1 | X | | |
| ... | X | | | | |
| SGn | | O | | | |
| Cyber security risk level | | | | | |
| Risk treatment | | | | | |

شکل ۷: ماتریس رابطه GG1 برای تحلیل تضاد اهداف امنیت سایبری با اهداف ایمنی.

| Goals (high-level requirements) | Safety goals | | | Cyber security risk level | Risk treatment |
|------------------------------------|--------------|-----|-----|---------------------------------|-------------------|
| | SG1 | ... | SGn | | |
| Cyber security goals | | | | | |
| CG1 | | GG2 | X | | |
| ... | X | | O | | |
| CGn | | O | | | |
| Safety risk level | | | | | |
| Risk treatment | | | | | |

شکل ۸: ماتریس رابطه GG2 برای تحلیل تضاد اهداف ایمنی با اهداف امنیت سایبری.

در همین حال، در شکل ۸، "O" نشان می‌دهد که هدف ایمنی (ستون) به تحقق هدف امنیت سایبری (ردیف) کمک می‌کند، در حالی که "X" به این معنی است که هدف ایمنی (ستون) با هدف امنیت سایبری (ردیف) در تضاد است. ماتریس‌های GG1 و GG2 همچنین برای توافق بر گزینه‌های مدیریت ریسک برای اهداف ایمنی و امنیت سایبری وابسته به یکدیگر مفید هستند.

۳.۱.۴ نقطه هم‌زمانی (۳): توافق بر نیازها و اقدامات ایمنی و امنیت سایبری

پس از نهایی شدن اهداف ایمنی و امنیت سایبری، نیازهایی با گزینه‌های مدیریت ریسک «کاهش» به نیازهای دقیق‌تری تبدیل می‌شوند – استراتژی‌های مستقل از طراحی برای دستیابی به اهداف. نیازهای ایمنی و امنیت سایبری همچنین به اقدامات ایمنی و امنیتی اختصاص داده می‌شوند که سپس به سیستم‌های وسیله نقلیه یا محیط آن تخصیص می‌یابند. در این مرحله، زمانی که اقدامات ایمنی و امنیتی توسط تیم‌های مربوطه تعیین شده‌اند، می‌توانیم شروع به تحلیل وابستگی‌های متقابل احتمالی بین آن‌ها کنیم.

برای شناسایی و حل تعارضات احتمالی بین اقدامات، می‌توانیم از چارچوب ارزیابی ریسک سایبری (CRAF) (Asplund و همکاران، ۲۰۱۹) استفاده کنیم. روش CRAF شامل موارد زیر است:

- یک نقشه از پیش تعریف‌شده بین ویژگی‌های امنیت داده و ایمنی (شکل ۹ را ببینید)؛

- مجموعه‌ای از جداول، که توسط هر دو تیم ایمنی و امنیتی تکمیل شده‌اند (شکل ۱۰، شکل ۱۱، شکل ۱۲ را ببینید).

شکل ۱۰ می‌تواند توسط تیم ایمنی برای تحلیل اینکه آیا نیازها و اقدامات امنیت سایبری با ایمنی در تضاد نیستند، استفاده شود، در حالی که شکل ۱۱ برای بررسی اینکه آیا نیازها و اقدامات ایمنی با امنیت سایبری در تضاد نیستند، استفاده می‌شود. اگر تعارضات احتمالی در شکل ۱۰ و شکل ۱۱ شناسایی شوند، هر دو تیم باید سعی کنند تعارضات را با بررسی راه‌حل‌های جایگزین حل کنند. برای ارزیابی راه‌حل‌های جایگزین، می‌توان از شکل ۱۲ استفاده کرد.

| Data security property | Data safety property |
|------------------------------|---|
| Confidentiality | Accessibility, disposability/ delectability, intended destination/ usage, suppression, traceability |
| Integrity | Accuracy, completeness, consistency, fidelity/ representation, format, history, integrity, resolution, sequencing |
| Availability | Accessibility, availability, lifetime, priority, sequencing, timeliness |
| Non-repudiation | History, integrity, traceability, verifiability |
| Authorisation/authentication | Accessibility, disposability/ delectability, integrity, intended destination/ usage, lifetime, suppression |

شکل ۹: نقشه‌برداری بین ایمنی داده‌ها و ویژگی‌های امنیتی.

| Cyber security requirement | Security measure | Data security property | Data safety Property | Conflict? | Conflict resolution | Selected alternative |
|---------------------------------|------------------|------------------------|--------------------------|-----------|-------------------------|----------------------|
| CR1 | CM1 | | | X | Alternatives 1...n | |
| CR2 | CM2 | | | | | |
| Competed by cyber security team | | | Completed by safety team | | Completed by both teams | |

شکل ۱۰: جدول CRAF برای تجزیه و تحلیل تضاد بین اقدامات امنیتی و ایمنی.

| Safety requirement | Safety measure | Data safety property | Data security property | Conflict? | Conflict resolution | Selected alternative |
|-------------------------|----------------|----------------------|----------------------------------|-----------|-------------------------|----------------------|
| SR1 | SM1 | | | X | Alternatives 1...n | |
| SR2 | SM2 | | | | | |
| Competed by safety team | | | Completed by cyber security team | | Completed by both teams | |

شکل ۱۱: جدول CRAF برای تجزیه و تحلیل تضاد بین اقدامات ایمنی و امنیت.

شکل ۱۲ انواع روابط ایمنی و امنیت سایبری را نشان می‌دهد که می‌توان با استفاده از روش CRAF تحلیل کرد. همان‌طور که در شکل ۱۶ می‌بینیم، کار ما رابطه تعارض را در نظر می‌گیرد و مدل‌هایی برای تحلیل وابستگی متقابل و مدیریت مبادلات (ارزیابی راه‌حل‌های جایگزین) شامل می‌شود. گزینه‌ها در کلید به عنوان ورودی‌های ممکن در ماتریس‌های ۴-MR۱ در شکل ۱۴ شامل رضایت، کمک به رضایت و تعارض هستند. این‌ها در شکل ۱۶ ثبت شده‌اند.

علاوه بر روش CRAF، می‌توانیم از ماتریس‌های رابطه برای کمک به تحلیل انواع دیگر روابط، یعنی وابستگی شرطی و تقویت، استفاده کنیم. شکل ۱۴، یک ماتریس رابطه را نشان می‌دهد که چهار ماتریس کوچکتر، MR۴-MR۱، را برای تحلیل روابط بین نیازها و اقدامات ایمنی/امنیت سایبری یکپارچه می‌کند.

مراحل تکمیل ماتریس‌های MR۴-MR۱ به شرح زیر است:

۱. تیم ایمنی ماتریس MR۱ را پر می‌کند.

۲. تیم امنیت سایبری ماتریس MR۲ را تکمیل می‌کند.

۳. تیم امنیت سایبری فهرست اقدامات امنیتی خود را با تیم ایمنی به اشتراک می‌گذارد و تیم ایمنی ماتریس MR۳ را تکمیل می‌کند؛

۴. تیم ایمنی فهرست اقدامات ایمنی را با تیم امنیت سایبری به اشتراک می‌گذارد و تیم امنیت سایبری ماتریس MR۴ را تکمیل می‌کند؛

۵. تیم‌های ایمنی و امنیت سایبری جلسه‌ای برگزار می‌کنند و نتایج ماتریس‌های MR۳ و MR۴ را برای رسیدن به توافق نهایی در مورد انتخاب اقدامات ایمنی و امنیتی مورد بحث قرار می‌دهند. در صورت بروز تعارض، شکل ۱۲ می‌تواند برای ارزیابی اقدامات جایگزین استفاده شود.

اگر داده‌های کمی از اثربخشی اقدامات ایمنی/امنیت سایبری در تحقق نیازها موجود باشد، می‌توان از این داده‌ها در شکل ۱۳ (در سراسر ماتریس‌های ۴-MR۱) استفاده کرد تا نماد "O" که تنها نشان می‌دهد که اقدام به تحقق نیاز کمک می‌کند، اما مشخص نمی‌کند که این اقدام چقدر مؤثر است، جایگزین شود. بنابراین، این ماتریس‌ها می‌توانند برای ثبت اطلاعات "شدت" نیز استفاده شوند.

شکل ۱۶ انواع روابط ایمنی و امنیت سایبری مورد نظر در ماتریس‌های پیشنهادی تاکنون را خلاصه می‌کند.

