ISSN:

مجله علمی نوآوری و تحقیق در مهندسی مکانیک

جلد ۱، شماره ۱، پاییز و زمستان ۱۴۰۴، صفحه: ۲۸۵ تا ۲۹۹

مجله علمی
مهندسی مکانیک

گذار به معماری‌های متمرکز در خودروهای نسل آینده: ارائه یک چارچوب یکپارچه برای مدیریت چالش‌های امنیت، قابلیت اطمینان و مدیریت انرژی واحدهای کنترل الکترونیکی

علیرضا محمودی فرد*[۱]، سید محمدرضا حسینی علی آباد[۲]

[۱] پسادکترای آینده‌پژوهی و مدرس دانشگاه ملی مهارت، دانشکده فنی انقلاب اسلامی، تهران، ایران، alireza۱۰.m۱۰@gmail.com

[۲] پست دکتری مدیریت بازرگانی-مدیریت استراتژیک، دانشگاه بین‌المللی نورث‌وست ارمنستان، info@confnashr.ir

ISSN

چکیده

تحول واحد کنترل الکترونیکی (ECU) از یک عنصر تخصصی به مغز متفکر سیستم‌های سایبر-فیزیکی پیچیده، صنعت خودرو را در آستانه‌ی یک تحول معماری اساسی قرار داده است. این مقاله به بررسی چالش‌های بنیادین معماری توزیع‌شده‌ی کنونی شامل پیچیدگی فزاینده، محدودیت‌های امنیتی شبکه‌های سنتی و موانع مقیاس‌پذیری و الزامات معماری‌های متمرکز (دامنه‌محور و منطقه‌محور) نسل آینده می‌پردازد. تمرکز اصلی بر شناسایی و ارائه‌ی راهکارهایی برای مسائل نوظهور در این گذار، به‌ویژه در سه حوزه‌ی کلیدی است: نخست، تهدیدات امنیت سایبری در شبکه‌های پهن‌باند و متمرکز و ضرورت طراحی الگوهای دفاعی لایه‌ای؛ دوم، نیاز به سخت‌افزارهای محاسباتی ناهمگن با قابلیت تحمل خطا و ملاحظات مدیریت حرارتی پیشرفته برای تضمین قابلیت اطمینان در سطح ASIL-D؛ و سوم، توسعه‌ی چارچوب‌های نرم‌افزاری مبتنی‌بر مدل و روش‌های تأیید رسمی برای سیستم‌های خود-تطبیق و مبتنی‌بر هوش مصنوعی. برپایه‌ی تحلیل داده‌های تجربی و شبیه‌سازی‌های پیشین، مقاله استدلال می‌کند که موفقیت این انتقال در گرو اتخاذ یک رویکرد طراحی سیستماتیک و همه‌جانبه‌نگر است که ملاحظات سخت‌افزاری، نرم‌افزاری، امنیتی و حرارتی را از مرحله‌ی مفهوم تا پایان عمر، یکپارچه کند. درنهایت، چارچوب مفهومی پیشنهادی و مسیرهای پژوهشی آینده برای تحقق این چشم‌انداز ارائه می‌شوند.

کلمات کلیدی

واحد کنترل الکترونیکی، معماری متمرکز خودرو، امنیت سایبری خودرو، قابلیت اطمینان سخت‌افزار، مدیریت حرارتی الکترونیک، شبکه‌ی اترنت خودرویی، تأیید رسمی نرم‌افزار، پردازش ناهمگن

ISSN: mechanical-eng.ir

مقدمه

سیر تحول خودرو از یک وسیله‌ی مکانیکی صرف به یک سیستم الکترومکانیکی پیچیده و فوق‌هوشمند، یکی از چشمگیرترین دستاوردهای مهندسی در قرن بیست‌ویکم محسوب می‌شود. در قلب این تحول، واحد کنترل الکترونیکی (ECU) به‌عنوان مغز متفکر و سیستم عصبی مرکزی خودروهای مدرن ایفای نقش می‌کند. ظهور و گسترش فزاینده‌ی ECUها را می‌توان پاسخی مستقیم به سه تقاضای کلیدی صنعت خودروسازی دانست: نیاز فزاینده به بهینه‌سازی مصرف سوخت و کاهش آلایندگی تحت قوانین سخت‌گیرانه‌ی زیست‌محیطی (مانند استانداردهای یورو ۶ و ۷)، تلاش برای ارتقای بی‌وقفه‌ی ایمنی فعال و غیرفعال (از ترمزهای ضدقفل ساده تا سامانه‌های پیشرفته‌ی کمک‌راننده راننده ADAS) و انتظارات روزافزون مشتریان برای راحتی، اتصال‌پذیری و تجربه‌ی رانندگی شخصی‌سازی‌شده (Robert Bosch GmbH, ۲۰۱۸). در گذر از سیستم‌های مکانیکی و الکترومکانیکی به سوی حکمرانی تمام‌عیار الکترونیک، ECUها مسئولیت تفسیر داده‌های دریافتی از شبکه‌ای گسترده از حسگرها، پردازش این داده‌ها در کسری از میلی‌ثانیه با استفاده از الگوریتم‌های پیچیده و صدور فرامین دقیق به اجرایی‌کننده‌ها (اکتوئاتورها) را بر عهده گرفته‌اند. این دگرگونی، خودروی امروزی را به یک «سیستم سایبر-فیزیکی (Cyber-Physical System)» متشکل از ده‌ها، و در مدل‌های پیشرفته تا بیش از صد، ECU تخصص‌یافته و اغلب ناهمگن تبدیل کرده است که از طریق شبکه‌های ارتباطی درون‌خودرویی مانند CAN، LIN، FlexRay و اترنت با یکدیگر در تبادل مداوم هستند (Navet et al., ۲۰۱۷). این معماری توزیع‌شده اگرچه انعطاف‌پذیری و قابلیت توسعه را افزایش داده، اما پیچیدگی طراحی، یکپارچه‌سازی، اعتبارسنجی و نگهداری سیستم را به‌صورت نمایی رشد داده است. چالش‌های مهندسی معاصر حول محور ECUها تنها محدود به پردازش سریع‌تر یا افزودن عملکردهای بیشتر نیست، بلکه مسائل بنیادین‌تری چون امنیت سایبری در برابر تهدیدات فزاینده، قابلیت اطمینان در طول چرخه‌ی عمر طولانی خودرو تحت شرایط سخت کاری، مدیریت انرژی الکتریکی و پیچیدگی نرم‌افزاری را در برمی‌گیرد (Macher et al., ۲۰۱۷). به‌طور مشخص، افزایش تصاعدی حجم و پیچیدگی کد نرم‌افزاری در ECUها (که از چند کیلوبایت در دهه‌ی ۱۹۸۰ به چندصد مگابایت در خودروهای امروزی رسیده) مستلزم اتخاذ روش‌های نوین مهندسی نرم‌افزار، چارچوب‌های مبتنی‌بر مدل (Model-Based Design) و رویکردهای توسعه‌ی مبتنی‌بر معماری (AUTOSAR) شده است (Broy et al., ۲۰۱۲). علاوه‌براین، انقلاب نوظهور در حرکت به سوی خودروهای الکتریکی، هیبریدی و خودران، نقش و اهمیت ECUها را به‌مراتب حیاتی‌تر کرده است. در این خودروها، ECUها نه‌تنهاباید عملکردهای سنتی را مدیریت کنند، بلکه مسئولیت کنترل دقیق موتورهای الکتریکی، مدیریت باتری‌های با ولتاژ بالا، پردازش داده‌های حجیم سنسورهای لیدار و رادار، و اتخاذ تصمیم‌های ایمن در شرایط بلادرنگ را نیز بر عهده دارند. این انتقال پارادایم، نیازمند نسل جدیدی از سخت‌افزارهای محاسباتی با کارایی بالا (همچون SoCها و پردازنده‌های چندهسته‌ای)، معماری‌های نرم‌افزاری امن و قابل اعتماد، و روش‌های ارتباطی با پهنای باند بسیار بالا هستند. بنابراین، پژوهش در حوزه‌ی ECUهای خودرو دیگر یک حوزه‌ی تخصصی صرفاً در مهندسی کنترل یا الکترونیک نیست، بلکه یک حوزه‌ی میان‌رشته‌ای پویاست که در تقاطع مهندسی کامپیوتر، مهندسی برق، علم مواد، مهندسی نرم‌افزار و امنیت سایبری قرار گرفته است. این مقاله با درنظرگرفتن این زمینه‌ی پیچیده و پویا، به بررسی عمیق چالش‌ها، فرصت‌ها و روندهای آتی در طراحی، توسعه و استقرار ECUهای نسل آینده می‌پردازد.