پس از نهایی شدن انتخاب اقدامات ایمنی و امنیت سایبری توسط تیم‌های ایمنی و امنیت سایبری، آن‌ها باید با تیم توسعه در مورد تخصیص این اقدامات به سیستم‌های سطح وسیله نقلیه که آیتم (عملکرد سطح وسیله نقلیه) را اجرا می‌کنند یا به محیط توافق کنند. برای تسهیل این فرآیند، می‌توان از ماتریس‌های رابطه، ME۲-ME۱ که اقدامات را به سیستم‌های وسیله نقلیه یا محیط نگاشت می‌کنند، استفاده کرد، همان‌طور که در شکل ۱۷ نشان داده شده است.

| Alternative | Security probability | Security impact | Safety probability | Safety impact |
|---------------------------------|----------------------|-----------------|--------------------------|---------------|
| 1 | | | | |
| n | | | | |
| Competed by cyber security team | | | Completed by safety team | |

شکل ۱۲: ارزیابی جایگزین‌های CRAF

| Relationship type Factors | I. Between safety requirements or measures and security requirements or measures | | |
|------------------------------|--|-------------------|---|
| | (a) Conditional dependency | (b) Reinforcement | (c) Antagonism |
| Direction | | | Safety -> Security Security -> Safety |
| Intensity | | | |
| Methods/ Models | | | <ul style="list-style-type: none"> Interdependencies Trade-off analysis |

شکل ۱۳: روابطی که با روش CRAF پرداخته شده است.

| Requirements | Initial risk level | Safety measures | | | Security measures | | | Residual risk level |
|------------------------------------|--------------------|-----------------|-----|-----|-------------------|-----|-----|---------------------|
| | | SM1 | ... | SMn | CM1 | ... | CMn | |
| Safety requirements | | | | | | | | |
| SR1 | | | MR1 | O | O | MR3 | C | |
| ... | | O | | | | | | |
| SRn | | | X | | | X | | |
| Cyber security requirements | | | | | | | | |
| CR1 | | O | MR4 | | O | MR2 | | |
| ... | | | | X | | | O | |
| CRn | | C | | | | X | | |

شکل ۱۴: ماتریس‌های رابطه MR1-MR4 برای وابستگی‌های متقابل بین اقدامات و نیازها.

O - اقدام (ستون) به تحقق نیاز (ردیف) کمک می‌کند؛

C - داشتن اقدام (ستون) شرطی برای تحقق نیاز است؛

X - اقدام (ستون) ممکن است نیاز (ردیف) را نقض کند.

این ماتریس‌ها به ویژه برای یکپارچه‌سازی نتایج تحلیل تهدیدات چندین آیتم مفید هستند، زیرا هر آیتم به طور مستقل تحلیل می‌شود، بنابراین نیازهای ایمنی و امنیت سایبری به طور مستقل مشخص و اقدامات انتخاب می‌شوند.

۴.۱.۴ خلاصه‌ای از ماتریس‌های استفاده شده در مرحله مفهومی

شکل ۱۵ و شکل ۱۸ خلاصه‌ای از ماتریس‌های استفاده شده در مرحله مفهومی را ارائه می‌دهند. در مجموع ۱۰ ماتریس وجود دارد: چهار ماتریس در سطح هدف و شش ماتریس در سطح نیازمندی‌ها ساخته شده‌اند.

۲.۴ مدیریت مبادلات در مرحله توسعه محصول

در مرحله توسعه محصول، ما چهار نقطه همگام‌سازی داریم، همان‌طور که در شکل ۱۹ نشان داده شده است.

۱.۲.۴ نقطه همگام‌سازی (۴): توافق بر روی نیازمندی‌های سطح سیستم، مکانیزم‌های ایمنی و کنترل‌های امنیتی، و تخصیص آن‌ها

پس از توسعه یک طراحی سیستم دقیق توسط تیم توسعه، تیم‌های ایمنی و امنیت سایبری می‌توانند نیازمندی‌های ایمنی و امنیت سایبری سطح مفهومی را به نیازمندی‌های دقیق‌تر سطح سیستم تبدیل کنند. علاوه بر این، اقدامات ایمنی و امنیتی سطح مفهومی به مکانیزم‌های فنی ایمنی و کنترل‌های امنیتی تبدیل می‌شوند که به عناصر مربوطه سیستم اختصاص داده می‌شوند. در این مرحله می‌توان از چندین ماتریس رابطه برای کمک به تیم‌ها در شناسایی وابستگی‌های متقابل و انجام مبادلات در صورت نیاز استفاده کرد.

ابتدا، ماتریس‌های MR5-MR8 می‌تواند ساخته شوند، همان‌طور که در شکل ۲۰ نشان داده شده است. این ماتریس‌ها نسخه‌های دقیق‌تر MR1-MR4 هستند که در مرحله مفهومی توسعه یافته‌اند.

مراحل زیر برای تکمیل ماتریس‌های MR5-MR8 است:

۱. تیم ایمنی ماتریس MR5 را تکمیل می‌کند.

| Matrices | Rows | Columns | Possible symbols and their meanings |
|----------|-----------------------------|----------------------|---|
| GA1 | Safety goals | System assets | O – goal (row) contributes to protecting the asset (column) |
| GA2 | Cyber security goals | System assets | O – goal (row) contributes to protecting the asset (column) |
| GG1 | Safety goals | Cyber security goals | O – cyber security goal (column) contributes to satisfying safety goal (row); X – cyber security goal (column) conflicts with safety goal (row) |
| GG2 | Cyber security goals | Safety goals | O – safety goal (column) contributes to satisfying security goal (row); X – safety goal (column) conflicts with cyber security goal (row) |
| MR1 | Safety requirements | Safety measures | O – measure (column) contributes to satisfying the requirement (row); X – measure (column) may violate the requirement (row) |
| MR2 | Cyber security requirements | Security measures | O – measure (column) contributes to satisfying the requirement (row); X – measure (column) may violate the requirement (row) |
| MR3 | Safety requirements | Security measures | O – measure (column) contributes to satisfying the requirement (row); C – having the measure (column) is a condition for satisfying the requirement; X – measure (column) may violate the requirement (row) |
| MR4 | Cyber security requirements | Safety measures | O – measure (column) contributes to satisfying the requirement (row); C – having the measure (column) is a condition for satisfying the requirement; X – measure (column) may violate the requirement (row) |
| ME1 | Safety measures | Systems/ environment | X – measure (row) is allocated to the system/environment (column) |
| ME2 | Security measures | Systems/ environment | X – measure (row) is allocated to the system/environment (column) |

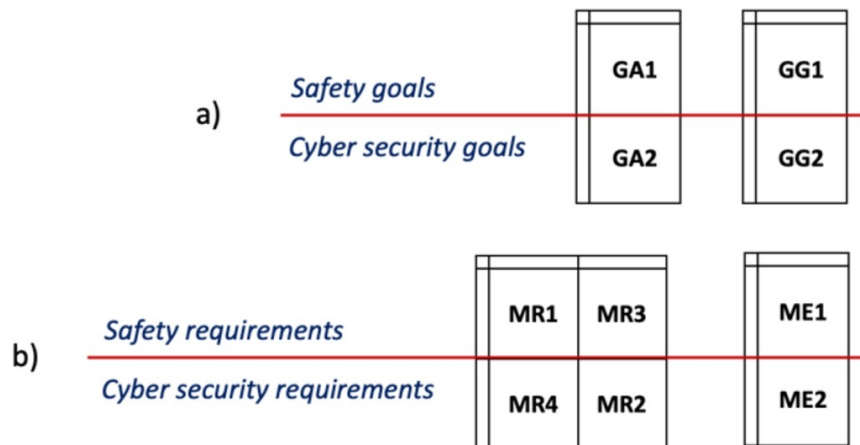
شکل ۱۵: شرح ۱۰ ماتریس مورد استفاده در فاز مفهومی.

| Relationship type Factors | I. Between safety requirements or measures and security requirements or measures | | |
|------------------------------|---|---|---|
| | (a) Conditional dependency | (b) Reinforcement | (c) Antagonism |
| Direction | Safety -> Security Security -> Safety | Safety -> Security Security -> Safety | Safety -> Security Security -> Safety |
| Intensity | | Measure effectiveness | |
| Methods/ Models | <ul style="list-style-type: none"> Interdependencies Trade-off analysis | <ul style="list-style-type: none"> Interdependencies Trade-off analysis | <ul style="list-style-type: none"> Interdependencies Trade-off analysis |

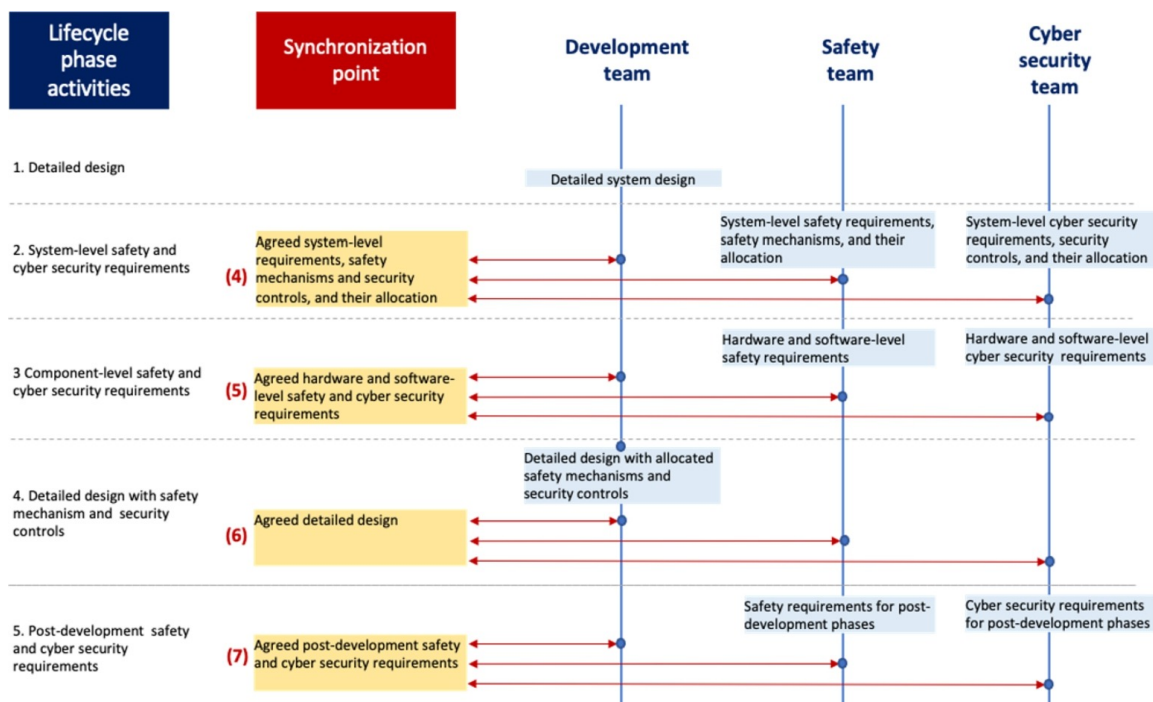
شکل ۱۶: روابط پرداخته شده توسط ماتریس های GG1-GG2 و MR1-MR4

| Mechanisms/controls | Allocation to system/environment | | |
|--------------------------|----------------------------------|-----|----|
| | E1 | ... | En |
| Safety measures | | | |
| SM1 | | ME1 | X |
| ... | X | | |
| SMn | | | |
| Security measures | | | |
| CM1 | X | ME2 | |
| ... | | | X |
| CMn | | | |

شکل ۱۷: ماتریس های رابطه ME1 و ME2 برای تخصیص اقدامات ایمنی و امنیتی به سیستم های خودرو/محیط
X - اندازه گیری (ردیف) به آیتم/محیط (ستون) اختصاص داده می شود



شکل ۱۸: خلاصه ماتریس فاز مفهومی در: الف) سطح هدف. ب) سطح نیاز.



شکل ۱۹: فعالیت های مرحله توسعه محصول و نقاط هماهنگ سازی بین تیم های توسعه، ایمنی و امنیت سایبری.

| Requirements | Initial risk level | Safety mechanisms | | | Security controls | | | Residual risk level |
|--|--------------------|-------------------|-----|-------|-------------------|-----|-------|---------------------|
| | | S-SM1 | ... | S-SMn | S-CM1 | ... | S-CMn | |
| System-level safety requirements | | C | | | | | | |
| S-SR1 | | | MR5 | O | O | MR7 | C | |
| ... | | O | | | | | | |
| S-SRn | | | X | | | X | | |
| System-level cyber security requirements | | | | | | | C | |
| S-CR1 | | O | MR8 | | O | MR6 | | |
| ... | | | | X | | | O | |
| S-CRn | | C | | | | X | | |

شکل ۲۰: ماتریس‌های رابطه‌ای MR۵-MR۸ برای تحلیل وابستگی‌های متقابل بین مکانیزم‌ها و نیازمندی‌ها.

O – مکانیزم/کنترل (ستون) به تحقق نیازمندی (ردیف) کمک می‌کند؛

C – داشتن مکانیزم/کنترل (ستون) شرط لازم برای تحقق نیازمندی است؛

X – مکانیزم/کنترل (ستون) ممکن است نیازمندی (ردیف) را نقض کند.

۲. تیم امنیت سایبری ماتریس MR۶ را تکمیل می‌کند.

۳. تیم امنیت سایبری فهرست کنترل‌های امنیتی خود را با تیم ایمنی به اشتراک می‌گذارد و تیم ایمنی ماتریس MR۷ را تکمیل می‌کند؛

۴. تیم ایمنی فهرست مکانیزم‌های ایمنی خود را با تیم امنیت سایبری به اشتراک می‌گذارد تا ماتریس MR۸ را تکمیل کنند؛

۵. تیم‌های ایمنی و امنیت سایبری دیدار می‌کنند و نتایج ماتریس‌های MR۵-MR۸ را برای رسیدن به توافق نهایی در مورد انتخاب اقدامات ایمنی و امنیتی بحث می‌کنند. در صورت وجود تضادها، تیم‌ها باید مبادلاتی انجام دهند تا تضادها را حذف کنند و در عین حال سطح ریسک باقی‌مانده قابل قبول را حفظ کنند.

پس از نهایی شدن انتخاب مکانیزم‌های ایمنی و کنترل‌های امنیتی توسط تیم‌های ایمنی و امنیت سایبری، باید با تیم توسعه درباره تخصیص اقدامات به عناصر سیستم به توافق برسند. برای تسهیل این فرآیند، ماتریس‌های رابطه‌ای ME۳-ME۴ که مکانیزم‌های ایمنی و کنترل‌های امنیتی را به عناصر سیستم نقشه‌برداری می‌کنند، در شکل ۲۱ نشان داده شده‌اند.

۲.۲.۴ نقطه هماهنگی (۵): توافق بر روی الزامات ایمنی و امنیت سایبری در سطح سخت‌افزار و نرم‌افزار

در این مرحله، الزامات امنیت سایبری در سطح سیستم به الزامات امنیت سایبری در سطح سخت‌افزار و نرم‌افزار تصحیح و مشخص می‌شوند. این نقطه هماهنگی به شناسایی وابستگی‌های ممکن بین الزامات ایمنی و امنیت سایبری برای اجزای سخت‌افزاری و نرم‌افزاری مشابه می‌پردازد. چهار ماتریس RE۱ تا RE۴ می‌توانند برای این منظور استفاده شوند، همانطور که در شکل ۲۲ نشان داده شده است. علاوه بر این، این ماتریس‌ها برای تعریف الزامات عملکردی اجزای نرم‌افزاری/سخت‌افزاری نیز مفید هستند.

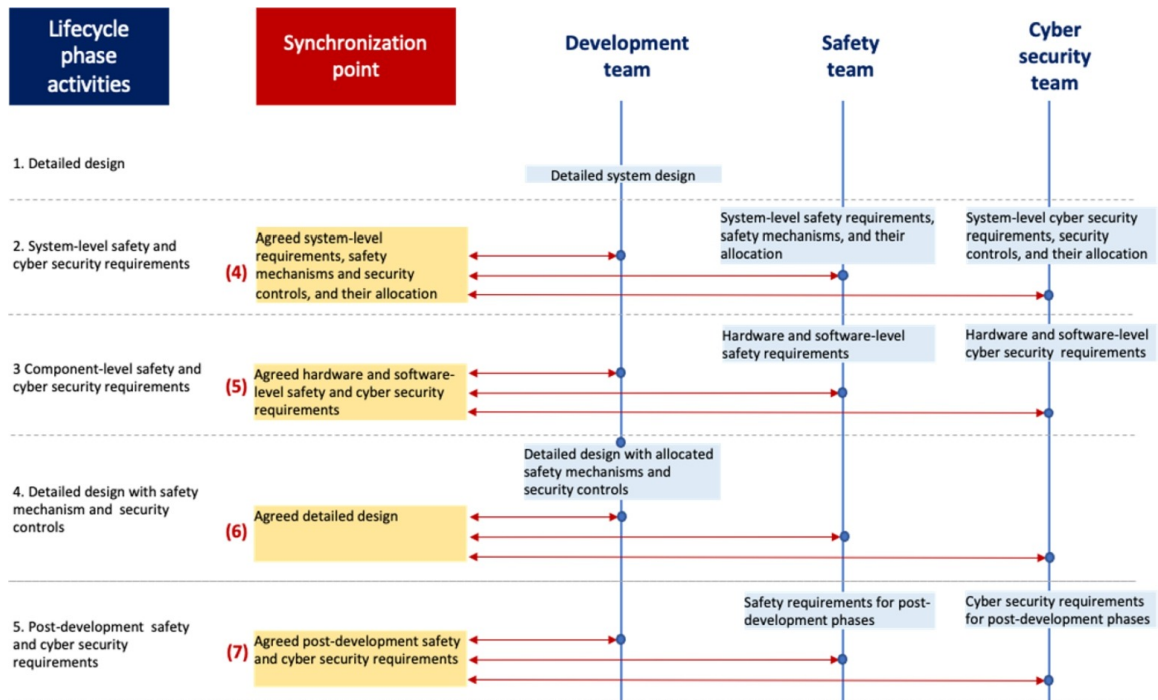
۳.۲.۴ نقطه هماهنگی (۶): توافق بر روی طراحی دقیق

در این مرحله، مکانیزم‌های ایمنی و کنترل‌های امنیت سایبری توسط تیم توسعه به طراحی دقیق سیستم اضافه می‌شوند، که سپس نیاز است توسط هر سه تیم بررسی شوند.