بیان مسأله

با وجود پیشرفت‌های چشمگیر در حوزه‌ی واحدهای کنترل الکترونیکی (ECU) خودرو، صنعت خودروسازی در آستانه‌ی یک گذار پارادایمی عمیق قرار دارد. معماری الکترونیکی توزیع‌شده‌ی کنونی متشکل از ده‌ها ECU ناهمگن و شبکه‌های ارتباطی سنتی (مانند CAN)، با چالش‌های بنیادین و فزاینده‌ای مواجه است. این چالش‌ها شامل پیچیدگی لاینحل در توسعه و یکپارچه‌سازی نرم‌افزار، محدودیت‌های ذاتی امنیت سایبری در پروتکل‌های موجود، افزایش نمایی وزن و هزینه سیم‌کشی و مشکلات در مقیاس‌پذیری برای پشتیبانی از قابلیت‌های آینده مانند خودران‌سازی سطح بالا و سرویس‌های دیجیتال پیوسته می‌شود. حرکت به سوی معماری‌های متمرکز با کامپیوترهای مرکزی قدرتمند، اگرچه وعده‌ی حل این مسائل را می‌دهد، اما خود مسائل جدیدی را ایجاد می‌کند. این مسائل جدید شامل تمرکز ریسک‌های امنیتی و نقاط شکست واحد، نیاز به سخت‌افزارهای محاسباتی امن و فوق‌قابل‌اطمینان با مصرف انرژی بهینه، چالش‌های مدیریت حرارتی در پردازش‌های فشرده و فقدان چارچوب‌های نرم‌افزاری و روش‌های اعتبارسنجی یکپارچه برای چنین سیستم‌های پیچیده و حیاتی است. بنابراین، مسأله‌ی اصلی، نبود یک چارچوب طراحی سیستماتیک، ایمن و مقیاس‌پذیر برای معماری الکترونیکی نسل آینده‌ی خودروهاست که بتواند به‌طور هم‌زمان به نیازهای متعارض عملکرد، ایمنی، امنیت، قابلیت اطمینان و کارایی اقتصادی پاسخ گوید.

اهداف پژوهش

هدف اصلی: ارائه‌ی یک چارچوب نوآورانه و همه‌جانبه برای طراحی و ارزیابی معماری‌های الکترونیکی متمرکز (Domain-Centralized و Zonal) در خودروهای نسل آینده که یکپارچگی عمیق ملاحظات سخت‌افزاری، نرم‌افزاری، امنیتی و حرارتی را ممکن می‌سازد.

اهداف فرعی:

۱. تحلیل و بررسی مدل‌سازی ریسک‌های امنیتی در معماری‌های متمرکز و ارائه‌ی یک الگوی دفاعی لایه‌ای (Layered Defense Model) برای محافظت از سیستم در برابر تهدیدات داخلی و خارجی.

۲. بررسی طراحی و شبیه‌سازی یک معماری مرجع پردازشی ناهمگن با قابلیت تحمل خطا برای کامپیوترهای مرکزی خودرو که الزامات سطح یکپارچگی ایمنی (ASIL) بالا را برآورده سازد.

۳. توسعه‌ی یک چارچوب نرم‌افزاری مبتنی‌بر میکروسرویس و مدل‌های تأیید رسمی (Formal Verification) برای تضمین رفتار ایمن و قابلیت اطمینان بالا در سیستم‌های خود-تطبیق و مبتنی‌بر یادگیری ماشین.

۴. ارائه‌ی راهکارهای عملی برای مدیریت انرژی و حرارت در سطح سیستم در معماری‌های متمرکز و بررسی کمّی‌سازی تأثیر آن‌ها بر پایداری عملکرد بلندمدت.