۴.۲.۴ نقطه هماهنگی (۷): توافق بر روی الزامات ایمنی و امنیت سایبری پس از توسعه

در پایان مرحله توسعه محصول، الزامات ایمنی و امنیت سایبری برای مرحله پس از توسعه باید تعریف شوند. این مراحل شامل تولید، عملیات و نگهداری، و از رده خارج کردن هستند. یک ماتریس رابطه‌ای می‌تواند برای هر مرحله استفاده شود، همانطور که در شکل ۲۳ نشان داده شده است. در مجموع، شش ماتریس تعریف شده‌اند، RA۱ تا RA۶.

الزامات اضافی برای فعالیت‌های فاز پس از توسعه، به منظور تسهیل پیاده‌سازی الزامات ایمنی و امنیت سایبری پس از توسعه، می‌توانند در انتهای شکل ۲۳ تعریف و اضافه شوند.



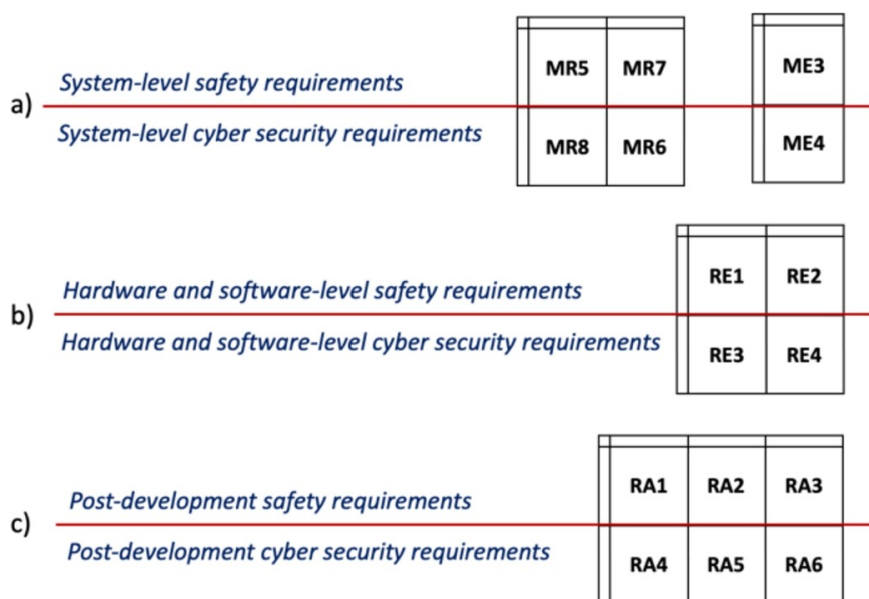
شکل ۲۱: ماتریس‌های رابطه ME^۳ و ME^۴ برای تخصیص مکانیسم‌های ایمنی و کنترل‌های امنیتی به عناصر سیستم. X – مکانیزم/کنترل (ردیف) به عنصر سیستم (ستون) اختصاص داده شده است.

| Goals | Hardware components | | | Software components | | |
|---|---------------------|-----|-------|---------------------|-----|-------|
| | HW-E1 | ... | HW-En | SW-E1 | ... | SW-En |
| Hardware-level safety requirements | | | | | | |
| HW-SR1 | | RE1 | X | | | |
| ... | X | | | | | |
| HW-SRn | | | | | | |
| Software-level safety requirements | | | | | | |
| SW-SR1 | | | | | RE2 | X |
| ... | | | | X | | |
| SW-SRn | | | | | | |
| Hardware-level cyber security requirements | | | | | | |
| HW-CR1 | X | RE3 | | | | |
| ... | | | X | | | |
| HW-CRn | | | | | | |
| Software-level cyber security requirements | | | | | | |
| SW-CR1 | | | | X | RE4 | |
| ... | | | | | | X |
| SW-CRn | | | | | | |
| Performance requirements | | | | | | |

شکل ۲۲: ماتریس‌های ارتباطی RE1-RE4 برای تخصیص الزامات سخت‌افزاری و نرم‌افزاری در سطح سخت‌افزار به قطعات سخت‌افزاری و نرم‌افزاری. X – نیاز (ردیف) به جز سخت‌افزاری یا نرم‌افزاری (ستون) اختصاص داده می‌شود.

| Goals | Production phase activities | | | Operation and maintenance phase activities | | | Decommissioning phase activities | | |
|---|-----------------------------|-----|-------|--|-----|-------|----------------------------------|-----|-------|
| | PR-A1 | ... | PR-An | OM-A1 | ... | OM-An | DC-A1 | ... | DC-An |
| Post-development safety requirements | | | | | | | | | |
| P-SR1 | | RA1 | X | | RA2 | X | | RA3 | X |
| ... | X | | | X | | | X | | |
| P-SRn | | | | | | | | | |
| Post-development cyber security requirements | | | | | | | | | |
| P-CR1 | | RA4 | X | X | RA5 | | | RA6 | X |
| ... | X | | | | | X | X | | |
| P-CRn | | | | | | | | | |
| Additional requirements | | | | | | | | | |

شکل ۲۳: ماتریس های رابطه RA1-RA۶ برای تخصیص الزامات ایمنی و امنیت سایبری به فعالیت های مرحله پس از توسعه. X - نیاز (ردیف) به یک فعالیت (ستون) اختصاص داده می شود.



شکل ۲۴: خلاصه ای از ماتریس های فاز توسعه محصول در:
الف) سطح نیاز در سطح سیستم. ب) سطح نیاز سخت افزار و نرم افزار؛ ج) سطح نیاز پس از توسعه.

۵.۲.۴ خلاصه ای از ماتریس های مورد استفاده در مرحله توسعه محصول

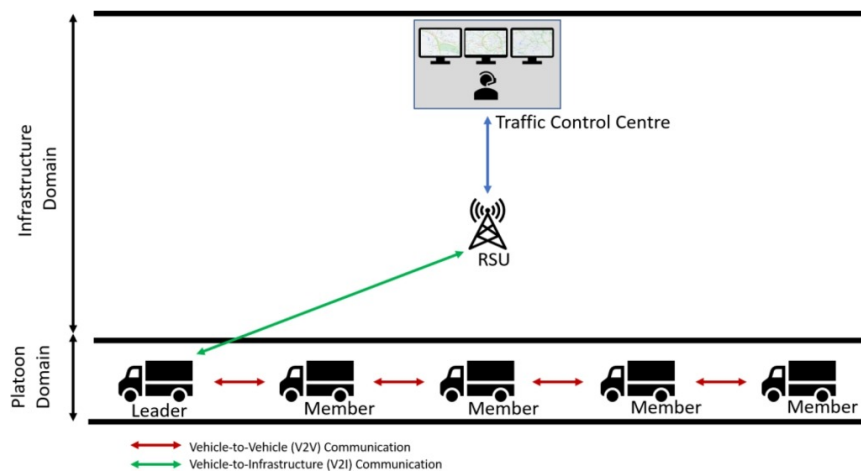
شکل ۲۳ و شکل ۲۴ شامل یک خلاصه از ماتریس های مورد استفاده در مرحله توسعه محصول هستند. در مجموع، شانزده ماتریس برای این فاز تعریف شده است: شش ماتریس برای تحلیل تعاملات در سطح الزامات سیستم؛ چهار ماتریس برای تحلیل در سطح الزامات سخت افزاری و نرم افزاری؛ و شش ماتریس برای تحلیل در سطح الزامات پس از توسعه.

۵ مطالعه موردی

مطالعه موردی انتخاب شده، یک پلوتون خودرویی است. پلوتونینگ یک برنامه کاربردی است که در آن گروهی از خودروها در فاصله نزدیک به طور پیوسته حرکت کرده و به صورت یک سیستم فیزیکی واحد عمل می کنند. اهداف پلوتونینگ بهبود ایمنی، کاهش مصرف سوخت و افزایش بهره وری از جاده ها است (Balador و همکاران، ۲۰۲۲).

پلوتونینگ به عنوان یک مورد کاربردی برای سیستم های سایبر-فیزیکی انتخاب شده است زیرا به طور مستقیم به ایمنی و امنیت سایبری مربوط می شود و تصمیمات اتخاذ شده درباره ایمنی و امنیت می تواند با یکدیگر تعامل داشته باشد.

هرگونه نقض امنیت سایبری در چنین شبکه ای با سرعت بالا می تواند ایمنی و امنیت سیستم را به خطر بیندازد. تحلیل های ایمنی و امنیتی مورد استفاده در این مطالعه موردی توسط ISO/SAE (۲۰۲۱b) و به طور داخلی با استفاده از یک ابزار تحلیل تهدید



شکل ۲۵: معماری پلوتون.

و امنیت خودرویی تجاری به نام ThreatGet (Christl و Tarrach، ۲۰۲۱) انجام شده است. تحلیل ایمنی با استفاده از روش تحلیل خطر و ارزیابی ریسک (HARA) مطابق با (ISO، ۲۰۱۸) و تحلیل امنیت با استفاده از فرایند تحلیل تهدید و ارزیابی ریسک (TARA) طبق دستورالعمل‌های ISO/SAE (۲۰۲۱a) صورت گرفته است.

۱.۵ معماری پلوتون خودرویی

حمل و نقل با استفاده از پلوتون‌های خودرویی مزایای زیادی در صنعت لجستیک دارد، جایی که می‌تواند به کاهش هزینه‌های سوخت و محیط زیست کمک کند (Taylor و همکاران، ۲۰۲۲). شکل ۲۵ معماری سطح بالای پلوتون‌های خودرویی را نشان می‌دهد. همان‌طور که مشاهده می‌شود، معماری از دو دامنه متمایز تشکیل شده است:

دامنه پلوتون شامل خودروهای پلوتون با ارتباطات (V2V) Vehicle-to-Vehicle بین آن‌ها است. در اینجا مشاهده می‌شود که پلوتون از دو نوع خودرو تشکیل شده است: (۱) یک خودروی رهبری - که به‌طور دستی رانده می‌شود و مسئول تمامی تصمیمات مربوط به سرعت و فاصله‌ای است که خودروهای دیگر باید رعایت کنند تا ایمنی حفظ شود. رهبر این اطلاعات را به‌طور مداوم به خودروهای عضو منتقل می‌کند. (۲) چندین خودروی عضو - این خودروها بخشی از پلوتون هستند و عمدتاً به‌صورت خودکار هدایت می‌شوند. آن‌ها به اطلاعات دریافتی از خودروی رهبر و اطلاعات حسگرها برای حفظ حداقل فاصله از خودروی جلویی متکی هستند. به‌عنوان مثال، اگر رهبر از خودروهای عضو بخواهد که سرعت خود را به میزان ۵ مایل بر ساعت کاهش دهند، خودروهای عضو باید به‌طور هم‌زمان سرعت خود را کاهش دهند. در غیر این صورت، ممکن است تصادفاتی بین خودروهای پلوتون رخ دهد. علاوه بر این، هر خودرویی در پلوتون به سیستم (CACC Cruise Automated Cooperative Control) مجهز است که به خودروها اجازه می‌دهد به‌صورت همکاری و هماهنگ در جاده‌ها حرکت کنند.

دامنه زیرساخت در این معماری نمایانگر بخش ثابت شبکه است و شامل یک واحد کنار جاده‌ای (RSU) و یک مرکز کنترل ترافیک می‌باشد. خودروی رهبر از طریق RSU با مرکز کنترل ارتباط برقرار می‌کند و از ارتباط (V2I) Vehicle-to-Infrastructure استفاده می‌کند. خودروهای پلوتون به‌طور مداوم با مرکز کنترل ارتباط برقرار می‌کنند تا اطلاعات مهمی از جمله موقعیت فعلی خود را فراهم کنند که به مرکز کنترل کمک می‌کند تا پلوتون خودروها را تحت نظر داشته باشد.

۲.۵ امنیت سایبری و مسائل ایمنی در پلوتون‌های خودرویی

امنیت سایبری و ایمنی از دغدغه‌های حیاتی در پلوتون‌های خودرویی هستند، که به‌عنوان گروهی از خودروها که برای بهبود ایمنی، کارایی و مصرف سوخت، ارتباط و هماهنگی حرکت‌های خود را انجام می‌دهند، تعریف شده‌اند (بخش ۱.۵). امنیت سایبری و ایمنی به‌طور مستقیم به یکدیگر مرتبط هستند در پلوتون‌های خودرویی. پلوتون‌های خودرویی به‌طور خاص به ارتباطات بی‌سیم متکی هستند که ممکن است در معرض انواع حملات قرار بگیرند (Taylor و همکاران، ۲۰۲۱).

در سیستم‌های خودرویی، تعارض بین ایمنی و امنیت ممکن است غیرمنتظره به نظر برسد. در نهایت، هدف اصلی هر دو حوزه، حفاظت از کاربران و اطمینان از عملکرد بهینه خودرو است. با این حال، استراتژی‌های دستیابی به این اهداف گاهی اوقات با یکدیگر در تعارض هستند،

به‌ویژه زمانی که به خودروهای متصل و مدرن مورد استفاده در پلوتون‌ها نگاه می‌کنیم.

برای مثال، مهاجم می‌تواند پیام‌های مهمی که توسط خودروی رهبر ارسال می‌شود را رهگیری کرده و سپس پیامی با اطلاعات دستکاری شده به خودروهای عضو ارسال کند. این می‌تواند تأثیر زیادی بر ایمنی داشته باشد زیرا هرگونه اطلاعات نادرست می‌تواند منجر به تصادف بین خودروها شود که نه تنها موجب آسیب‌های شخصی می‌شود بلکه به خسارات عملیاتی و مالی نیز منجر می‌شود. بنابراین، برای اطمینان از ایمنی پلوتون‌های خودرویی، باید اطمینان حاصل کرد که مسائل امنیت سایبری به‌خوبی مورد بررسی و حل و فصل قرار گرفته‌اند.

اجرای پلوتون‌های خودرویی نگرانی‌های ایمنی و امنیت سایبری را به‌همراه دارد، از جمله اما نه محدود به: ایمنی: ارتباطات Vehicle-to-Vehicle (V2V) برای عملکرد پلوتون‌های خودرویی حیاتی است و هرگونه اختلال در این ارتباط می‌تواند به مسائل ایمنی منجر شود. به‌عنوان مثال، اگر یکی از خودروهای پلوتون قادر به برقراری ارتباط با سایرین نباشد، ممکن است موجب شکست در تشکیل پلوتون شود که می‌تواند به تصادف منجر گردد.

امنیت سایبری: وابستگی به ارتباطات V2V برای هماهنگی حرکت‌های پلوتون آنها را در برابر حملات سایبری آسیب‌پذیر می‌کند. مهاجمان ممکن است بتوانند ارتباط بین خودروها را دستکاری کرده و موجب رفتار غیرمنتظره خودروها شوند که ایمنی و امنیت خودروها و سرنشینان آنها را به خطر می‌اندازد.

حریم خصوصی داده‌ها: فناوری ارتباط Vehicle-to-Everything (V2X) به خودروها اجازه می‌دهد تا با سایر خودروها و زیرساخت‌ها، مانند چراغ‌های راهنمایی، واحدهای کنار جاده‌ای (RSUs) و سایر کاربران جاده ارتباط برقرار کنند. جمع‌آوری و به اشتراک‌گذاری این داده‌ها نگرانی‌های حریم خصوصی را به‌دنبال دارد، زیرا اطلاعات حساس مانند موقعیت و سرعت خودروها می‌تواند توسط عوامل مخرب سوءاستفاده شود. تداخل: تداخل از سایر فناوری‌های ارتباطات بی‌سیم، مانند Wi-Fi، می‌تواند به ارتباطات V2V آسیب زده و به مسائل ایمنی منجر شده و قابلیت اطمینان سیستم پلوتون را به خطر اندازد.

حسگرها: استفاده از حسگرها، مانند دوربین‌ها، لیدارها و رادارها، برای عملکرد پلوتون‌های خودرویی ضروری است. با این حال، هرگونه خرابی یا نقص در این حسگرها می‌تواند منجر به انتقال اطلاعات نادرست شده و ایمنی خودروها و سرنشینان آنها را به خطر بیندازد. همچنین، حسگرها می‌توانند در برابر حملات سایبری آسیب‌پذیر باشند و داده‌های منتقل شده از حسگرها ممکن است به‌طور غیرقانونی دستکاری شود. جمع‌آوری و انتقال داده‌های حسگرها، مانند دوربین‌ها و رادارها، همچنین می‌تواند نگرانی‌های حریم خصوصی را به‌دنبال داشته باشد.