سوالات پژوهش

سوال اصلی: چگونه می‌توان یک چارچوب طراحی یکپارچه ارائه داد که انتقال از معماری الکترونیکی توزیع‌شده‌ی فعلی به معماری‌های متمرکز نسل آینده را با مدیریت هم‌زمان چالش‌های امنیتی، ایمنی عملکردی، قابلیت اطمینان و مدیریت حرارتی/انرژی تسهیل و بهینه‌سازی کند؟

سوالات فرعی:

۱. آسیب‌پذیری‌های امنیتی کلیدی در یک معماری منطقه‌ای (Zonal) مبتنی‌بر اترنت خودرویی کدامند و چه مکانیزم‌های حفاظتی چندلایه‌ای می‌توانند این آسیب‌پذیری‌ها را با حداقل تأثیر بر عملکرد و تأخیر سیستم کاهش دهند؟

۲. چه ترکیبی از فناوری‌های سخت‌افزاری (مانند قفل‌قدم، جداسازی فیزیکی هسته‌ها) و راهکارهای نرم‌افزاری می‌تواند سطح مورد نیاز ASIL-D را برای عملکردهای بحرانی در یک کامپیوتر مرکزی ناهمگن فراهم آورد و هزینه (مصرف انرژی منطقه) این افزونگی چقدر است؟

۳. چگونه می‌توان از روش‌های تأیید رسمی برای ایجاد تضمین‌های قوی در مورد رفتار ایمن سیستم‌های کنترل مبتنی‌بر یادگیری عمیق در سناریوهای Corner Case که در داده‌های آموزشی موجود نیستند، استفاده کرد؟
۴. یک مدل مدیریت حرارتی پویا و سطح سیستم برای یک مرکز داده‌ی متحرک (Vehicle Data Center) چگونه باید طراحی شود تا از افت عملکرد (Thermal Throttling) در شرایط کاری سنگین و طولانی‌مدت جلوگیری کند و تأثیر آن بر عمر مفید قطعات الکترونیکی چیست؟

متن اصلی

واحد کنترل الکترونیکی (ECU) در خودروهای مدرن، دیگر یک کنترل‌کننده‌ی منفرد و ساده نیست، بلکه به یک اکوسیستم محاسباتی توزیع‌شده و بسیار پیچیده تحول یافته است که می‌توان آن را در چند لایه‌ی مفهومی تحلیل کرد. در لایه‌ی سخت‌افزاری، یک ECU مدرن متشکل است از یک یا چند ریزپردازنده یا میکروکنترلر (معمولاً مبتنی‌بر معماری ARM یا PowerPC)، حافظه‌های مختلف (Flash برای نگهداری نرم‌افزار، RAM برای اجرا، EEPROM برای داده‌های کالیبراسیون)، مدارهای مجتمع مخصوص (ASIC) برای واسط‌های ارتباطی و درایورها، و مدارهای تغذیه‌ی ولتاژ و تنظیم‌کننده‌ها (Freescale Semiconductor, ۲۰۱۵). این سخت‌افزار باید در گستره‌ی دمایی وسیع (از ۴۰- تا ۱۵۰+ درجه سانتی‌گراد)، تحت لرزش‌های مداوم و در معرض نویز الکترومغناطیسی قابل‌توجهی که در محیط خودرو وجود دارد، با قابلیت اطمینان بسیار بالا به‌مدت بیش از ۱۵ سال عمل کند. لایه‌ی نرم‌افزاری، که امروزه پیچیده‌ترین و حیاتی‌ترین بخش را تشکیل می‌دهد، شامل سیستم عامل بلادرنگ (RTOS)، میان‌افزار (Middleware)، لایه‌ی انتزاع سخت‌افزار (HAL) و نرم‌افزار کاربردی (Application Software) است. ظهور استاندارد AUTOSAR (AUTomotive Open System ARchitecture)تلاشی بنیادین برای ساختاردهی و استانداردسازی این لایه‌ی نرم‌افزاری، به‌منظور تسهیل توسعه، یکپارچه‌سازی و قابلیت استفاده‌ی مجدد نرم‌افزار در بین تولیدکنندگان مختلف و نسل‌های مختلف خودرو بوده است (AUTOSAR Partnership, ۲۰۲۱). در لایه‌ی عملکردی، ECUها را می‌توان به‌صورت عمده در سه حوزه‌ی کلیدی دسته‌بندی کرد: ۱. کنترل پیشرانه و مدیریت انرژی: این شامل ECU مدیریت موتور ((ECM، ECU کنترل انتقال (TCM) و در خودروهای الکتریکی/هیبریدی، واحد کنترل پیشرانه‌ی الکتریکی (PCU) و مدیریت سیستم باتری (BMS) است. این واحدها با اجرای الگوریتم‌های کنترل پیشرفته (مانند کنترل نظارتی و تطبیقی) بهینه‌ترین نقطه‌ی عملکردی موتور، کاهش آلایندگی و حداکثر بازده انرژی را هدف می‌گیرند (Heywood, ۲۰۱۸). ۲. ایمنی و کمک‌راننده: حوزه‌ای که با رشد انفجاری در پیچیدگی و اهمیت مواجه است و شامل ECUهای ترمز ضدقفل (ABS)، کنترل پایداری الکترونیکی (ESC)، کیسه‌هوا، و سیستم‌های پیشرفته‌ی کمک راننده (ADAS) مانند کروز کنترل تطبیقی، کمک حفظ خط و ترمز اضطراری خودکار می‌شود. این سیستم‌ها اغلب مبتنی‌بر سنسورهای چندگانه (رادار، دوربین، لیدار) و نیازمند پردازش سیگنال و داده در زمان واقعی با درجه اطمینان بسیار بالا (Safety Integrity Level بالا) هستند (Winner et al., ۲۰۱۶). ۳. راحتی، اطمینان و اتصال‌پذیری: این حوزه شامل ECUهای مدیریت بدنه (برای قفل مرکزی، پنجره‌ها، چراغ‌ها)، سیستم‌های صوتی و اینفوتیمنت، و ماژول‌های ارتباطی (T-Box) برای اتصال به شبکه‌های مخابراتی و خدمات مبتنی‌بر ابر است. چالش اصلی در طراحی مدرن، یکپارچه‌سازی هماهنگ و ایمن این ده‌ها ECU از طریق شبکه‌های ارتباطی درون‌خودرویی است. شبکه‌ی CAN (Controller Area Network) همچنان ستون فقرات برای ارتباطات حیاتی و زمان‌مند است، اما محدودیت پهنای باند آن برای حجم داده‌های سیستم‌های جدید (مانند دوربین‌ها) موجب گسترش