نگرانی‌های فوق اهمیت متعادل‌سازی تعارضات بین امنیت سایبری و ایمنی در پلوتون‌های خودرویی را نشان می‌دهد، که نیاز به یک رویکرد جامع دارد، یعنی متدولوژی پیشنهادی در بخش ۳، که به بررسی خطرات و پیامدهای هر دو حوزه امنیت و ایمنی با یا بدون تأثیرات متقابل آنها، نیازها و اقدامات مربوطه برای دستیابی به تعادل بهینه بین امنیت و ایمنی می‌پردازد.

به‌طور کلی، برای پاسخ به نگرانی‌های فوق، سازمان‌ها اقدام به پیاده‌سازی تدابیر امنیت سایبری و ویژگی‌های ایمنی قوی از جمله (۱) رمزنگاری و احراز هویت برای محافظت از ارتباطات V2V و V2X در برابر حملات سایبری، و (۲) سیستم‌های ارتباطی افزونه و مکانیزم‌های ایمنی برای کاهش خطر مسائل ایمنی در صورت بروز اختلالات ارتباطی می‌کنند.

متدولوژی پیشنهادی یک رویکرد جامع را ارائه می‌دهد که به بررسی خطرات و پیامدهای احتمالی هر دو حوزه امنیت و ایمنی با تأثیرات متقابل آنها، نیازها و اقدامات مربوطه برای دستیابی به تعادل بهینه بین امنیت و ایمنی می‌پردازد.

۳.۵ بحث و بررسی

ابزار Excel ای از متدولوژی پیشنهادی ساخته شده است که نتایج اصلی گزارش‌های تحلیل ایمنی و امنیت را دریافت کرده و ماتریس‌های رابطه متقابل تعریف‌شده را به‌صورت گام‌به‌گام تولید می‌کند. همان‌طور که در بخش ۳ توضیح داده شده است، این ماتریس‌ها و به‌ویژه شکل‌های ۱۰ و ۱۱، با استفاده از روش‌های CRAF تجزیه و تحلیل شده و تعارضات بالقوه را حل و فصل می‌کنند. به دلیل محدودیت‌های فضایی، آثار تحلیلی ارائه‌شده در ادامه صرفاً به‌عنوان نماینده‌ای از نحوه استفاده از متدولوژی پیشنهادی برای کاربرد عملی آن می‌باشند. شکل ۲۶ تصویری از ابزار Excel را نشان می‌دهد. این مجموعه رنگارنگ از صفحات گسترده، پیاده‌سازی‌های گام‌به‌گام متدولوژی پیشنهادی و ماتریس‌های تولیدشده آن را نمایش می‌دهد.

ارتباطات در سطح شبکه و سیستم مانند سیستم‌های ارتباطی V2X (وسیله به همه چیز) و V2V (وسیله به وسیله) اجزای حیاتی خودروهای متصل، به‌ویژه در پلوتون‌های خودرویی، هستند و به وسایل نقلیه امکان می‌دهند با یکدیگر و با زیرساخت‌های اطراف خود ارتباط برقرار کنند. این سیستم‌های ارتباطی از مکانیزم‌های مختلف رمزنگاری برای ایمن‌سازی ارتباطات و جلوگیری از دسترسی غیرمجاز استفاده می‌کنند. با این حال،

| | A | B | C | D | E | F |
|--|--|---|---|----------------------------|--|---|
| 1 | Completed by Safety Team | | | Completed by Security Team | | Completed by Both Teams |
| 2 | Safety Requirement | Safety Measure | Data Safety Property | Data Security property | Conflict? | Conflict Resolution |
| 3 | Avoid collision due to loss of V2V braking information from the forward vehicle | The following trucks' autonomous driving HW shall have enough processing power, memory and bus resources to track and update the relevant metadata of at least 20 of the closest vehicles/pedestrians/obstacles in realtime | Accessibility, availability, lifetime, priority, sequencing, timeliness | Confidentiality | Yes, heavy encryption mechanism will occupy hardware resources and introduce latency | 1) The autonomous driving HW shall have both enough processing power, memory and bus resources to track and update the relevant metadata of at least 20 of the closest vehicles/pedestrians/obstacles in realtime and also capable to accommodate an encryption mechanism to protect the data flow. 2) Implementation of a light version of the encryption mechanism to avoid consuming the HW resources. |
| 4 | Avoid collision due to the communication of wrong (lower than actual by 50%) deceleration value by the forward vehicle | The following trucks shall be able to localize and track intruders in all weather and light conditions within the ODD. - The following trucks shall be able to detect and track relevant motorcycles and cyclists in all weather and light conditions within the ODD. - The following trucks shall be able to detect vehicles with unusual livery | Accessibility, availability, lifetime, priority, sequencing, timeliness | Confidentiality | Yes, heavy encryption mechanism will occupy hardware resources and introduce latency | 1) The autonomous driving HW shall have both enough processing power, memory and bus resources to track and update the relevant metadata of at least 20 of the closest vehicles/pedestrians/obstacles in realtime and also capable to accommodate an encryption mechanism to protect the data flow. 2) Implementation of a light version of the encryption |
| 5 | Avoid collision due to the communication of wrong (lower than actual by 75%) deceleration value by the forward vehicle | localize and track intruders in all weather and light conditions within the ODD. - The following trucks shall be able to detect and track relevant motorcycles and cyclists in all weather and light conditions within the ODD. - The following trucks shall be able to detect vehicles with unusual livery | Accessibility, availability, lifetime, priority, sequencing, timeliness | Confidentiality | Yes, heavy encryption mechanism will occupy hardware resources and introduce latency | 1) The autonomous driving HW shall have both enough processing power, memory and bus resources to track and update the relevant metadata of at least 20 of the closest vehicles/pedestrians/obstacles in realtime and also capable to accommodate an encryption mechanism to protect the data flow. 2) Implementation of a light version of the encryption mechanism to avoid consuming the HW resources. |
| | Avoid collision due to the communication of wrong (lower than actual by 37.5%) | The following trucks shall be able to localize and track intruders in all weather and light conditions within the ODD. - The following trucks shall be able to detect and track relevant | Accessibility, availability, lifetime, priority, sequencing, timeliness | Confidentiality | Yes, heavy encryption mechanism will occupy hardware resources and introduce latency | 1) The autonomous driving HW shall have both enough processing power, memory and bus resources to track and update the relevant metadata of at least 20 of the closest vehicles/pedestrians/obstacles in realtime and also capable to accommodate an |
| Assests_ConceptPhase SafetyGoals SecurityGoals GA1_SafetytoAssets GG1_SafetytoSecurity GA2_SecuritytoAssets GG2_SecuritytoSafety CRAF_SafetytoSecurity CRAF_SecuritytoSafety ConflictResolution MR1-SafetytoSecurity | | | | | | |

شکل ۲۶: مروری بر ابزار TOMSAC

همان‌طور که توسط ابزار TOMSAC شناسایی شده است (شکل ۲۷)، این سیستم‌ها برخی از نقاط اصلی تعارضات ایمنی و امنیتی هستند. الزامات ایمنی ایجاب می‌کند که سیستم ارتباطی باید به‌صورت بلادرنگ با حداقل تأخیر و با قابلیت اطمینان بالا عمل کند تا ایمنی مسافران و سایر کاربران جاده تضمین شود. از سوی دیگر، الزامات امنیتی ایجاب می‌کند که سیستم ارتباطی باید ایمن بوده و در برابر حملات سایبری مقاوم باشد.

مکانیزم‌های رمزنگاری استفاده‌شده در سیستم‌های ارتباطی V۲X (وسیله به همه چیز) و V۲V (وسیله به وسیله) برای تأمین امنیت ارتباطات و جلوگیری از دسترسی غیرمجاز به‌کار می‌روند. با این حال، این مکانیزم‌ها ممکن است به افزایش تأخیر و پیچیدگی سیستم منجر شوند، که می‌تواند بر جنبه‌های ایمنی سیستم تأثیر بگذارد. به‌عنوان مثال، اگر سیستم ارتباطی به دلیل رمزنگاری یا رمزگشایی دچار تأخیر شود، این تأخیر می‌تواند به زمان واکنش سیستم‌های ایمنی خودرو آسیب بزند و منجر به تصادف گردد.

بنابراین، ضروری است که جنبه‌های ایمنی و امنیتی سیستم‌های ارتباطی V۲X و V۲V به‌خوبی متعادل شوند. طراحی یک سیستم به‌طور دقیق که الزامات ایمنی و امنیتی را یکپارچه کند، می‌تواند اطمینان حاصل کند که سیستم به‌طور بهینه عمل می‌کند و در عین حال ایمنی مسافران و سایر کاربران جاده را حفظ می‌کند.

برای اطمینان از رانندگی خودران ایمن و کارآمد و همچنین حل تعارضات، سخت‌افزار (HW) باید با پردازشگرها، حافظه، و منابع باس کافی طراحی شود. به‌ویژه، سخت‌افزار باید قادر به پیگیری و به‌روزرسانی متاداده‌های مرتبط در یک دامنه خاص برای نظارت بر نزدیک‌ترین وسایل نقلیه، عابران پیاده، و موانع در زمان واقعی باشد. علاوه بر این، سخت‌افزار باید قادر به پشتیبانی از یک مکانیزم رمزنگاری برای حفاظت از جریان داده‌ها باشد. با این حال، پیاده‌سازی یک مکانیزم رمزنگاری کامل ممکن است منابع سخت‌افزاری زیادی مصرف کند که می‌تواند بر عملکرد تأثیر بگذارد. برای حل این مشکل، می‌توان نسخه‌ای سبک از مکانیزم رمزنگاری را پیاده‌سازی کرد تا از مصرف بیش از حد منابع سخت‌افزاری جلوگیری شود و تعادلی میان حفظ امنیت جریان داده‌ها و بهینه‌سازی عملکرد سیستم خودران ایجاد شود.

علاوه بر این، باید به تعارض میان به‌روزرسانی‌های امن نرم‌افزار و نیاز سیستم به دوران کار (uptime) پیوسته توجه کرد. به‌روزرسانی‌های امن نرم‌افزار در خودروهای مدرن برای رفع آسیب‌پذیری‌های امنیتی جدید و به‌روزرسانی عملکردهای خودرو ضروری هستند. با این حال، این به‌روزرسانی‌ها می‌تواند با نیاز به بالا بودن دوران کار سیستم در سناریوهای تجاری مانند پلانون‌های خودرویی که در آن کاهش زمان کار به‌طور مستقیم به از دست دادن تولید منجر می‌شود، تعارض داشته باشد. در این حالت، به‌عنوان مثال، می‌توان راه‌حلی مانند استفاده از به‌روزرسانی‌های Over-The-Air (OTA) همراه با یک سیستم Dual-Banking پیشنهاد کرد. در یک سیستم Dual-Banking، نرم‌افزار خودرو در دو حافظه مجزا ذخیره می‌شود. به‌روزرسانی‌ها می‌توانند در حافظه غیرفعال دانلود و نصب شوند در حالی که حافظه فعال به اجرای خودرو ادامه می‌دهد و بدین ترتیب دوران کار حفظ می‌شود. پس از کامل شدن به‌روزرسانی، سیستم به بانک به‌روزشده سوئیچ می‌کند (Feng و همکاران، ۲۰۱۷).

تعارض دیگری که ممکن است به وجود آید، از نیاز به ارتباط مداوم و قابل‌اعتماد در یک گروه پلانونی ناشی می‌شود. هر وسیله نقلیه در پلانون

| A | B | C | D | E | F | G | H | I |
|--|---|------------------------|-----------------------------|--------------|---------------------------------|------------|-----------|--|
| | Threat Description | Threat Category | Safety Malfunction Category | Impact Level | Attack Feasibility (Likelihood) | Risk Level | Treatment | Security Goal |
| 1 | CG1 Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content | Tampering | | Moderate | Medium | 2 | Accept | Avoid receiving malicious |
| 2 | CG2 Manipulation of the connectivity of vehicle functions enables a cyber-attack, this can include telematics; systems that permit remote operations; and systems using short-range wireless communications | Tampering | | Moderate | Medium | 2 | Accept | Avoid manipulation of the connectivity |
| 3 | CG3 Physical manipulation of systems can enable an attack | Tampering | | Moderate | Medium | 2 | Accept | Avoid physical manipulation |
| 4 | CG4 Parts or supplies could be compromised to permit vehicles to be attacked | Tampering | | Moderate | Medium | 2 | Accept | Avoid manipulation of the |
| 5 | CG5 Install a compromised update | Tampering | | Negligible | Medium | 1 | Accept | Avoid installation of a compromised |
| 6 | CG6 Physical Tampering of Sensor | Tampering | | Severe | High | 5 | Reduce | Avoid manipulation of the |
| 7 | CG7 Spoof messages in the vehicle network | Spoofing | | Severe | Very Low | 1 | Accept | Avoid spoof communication on the |
| 8 | CG8 Viruses embedded in communication media are able to infect vehicle systems | Spoofing | | Moderate | Medium | 2 | Accept | Avoid having viruses embedded in communication |
| 9 | CG9 Attack against remote wireless interfaces | Spoofing | | Severe | High | 5 | Reduce | Avoid attacks on the remote wireless interface |
| 10 | CG10 Data Flow Sniffing | Information Disclosure | | Negligible | High | 1 | Accept | Avoid data flow sniffing across the |
| 11 | CG11 Information can be readily disclosed. For example through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders | Information Disclosure | | Moderate | Medium | 2 | Accept | Avoid information disclosure |
| 12 | CG12 Misuse or compromise of update procedures | Information Disclosure | | Moderate | Medium | 2 | Accept | Avoid installation of a compromised |
| 13 | CG13 Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks | Elevation of Privilege | | Moderate | Medium | 2 | Accept | Avoid information disclosure |
| 14 | CG14 Deceive vehicles by falsifying vehicle identity | Elevation of Privilege | | Negligible | Very Low | 1 | Accept | Avoid falsifying vehicle identity |
| 15 | CG15 An unprivileged user is able to gain privileged access to vehicle systems | Elevation of Privilege | | Moderate | Medium | 2 | Accept | Avoid unprivileged user to gain |
| 16 | CG16 Manipulation of vehicle data/code | Elevation of Privilege | | Major | Medium | 3 | Reduce | Avoid spoof communication on the |
| 17 | | | | | | | | |
| Concept Phase Guidelines Assests_ConceptPhase SafetyGoals SecurityGoals GA1_SafetytoAssets GG1_SafetytoSecurity GA2_SecuritytoAssets GG2_SecuritytoSafety CRAF_SafetytoSecurity CRAF_SecuritytoSafety Conflict | | | | | | | | |

شکل ۲۷: شناسایی درگیری‌های ایمنی و امنیتی جوخه‌های خودرو.

باید ارتباطی پایدار و امن با دیگران حفظ کند و اطلاعاتی مانند وضعیت، موقعیت، سرعت و موارد دیگر را به اشتراک بگذارد. با این حال، تضمین ایمنی و امنیت این کانال‌های ارتباطی یک وظیفه پیچیده است. اقدامات امنیتی مانند رمزنگاری می‌تواند تأخیر یا از دست رفتن داده‌ها را به دنبال داشته باشد که به وضعیت‌های خطرناکی مانند ترمز ناگهانی یا انحراف منجر شود. برای حل این مشکل، می‌توان الگوریتم‌های پیشرفته‌ای توسعه داد که داده‌های حیاتی برای ایمنی را برای انتقال و پردازش فوری اولویت‌بندی کند، در حالی که داده‌های غیرحیاتی می‌تواند تحت تدابیر امنیتی دقیق‌تری قرار گیرد بدون اینکه ایمنی به خطر بیفتد (Yaacoub و همکاران، ۲۰۲۰).

۶ کارهای آتی

به نگاه به آینده، امیدواریم که به بررسی سیستم‌های سایبر-فیزیکی (CPS) به‌طور کلی (نه تنها خودروهای خودران) بپردازیم. در اینجا، عوامل متنوع دیگری فراتر از ایمنی و امنیت وجود دارد که باید به‌طور کامل در نظر گرفته شوند تا تعارضات احتمالی که ممکن است در یک CPS به وجود آید، به‌خوبی درک شود.

خودروهای متصل و خودران با طیف وسیعی از تعارضات بالقوه مواجه هستند که هرکدام چالش‌های منحصر به‌فرد خود را دارند. در اینجا، به برخی از این چالش‌ها پرداخته می‌شود که هدف ما شامل کردن آن‌ها در روش‌شناسی است.