استفاده از FlexRay برای سیستم‌های X-by-Wire و اترنت خودرویی (Automotive Ethernet) با استانداردهایی مانند BASE-T۱۱۰۰ برای دامنه‌های با پهنای باند بالا شده است (Navet et al., ۲۰۱۷). علاوه‌بر این، معماری متمرکزشونده‌ی مبتنی‌بر دامنه (Domain-Centralized Architecture) و در نهایت معماری رایانه‌ی مرکزی (Central Computer Architecture) در حال ظهور است که در آن تعداد زیادی از عملکردهای سنتیِ توزیع‌شده در چندین ECU، در واحدهای محاسباتی مرکزی قدرتمند و تعداد محدودی ECU منطقه‌ای (Zone ECUs) ادغام می‌شوند. این انتقال، غلبه‌بر چالش‌های افزایش وزن سیم‌کشی، پیچیدگی و هزینه را هدف قرار داده است (Zheng et al., ۲۰۲۰). با این حال، این ادغام، چالش‌های جدیدی در زمینه‌ی امنیت سایبری ایجاد می‌کند، زیرا حمله به یک واحد مرکزی می‌تواند بر سیستم‌های متعددی تأثیر بگذارد. بنابراین، پیاده‌سازی مکانیزم‌های امنیتی سخت‌افزاری و نرم‌افزاری قوی مانند ماژول‌های امنیتی سخت‌افزاری (HSM)، رمزنگاری end-to-end و به‌روزرسانی امن نرم‌افزار (SOTA) به یک ضرورت غیرقابل‌انکار تبدیل شده‌اند (Koscher et al., ۲۰۱۰)

مباحث ECU در خودروها

مباحث مرتبط با واحد کنترل الکترونیکی (ECU) در خودروها طیف وسیعی از جنبه‌های سخت‌افزاری، نرم‌افزاری، شبکه‌ای و امنیتی را در برمی‌گیرد. از منظر سخت‌افزاری، طراحی ECUها با چالش‌های منحصربه‌فردی مواجه است که نیازمند استفاده از قطعات خودرویی (Automotive-Grade) با درجه‌ی کیفی AEC-Q۱۰۰ و قابلیت اطمینان بالا در بازه‌های دمایی گسترده و شرایط محیطی خشن است. معماری پردازنده‌های مدرن در ECUها از هسته‌های تک‌واحد به‌سمت پردازنده‌های چندهسته‌ای (Multi-core) و سیستم‌های روی تراشه (SoC) پیش رفته‌اند تا هم نیازهای محاسباتی فزاینده‌ی سیستم‌های پیشرفته‌ی کمک‌راننده (ADAS) و خودران را پاسخ دهند و هم امکان جداسازی عملکردهای با سطح ایمنی متفاوت (مطابق استاندارد ISO ۲۶۲۶۲) را روی یک قطعه‌ی فیزیکی فراهم کنند (Macher et al., ۲۰۱۷). لایه‌ی نرم‌افزاری یکی از پیچیده‌ترین حوزه‌هاست که شامل سیستم‌عامل بلادرنگ (RTOS)، کتابخانه‌ها، درایورها و نرم‌افزار کاربردی می‌شود. استاندارد AUTOSAR به‌عنوان یک چارچوب نرم‌افزاری جامع، با ارائه‌ی یک معماری لایه‌ای، واسط‌های استاندارد و روش‌های توصیف، هدف جداسازی نرم‌افزار کاربردی از سخت‌افزار زیرین و تسهیل قابلیت حمل و استفاده‌ی مجدد کد را دنبال می‌کند (AUTOSAR Partnership, ۲۰۲۱). بحث شبکه‌های درون‌خودرویی برای ارتباط بین ECUها نقشی حیاتی دارد. شبکه‌ی CAN (Controller Area Network) با پروتکل‌های لایه‌ی بالاتر مانند CANopen و J۱۹۳۹ همچنان پرکاربردترین بستر برای سیستم‌های کنترل زمان‌مند است. با این حال، محدودیت پهنای باند (معمولاً تا ۱ Mbps) و عدم ذاتی امنیت در آن، توسعه‌ی پروتکل‌های جدیدی مانند FlexRay (برای سیستم‌های X-by-Wire با نیازهای ایمنی بالا و پهنای باند تا ۱۰ Mbps) و به‌ویژه اترنت خودرویی (Automotive Ethernet) با استانداردهایی مانند BASE-T۱۱۰۰ و BASE-T۱۱۰۰۰ را ضروری ساخته است. اترنت با ارائه پهنای باند بالا، امکان استفاده از الگوهای ارتباطی مانند سرویس‌گرا (SOA) و پشتیبانی ذاتی از پروتکل‌های امنیتی مانند IPsec را فراهم می‌کند (Navet et al., ۲۰۱۷). امنیت سایبری به‌دلیل افزایش اتصال‌پذیری و پیچیدگی، به یکی از اولویت‌های اصلی تبدیل شده است. تهدیداتی از قبیل دسترسی غیرمجاز از راه‌دور، استخراج کلیدهای دیجیتال و حملات انکار سرویس (DoS) مستلزم پیاده‌سازی لایه‌های دفاعی چندگانه‌ای همچون ماژول امنیتی سخت‌افزاری (HSM) برای مدیریت کلید و عملیات رمزنگاری، فایروال‌های شبکه‌ای، سیستم‌های تشخیص نفوذ (IDS) و مکانیزم‌های به‌روزرسانی امن نرم‌افزار (SOTA) هستند (Koscher et al., ۲۰۱۰). فرآیند توسعه و اعتبارسنجی ECUها نیز خود بحثی گسترده است. رویکرد توسعه‌ی مبتنی‌بر مدل (MBD) با استفاده از ابزارهایی مانند MATLAB/Simulink، امکان طراحی، شبیه‌سازی و تولید کد را به‌صورت یکپارچه فراهم می‌کند. اعتبارسنجی و آزمون این سیستم‌های پیچیده، ترکیبی از روش‌های آزمون مبتنی‌بر مدل (MiL)، آزمون نرم‌افزار روی سخت‌افزار (HiL)، آزمون سیستم و آزمون وسیله‌ی نقلیه است. استاندارد ISO ۲۶۲۶۲ (فقط‌الکترونیک) چارچوبی را برای مدیریت ریسک‌های عملکردی و دستیابی به

سطح ایمنی مورد نیاز (ASIL) تعریف می‌کند (ISO ۲۶۲۶۲, ۲۰۱۸). در نهایت، روندهای آتی همچون حرکت به سمت معماری‌های متمرکز (Domain-Centralized و سپس Vehicle Computer) در حال تغییر اساسی نقش و جایگاه ECUها هستند. در این معماری‌ها، عملکردهای پردازشی در چند کامپیوتر مرکزی قدرتمند ادغام شده و ECUهای منطقه‌ای (Zone ECUs) عمدتاً مسئولیت توزیع برق، اتصال سیم‌کشی و درایو عملگرها را بر عهده خواهند داشت. این انتقال، چالش‌های جدیدی در زمینه‌ی مدیریت توان حرارتی، زمان‌بندی وظایف و تضمین تأخیر ارتباطی ایجاد می‌کند (Zheng et al., ۲۰۲۰).

مباحث پیشرفته‌تر در حوزه‌ی ECUها شامل ورود به قلمرو الگوریتم‌های هوشمند و یادگیری ماشین در خودرو می‌شود. امروزه ECUهایی که وظیفه‌ی پردازش تصویر برای سیستم‌های تشخیص عابرپیاده یا شناسایی علائم راهنمایی را بر عهده دارند، از شبکه‌های عصبی کانولوشنی (CNN) بهره می‌برند. اجرای این مدل‌های پیچیده بر روی سخت‌افزارهای محدود و با محدودیت‌های شدید تأخیر و مصرف انرژی، منجر به ظهور زیرشاخه‌ای تخصصی به نام بهینه‌سازی شبکه‌های عمیق برای محیط‌های نهفته (Deep Learning for Embedded Systems) شده است. تکنیک‌هایی مانند کوانتیزاسیون (Quantization)، هرس شبکه (Pruning) و استفاده از چارچوب‌هایی مانند TensorFlow Lite یا NVIDIA TensorRT برای تبدیل و بهینه‌سازی مدل‌ها برای اجرا روی واحدهای پردازش گرافیکی نهفته (GPU) یا واحدهای پردازش عصبی (NPU) داخل ECUها، از مباحث داغ پژوهشی هستند (Han et al., ۲۰۱۶)؛ علاوه‌براین، مدیریت انرژی و قابلیت اطمینان در سطح سیستم موضوعی حیاتی است. با افزایش تعداد ECUها و قدرت پردازشی آن‌ها، مدیریت مصرف برق کل خودرو به یک چالش تبدیل شده است. استراتژی‌هایی مانند مدیریت توان پویا (Dynamic Power Management) که در آن برخی ECUها یا هسته‌های پردازشی در مواقع غیرضروری در حالت کم‌مصرف (Sleep Mode) قرار می‌گیرند، و نیز معماری‌های شبکه‌ی توان که از سیستم‌های چندولتاژی (۱۲V/۴۸V) پشتیبانی می‌کنند، از راه‌حل‌های مطرح هستند (Zhou et al., ۲۰۲۱). از منظر قابلیت اطمینان، تکنیک‌های تحمل پذیری خطا (Fault Tolerance) مانند استفاده از پردازنده‌های قفل‌قدم (Lockstep Processors)، مکانیسم‌های نظارت بر واچداگ (Watchdog) پیشرفته و طراحی سیستم‌های افزونه (Redundant Systems) برای عملکردهای ایمنی‌حیاتی (مانند فرمان‌برقی یا ترمزبرقی) به امری استاندارد تبدیل شده‌اند. به‌روزرسانی بیش‌ازهوا (OTA) نرم‌افزار نیز خود به یک مبحث مستقل و پیچیده تبدیل شده است. طراحی یک سیستم OTA امن و قابل اعتماد، مستلزم توجه به چالش‌هایی مانند مدیریت نسخه‌های نرم‌افزاری در ناهمگن‌ترین شبکه‌ی ممکن، تضمین یکپارچگی و صحت بسته‌های به‌روزرسانی حتی در صورت قطع ارتباط، و امکان بازگشت (Rollback) به نسخه‌ی پایدار در صورت بروز مشکل است. پیاده‌سازی چنین سیستم‌هایی نیازمند همکاری لایه‌ای از پروتکل‌های امنیتی، نرم‌افزار مدیریت به‌روزرسانی روی ECU و سرورهای ابری مطمئن است (Nilsson et al., ۲۰۱۷). در نهایت، اثرپذیری از فیزیک کوانتوم اگرچه در حال حاضر یک موضوع آینده‌نگرانه است، اما شروع به تأثیرگذاری کرده است. با افزایش قدرت محاسباتی، الگوریتم‌های رمزنگاری کلاسیک فعلی ممکن است در آینده‌ای نه‌چندان دور در برابر کامپیوترهای کوانتوم آسیب‌پذیر شوند. این امر لزوم تحقیق و مهاجرت به‌سوی رمزنگاری پساکوانتومی (Post-Quantum Cryptography) را برای محافظت از ارتباطات درون‌خودرویی و به‌روزرسانی‌های نرم‌افزاری در بلندمدت مطرح می‌سازد. این لایه‌های پیشرفته نشان می‌دهند که مباحث ECU از مهندسی کنترل سنتی فراتر رفته و در عمیق‌ترین لایه‌های علوم کامپیوتر، رمزنگاری و هوش مصنوعی نیز نفوذ کرده است.