هزینه در مقابل امنیت: پیاده‌سازی اقدامات قوی امنیت سایبری، مانند پروتکل‌های امن ارتباطی و ماژول‌های رمزنگاری سخت‌افزاری، ممکن است هزینه‌های قابل‌توجهی را به دنبال داشته باشد. اما کوتاهی در این اقدامات می‌تواند سیستم را در معرض حملات سایبری قرار دهد. نکته اصلی در این مسئله تعیین این است که افزایش هزینه تا چه حد برای تقویت امنیت توجیه‌پذیر است. هیچ پاسخ ساده‌ای برای این سؤال وجود ندارد، زیرا این مسئله از موردی به مورد دیگر بسته به عواملی مانند عملکرد خودرو، گروه هدف کاربران و غیره متفاوت است. تولیدکنندگان خودروهای برقی لوکس (EV) به پیاده‌سازی اقدامات امنیت سایبری قوی برای حفاظت از خودروها و مشتریان خود در برابر تهدیدات سایبری احتمالی اولویت می‌دهند. این تعهد به امنیت سایبری اغلب منجر به افزایش هزینه کلی خودرو می‌شود و آن را از سایر گزینه‌های EV گران‌تر می‌کند. سرمایه‌گذاری در اقدامات امنیت سایبری پیشرفته به دلیل آسیب‌پذیری‌های بالقوه خودروهای متصل و ایستگاه‌های شارژ EV در برابر حملات سایبری، اهمیت ویژه‌ای دارد، همان‌طور که در مراجع متعدد (Anon، ۲۰۲۳؛ Boulton، ۲۰۲۳؛ Wilson، ۲۰۲۳) به آن اشاره شده است. قابلیت استفاده در مقابل امنیت: امنیت پیشرفته اغلب با هزینه‌های مربوط به راحتی کاربر همراه است. به‌عنوان مثال، سیستمی برای خودروهای متصل که نیاز به پسوردهای پیچیده یا احراز هویت چند مرحله‌ای داشته باشد، ممکن است امنیت بیشتری ارائه دهد، اما ممکن

است کاربران را به دلیل زمان و تلاش اضافی مورد نیاز برای استفاده از آن، ناامید کند. پیدا کردن توازن میان این دو بسیار حیاتی است - طراحی سیستم‌هایی که سطح بالایی از امنیت را حفظ کرده و در عین حال کاربرپسند باشد، یک چالش بزرگ است. به عنوان مثال، استفاده از احراز هویت بیومتریک در برخی مدل‌های خودروهای لوکس می‌تواند امنیت بالایی را فراهم کند، اما برخی از رانندگان آن را خسته‌کننده می‌دانند و ترجیح می‌دهند از کلیدهای سنتی یا فوب‌های ساده استفاده کنند. این می‌تواند باعث شود که آن‌ها این ویژگی‌های امنیتی را غیر فعال کرده و خودرو را آسیب‌پذیرتر کنند (Tengler، ۲۰۲۱؛ Nuspire، ۲۰۲۳؛ Vellinga، ۲۰۲۲).

حریم خصوصی در مقابل امنیت: خودروهای متصل داده‌های زیادی تولید می‌کنند که شامل اطلاعات شخصی حساس ممکن است باشد. در حالی که تأمین امنیت این داده‌ها در برابر حملات سایبری بسیار مهم است، انجام این کار می‌تواند به نگرانی‌های حریم خصوصی منجر شود. توازن میان امنیت داده‌ها و حفاظت از حریم خصوصی یک مسئله پیچیده است که راه‌حل‌های آن اغلب شامل مدیریت دقیق داده‌ها، از جمله تکنیک‌های pseudonymization و کنترل‌های دسترسی شدید است. به عنوان مثال، استفاده از داده‌های تلماتیک توسط شرکت‌های بیمه. این داده‌ها می‌توانند به بیمه‌گران کمک کنند تا قیمت‌های بیمه را به دقت بر اساس رفتار واقعی راننده تنظیم کنند و مدل‌های ریسک خود را بهبود بخشند. با این حال، جمع‌آوری چنین داده‌های دقیقی درباره الگوها و مکان‌های رانندگی افراد می‌تواند نگرانی‌های جدی حریم خصوصی را به همراه داشته باشد و بدون اقدامات حفاظتی مناسب ممکن است به صورت بدخواهانه مورد سوءاستفاده قرار گیرد (Liu و همکاران، ۲۰۲۲).

استانداردها در مقابل نوآوری: پیروی از استانداردهای شناخته شده، مانند ISO/SAE ۲۱۴۳۴ برای مدیریت امنیت سایبری و ISO ۲۶۲۶۲ برای ایمنی عملکردی، سطح پایه‌ای از امنیت و ایمنی را تضمین می‌کند. با این حال، پایبندی به این استانداردها ممکن است باعث کاهش نوآوری شود. یافتن توازن میان نیاز به پیروی از استانداردهای معتبر و پشتیبانی از نوآوری یکی دیگر از چالش‌های بزرگ در صنعت خودرو است. به عنوان مثال، یک استارت‌آپ ممکن است سیستم ایمنی جدید و کارآمدتری را توسعه دهد که با استانداردهای ISO کاملاً هم‌راستا نباشد. این ممکن است باعث تأخیر در معرفی فناوری‌های بالقوه نجات‌بخش یا منجر به عدم انطباق با مراجع نظارتی شود. پروژه خودران Waymo از گوگل نمونه جالبی است. آن‌ها فناوری خودران خود را توسعه داده‌اند که شامل راه‌حل‌های منحصربه‌فردی است که ممکن است کاملاً با استانداردهای موجود هم‌راستا نباشد. به عنوان مثال، فرآیند تصمیم‌گیری مبتنی بر هوش مصنوعی آن‌ها ممکن است به سختی استانداردسازی شود، زیرا ممکن است به عنوان یک "جعبه سیاه" دیده شود که به طور کامل قابل درک یا پیش‌بینی نیست (Anon ۲۰۲۲b، Anon ۲۰۲۲a).

هر یک از این مثال‌ها نشان می‌دهد که مدیریت تعارضات در خودروهای متصل و خودران یک وظیفه پیچیده است که نیاز به بررسی دقیق بسیاری از جوانب مانند هزینه، قابلیت استفاده، ایمنی، امنیت، حریم خصوصی و نیاز به نوآوری دارد. ادغام این پارامترها در TOMSAC نیازمند توازن مناسبی است که تنها با در نظر گرفتن همه این عوامل به صورت یک رویکرد جامع و یکپارچه قابل دستیابی است.

۷ جمع‌بندی و نتیجه‌گیری

در پایان، این تحقیق با موفقیت، TOMSAC یک روش‌شناسی نوین برای مدیریت تعارضات میان ایمنی و امنیت سایبری در چرخه عمر توسعه سیستم‌های سایبر-فیزیکی را توسعه و معرفی کرده است. این روش‌شناسی یک راه‌حل عملی و کاربرپسند را ارائه می‌دهد که به مسئله دیرینه عدم توجه به تعاملات ایمنی و امنیت پرداخته و با ترکیب سیستماتیک داده‌های تحلیل ایمنی و امنیت، تعارضات و تعاملات زیرین را روشن می‌سازد و بدین ترتیب، تصمیم‌گیری جامع‌تری را تشویق می‌کند.

علاوه بر این، ایجاد یک ابزار اکسل همراه به قابلیت استفاده TOMSAC افزوده و یک روش مناسب و قابل دسترس برای پیاده‌سازی این روش‌شناسی توسط فعالان این حوزه فراهم می‌آورد. این ابزار به طور قابل توجهی قابلیت اجرایی TOMSAC را در محیط‌های واقعی افزایش می‌دهد و مسیر را برای پذیرش گسترده‌تر آن هموار می‌سازد.

مطالعه موردی نشان می‌دهد که چگونه روش‌شناسی پیشنهادی می‌تواند به طور ملموس توسط OEM خودرو برای ایجاد کانال‌های ارتباطی لازم میان امنیت سایبری و ایمنی عملکرد استفاده شود و چگونه این روش می‌تواند به سایر رشته‌های مهندسی مرتبط گسترش یابد، همان‌طور که در ISO/SAE ۲۱۴۳۴ نیاز است. چنین رویکردی به تولیدکنندگان این امکان را می‌دهد که استفاده مؤثر از منابع محدود موجود خود را با مهارت‌های لازم در زمینه امنیت و ایمنی به حداکثر برسانند.

با این حال، این مطالعه همچنین ضرورت تحقیق مستمر در این حوزه را روشن می‌سازد، به ویژه در زمینه تکمیل و اعتبارسنجی TOMSAC در انواع مختلف سیستم‌های سایبر-فیزیکی. مقاومت و عدم تمایل به تغییر در شیوه‌های جاری، همان‌طور که در ابتدای مقاله بیان شد، بر لزوم آموزش مداوم، ترویج و مطالعات آزمایشی بیشتر برای ترویج درک جامع و پذیرش تعاملات ایمنی و امنیت سایبری تأکید دارد.

این مقاله پایه‌ای برای این تغییر پارادایم در چرخه عمر توسعه سیستم‌های سایبر-فیزیکی را بنا کرده و نقشه راهی برای این شیوه‌ی جدید ایجاد کرده است. با فراهم کردن یک رویکرد یکپارچه و متوازن برای ایمنی و امنیت سایبری، روش‌شناسی TOMSAC می‌تواند به‌طور قابل توجهی به ایجاد سیستم‌های امن‌تر، مطمئن‌تر و قابل‌اعتمادتر کمک کند. پیامدهای آینده این تحقیق گسترده و مهم است و امید است که این کار به تحقیقات و توسعه‌های بیشتری در این حوزه ضروری دامن زند.