مباحث عمیق‌تر پیرامون ECUها به‌سمت معماری‌های محاسباتی ناهمگن و پردازش در لبه (Edge Computing) در خودرو پیش می‌رود. با افزایش حجم داده‌های سنسورهای خودران (لیدار، رادار، دوربین)، انتقال تمامی این داده‌ها به یک واحد مرکزی برای

پردازش، به‌دلیل محدودیت پهنای باند شبکه و تأخیر غیرقابل‌تحمل، غیرعملی است. بنابراین، مفهوم پردازش سلسله‌مراتبی (Hierarchical Processing) مطرح می‌شود، جایی که ECUهای لبه‌ای (Edge ECUs) یا واحدهای حسگر هوشمند، ابتدا پردازش‌های اولیه و سنگین مانند فیلتر کردن، فشرده‌سازی و استخراج ویژگی‌ها را به‌صورت محلی انجام داده و تنها داده‌های پردازش‌شده یا اطلاعات با سطح انتزاع بالاتر را به کامپیوتر مرکزی ارسال می‌کنند. این امر نیازمند تخصیص بهینه‌ی وظایف (Task Allocation) بین واحدهای پردازشی با قابلیت‌های متفاوت (CPU، GPU، NPU، FPGA) در یک سیستم ناهمگن است (Chen et al., ۲۰۲۲). در کنار این، مهندسی همزمان سخت‌افزار-نرم‌افزار (Hardware-Software Co-Design) برای دستیابی به کارایی و بهره‌وری انرژی بهینه، ضرورتی انکارناپذیر است. در این پارادایم، معماری سخت‌افزاری ویژه‌کار (مانند شتاب‌دهنده‌های اختصاصی برای پردازش شبکه عصبی خاص) و نرم‌افزار آن به‌طور هم‌زمان و با درنظرگرفتن محدودیت‌های یکدیگر طراحی می‌شوند تا حداکثر کارایی از منابع محدود موجود استخراج شود. این رویکرد به‌ویژه برای الگوریتم‌های بینایی ماشین و پردازش زبان طبیعی در کاربردهای تعامل انسان-ماشین داخل خودرو حیاتی است. از سوی دیگر، شبیه‌سازی دیجیتال (Digital Twin) در طول چرخه‌ی عمر ECU در حال تبدیل شدن به یک ابزار کلیدی است. یک دوقلوی دیجیتال از ECU یا کل شبکه‌ی الکترونیکی خودرو، مدلی پویا و به‌هم‌پیوسته است که می‌توان از آن برای شبیه‌سازی، پیش‌بینی، عیب‌یابی و حتی بهینه‌سازی عملکرد در زمان واقعی استفاده کرد. این مدل می‌تواند رفتار ECU را تحت شرایط مختلف بارکاری، دمایی و وضعیت سلامت (State of Health) شبیه‌سازی کرده و به‌عنوان مثال، پیش‌بینی کند که یک الگوریتم خاص در دمای خاصی از کار می‌افتد یا خیر. همچنین، تأییدیه‌ی رسمی (Formal Verification) برای سیستم‌های بحرانی-ایمن، فراتر از آزمون‌های تجربی، در حال کسب توجه است. روش‌هایی مانند مدل چکینگ (Model Checking) و اثبات قضیه (Theorem Proving) برای اثبات ریاضیاتی صحت الگوریتم‌های کنترلی پیچیده (مانند الگوریتم‌های اجتناب از برخورد) در برابر مجموعه‌ای از مشخصات (Specifications) فرمال به‌کار گرفته می‌شوند تا اطمینان حاصل شود که سیستم تحت هر شرایط ممکن، رفتاری ایمن خواهد داشت (Alur, ۲۰۱۵). در نهایت، مبحث پایداری زنجیره‌ی تأمین و امنیت سخت‌افزار نیز با توجه به بحران‌های جهانی، اهمیت یافته است. اطمینان از یکنواختی و کیفیت میکروکنترلرها در طول تولید انبوه، محافظت در برابر حملات سخت‌افزاری مانند حملات کانال جانبی (Side-Channel Attacks) برای استخراج کلیدهای رمزنگاری و اطمینان از عدم وجود درپشت‌درهای سخت‌افزاری (Hardware Trojans) در تراشه‌های تأمین‌شده از فروشندگان مختلف، به حوزه‌های تحقیقاتی فعال تبدیل شده‌اند. این لایه‌های پیچیده نشان می‌دهند که آینده‌ی توسعه‌ی ECUها در گرو همگرایی عمیق‌تر بین تخصص‌هایی است که پیش از این مجزا تصور می‌شدند.

با توجه به محدودیت دسترسی به اطلاعات جزئی و محرمانه‌ی معماری سخت‌افزاری و نرم‌افزاری ECUهای اختصاصی هر خودرو، جدول زیر بر اساس اطلاعات فنی منتشرشده، ادعاهای سازندگان و تحلیل‌های کارشناسی معتبر از رویکرد کلی و فناوری‌های کلیدی به‌کارگرفته‌شده در مدل‌هایی تنظیم شده است.

جدول ۱. بررسی ECUهای اختصاصی برخی از بهترین خودروهای جهان

خودرو / سازنده	رویکرد کلیدی معماری الکترونیکی	فناوری‌های شاخص مرتبط با ECU	پردازنده / سکوی محاسباتی مرکزی	اهداف عملکردی و تمایزات
تسلا مدل اس / ایکس / رودستر	متمرکزسازی شدید. کمترین تعداد ECU با ابرکامپیوتر مرکزی.	ECU مرکزی: "Hardware ٤" با تراشه‌های اختصاصی تسلا (D١ برای آموزش، FSD برای استنتاج). شبکه: اترنت خودرویی ١٠ گیگابیت. به‌روزرسانی: OTA عمیق و کامل.	سکوی اختصاصی تسلا با پردازنده‌های FSD (بیش از ٢٠٠ TOPS)، پردازنده‌های AMD برای اینفوتینمنت.	یکپارچه‌سازی بی‌نظیر سخت‌افزار و نرم‌افزار. توانایی اضافه کردن قابلیت‌های کامل (مانند خودران) از طریق OTA. کاهش پیچیدگی سیم‌کشی.
مرسدس بنز / EQSکلاس S	معماری مبتنی‌بر دامنه‌های بسیار یکپارچه با کامپیوتر مرکزی.	MBUX Hyperscreen:یک ECU گرافیکی/صوتی فوق‌پیشرفته. سیستم: MB.OS	چندین SoC قدرتمند (احتمالاً از سازندگانی مانند NVIDIA یا	تمرکز بر تجربه‌ی بی‌درز و لوکس کاربری (UI/UX). امنیت و قابلیت اطمینان سطح بالا. آماده‌سازی

		(سیستم عامل اختصاصی). شبکه: بستر ارتباطی یکپارچه با پهنای باند بالا.	(Qualcomm) برای دامنه‌های مختلف.	برای عملکردهای خودران سطح بالا.
بی‌ام‌دابلیو iX / سری ۷	معماری "خوشه‌ای" با کامپیوترهای مرکزی قدرتمند و ECUهای منطقه‌ای.	iDrive ۸: واحد محاسباتی و نمایشگر یکپارچه. شبکه: اترنت و CAN FD. پردازش: پلتفرم اختصاصی برای رانندگی خودکار و کمک راننده.	پلتفرم Qualcomm Snapdragon یا NVIDIA برای اینفوتینمنت و واحدهای پردازش خودران.	تعادل بین عملکرد پیشرانه‌ای، راحتی و تجربه‌ی دیجیتال. قابلیت شخصی‌سازی گسترده. ادغام حسگرها برای سیستم‌های پیشرفته.
پورشه تایکان	معماری الکتریکی/الکترونیکی (E/E) کاملاً جدید با تمرکز بر عملکرد و کارایی.	معماری E/E: بستر جدید با هسته‌های پردازشی مرکزی. سیستم‌عامل: مبتنی‌بر VW Group (سهم‌دار پورشه). خنک‌کاری: سیستم مدیریت حرارتی پیشرفته برای ECUها.	واحدهای پردازشی قدرتمند متمرکز، احتمالاً از خانواده‌ی AUDI/VW.	اولویت دادن به زمان‌بندی بلادرنگ و عملکرد دینامیکی (مانند کنترل کشش و تعلیق فعال). یکپارچه‌سازی عمیق با مدیریت باتری ۸۰۰ ولتی.
رولز رویس اسپکتر	معماری انعطاف‌پذیر و بسیار پیچیده با تأکید بر بی‌نقصی و سفارشی‌سازی.	Architecture of Luxury: چارچوب آلومینیمی که میزبان شبکه‌ی الکتریکی/الکترونیکی پیچیده است. تأکید: بر قابلیت اطمینان مطلق، نویزگیری و عملکرد آرام.	ترکیبی از ECUهای با درجه‌ی کیفی بسیار بالا از تأمین‌کنندگان منتخب، با پردازنده‌های قدرتمند.	دستیابی به "سکوت الکترونیکی" و عیب‌ناپذیری قابل‌لمس. امکان یکپارچه‌سازی سامانه‌های سفارشی‌شده‌ی مشتری در شبکه.
ریمک ناورا	ادغام عمیق سیستم‌های الکتریکی پرتوان با الکترونیک کنترل.	ECUهای سفارشی: برای مدیریت موتورهای چهارگانه، باتری kWh۱۲۰ و سیستم توربوکولر. پردازش: واحدهای اختصاصی برای کنترل کشش و پایداری در توان بسیار بالا.	ترکیبی از پردازنده‌های با کارایی بالا و مبتنی‌بر FPGA برای کنترل زمان‌واقعی موتورها.	کنترل بی‌نقص و هماهنگ توان ۱۹۱۴ اسب بخاری. اولویت قاطع بر عملکرد و کارایی انتقال قدرت، با یکپارچه‌سازی هوشمند الکترونیک قدرت و کنترل.
لوکال موتورز ایریا	رویکرد ماژولار و نرم‌افزار-محور با استانداردهای باز.	پلتفرم توسعه: مبتنی‌بر استانداردهای AUTOSAR و فریم‌ورک‌های متن‌باز. اتصال: تمرکز بر APIهای باز و امکان توسعه‌ی نرم‌افزار توسط جامعه.	استفاده از پلتفرم‌های استاندارد صنعتی (مانند NVIDIA Drive) برای تسهیل توسعه.	ایجاد اکوسیستمی برای نوآوری باز. کاهش وابستگی به تأمین‌کنندگان انحصاری. امکان ارتقا و شخصی‌سازی آسان توسط مالک.

جمع‌بندی تحلیلی: مقایسه نشان می‌دهد که رویکردها از تمرکزگرایی افراطی و یکپارچگی عمودی (تسلا) تا توزیع‌شدگی پیچیده با تمرکز بر لوکس و قابلیت اطمینان (رولز رویس) در نوسان است. مرسدس و بی‌ام‌دبلیو یک راه‌حل میانه با کامپیوترهای مرکزی قدرتمند اما در چارچوب سنتی‌تر ارائه می‌دهند. پورشه و ریمک نشان‌دهنده‌ی تخصص‌گرایی شدید در ادغام الکترونیک با پلتفرم‌های پیشرانه‌ی افراطی هستند. در نهایت، لوکال موتورز نماینده‌ی یک پارادایم کاملاً متفاوت مبتنی‌بر "باز بودن" است. انتخاب هر معماری، بازتاب مستقیمی از فلسفه‌ی کلی، بازار هدف و استراتژی فناوری هر سازنده است. روند کلی صنعت، اگرچه با سرعت‌های متفاوت، به سمت کاهش تعداد ECUهای تخصصی و حرکت به سمت کامپیوترهای مرکزی قدرتمند و نرم‌افزار-محور است.

پیشینه پژوهش

تکامل واحد کنترل الکترونیکی (ECU) به‌صورت مستقیم با پیشرفت فناوری‌های نیمه‌هادی، الزامات قانونی و انتظارات عملکردی خودروها گره خورده است. نخستین نمونه‌های عملیاتی ECUها در دهه‌ی ۱۹۷۰ میلادی و با معرفی سیستم‌های کنترل الکترونیکی

جرقه (Electronic Spark Controlو سپس کنترل الکترونیکی سوخت (EFI) ظهور کردند. این سیستم‌های اولیه مبتنی‌بر مدارهای مجتمع ساده با قابلیت پردازش محدود بودند و عمدتاً یک وظیفه‌ی واحد را انجام می‌دادند (Robert Bosch GmbH, ۲۰۱۸). تحول واقعی در دهه‌ی ۱۹۸۰ با معرفی ریزپردازنده‌ها و به‌ویژه استانداردسازی شبکه‌ی CAN (Controller Area Network) توسط بوش در سال ۱۹۸۶ رخ داد. استاندارد CAN امکان ارتباط قابل‌اطمینان و زمان‌مند بین واحدهای کنترل پراکنده را فراهم کرد و سنگ‌بنای معماری توزیع‌شده‌ی الکترونیک خودرو را بنا نهاد (Leen & Heffernan, ۲۰۰۲). در دهه‌ی ۱۹۹۰ و ۲۰۰۰، افزایش قوانین سخت‌گیرانه‌ی آلایندگی و ایمنی (مانند استانداردهای یورو و الزامات کیسه‌هوا) و همچنین تقاضای بازار برای راحتی و عملکرد، منجر به افزایش تصاعدی تعداد و پیچیدگی ECUها شد. این دوره شاهد ظهور سیستم‌های یکپارچه‌ای مانند کنترل پایداری الکترونیکی (ESC) بود که نیاز به همکاری نزدیک چندین حسگر و ECU داشت. افزایش پیچیدگی، چالش‌های جدیدی در مهندسی نرم‌افزار و یکپارچه‌سازی ایجاد کرد که پاسخ آن در قالب معرفی چارچوب استاندارد AUTOSAR (اتوموتیو اوپن سیستم آرکیتکتچر) در سال ۲۰۰۳ ظاهر شد. هدف AUTOSAR جداسازی نرم‌افزار از سخت‌افزار و ایجاد قابلیت استفاده‌ی مجدد و مقیاس‌پذیری در توسعه‌ی نرم‌افزارهای خودرویی بود (AUTOSAR Partnership, ۲۰۲۱). هم‌زمان، پژوهش‌های آکادمیک و صنعتی بر روی بهبود روش‌های طراحی و اعتبارسنجی متمرکز شد. رویکرد توسعه‌ی مبتنی‌بر مدل (Model-Based Design) با استفاده از ابزارهایی مانند MATLAB/Simulink به‌عنوان پارادایم غالب برای طراحی الگوریتم‌های کنترلی پیچیده و تولید کد مورد پذیرش قرار گرفت (Broy et al., ۲۰۱۲). با ورود به عصر اتصال‌پذیری و خودران‌سازی در دهه‌ی ۲۰۱۰ به‌بعد، چالش‌های تحقیقاتی جدیدی مطرح شد. محدودیت‌های شبکه‌های سنتی مانند CAN از نظر پهنای باند و امنیت، پژوهش‌ها را به سمت پروتکل‌های جدیدی مانند اترنت خودرویی (Automotive Ethernet) سوق داد. مطالعاتی مانند پژوهش‌های ناوه و همکاران به‌طور گسترده به تحلیل مقایسه‌ای و آینده‌نگاری شبکه‌های درون‌خودرویی پرداختند (Navet et al., ۲۰۱۷). از سوی دیگر، افزایش حملات سایبری به خودروهای متصل، حوزه‌ی امنیت سایبری خودرو را به یک زمینه‌ی پژوهشی حیاتی تبدیل کرد. کار پیشگامانه‌ی کوچر و همکاران در سال ۲۰۱۰ که با نفوذ به یک خودروی مدرن آسیب‌پذیری‌های گسترده‌ای را نشان داد، تأثیر عمیقی بر جهت‌گیری پژوهش‌های بعدی در زمینه‌ی ایمنی‌سازی شبکه‌های ارتباطی و معماری ECU گذاشت (Koscher et al., ۲۰۱۰). در سال‌های اخیر، تمرکز اصلی تحقیقات بر روی مدیریت پیچیدگی فزاینده از طریق تحول در معماری است. مفهوم ادغام عملکردها در کامپیوترهای مرکزی قدرتمند به‌جای ده‌ها ECU تخصصی، موضوع مطالعاتی مقالاتی همچون پژوهش ژنگ و همکاران بوده است که به بررسی معماری‌های متمرکز و مبتنی‌بر دامنه برای خودروهای متصل و خودران پرداخته‌اند (Zheng et al., ۲۰۲۰). همچنین، با ورود یادگیری ماشین به حوزه‌ی خودرو، چگونگی استقرار کارآمد و ایمن مدل‌های عصبی بر روی سخت‌افزارهای نهفته‌ی خودرویی (Edge AI) به یک خط پژوهشی فعال تبدیل شده است. اگرچه پیشینه‌ی پژوهش نشان‌دهنده‌ی پیشرفت‌های خارق‌العاده است، اما شکاف‌های دانشی مهمی در زمینه‌ی روش‌های رسمی برای تضمین صحت سیستم‌های هوشمند، چارچوب‌های یکپارچه برای مهندسی هم‌زمان سخت‌افزار-نرم‌افزار در معماری‌های متمرکز و پروتکل‌های ارتباطی کاملاً امن و قابل‌اطمینان برای خودروهای خودران سطح ۴ و ۵ وجود دارد که پژوهش حاضر در پی پرداختن به آن‌ها است.

پژوهش‌های گسترده‌ای در حوزه‌ی واحدهای کنترل الکترونیکی (ECU) خودرو را می‌توان در چندین محور اصلی طبقه‌بندی کرد. محور نخست، بهینه‌سازی و اعتبارسنجی نرم‌افزار است. با افزایش حجم کد نرم‌افزاری در ECUها، روش‌های توسعه‌ی مبتنی‌بر مدل (MBD) به‌صورت گسترده مورد مطالعه و بکارگیری قرار گرفته‌اند. در این زمینه، پژوهش‌هایی مانند کار بروی و همکاران به تحلیل مزایای MBD در کاهش خطاها و تسهیل تولید کد خودکار پرداخته‌اند (Broy et al., ۲۰۱۲). استاندارد AUTOSAR نیز به‌عنوان چارچوبی برای مدیریت این پیچیدگی، موضوع تحقیقات بسیاری بوده است؛ برای نمونه، مطالعات ماکر و همکاران به بررسی چالش‌های پیاده‌سازی و مزایای قابلیت استفاده‌ی مجدد مؤلفه‌های نرم‌افزاری در این چارچوب پرداخته‌اند (Macher et al., ۲۰۱۷).

محور دوم، شبکه‌های ارتباطی درون‌خودرویی است. در این حوزه، تحقیقات ابتدا بر روی تحلیل کارایی و قابلیت اطمینان شبکه‌ی CAN متمرکز بود. با گذر زمان و با افزایش نیاز به پهنای باند، پژوهش‌ها به‌سمت پروتکل‌های جدیدتر سوق یافت. ناوت و همکاران به‌طور جامعی مزایا، معماری و چالش‌های مهاجرت به شبکه‌های مبتنی‌بر اترنت خودرویی و FlexRay را بررسی کرده‌اند (Navet et al., ۲۰۱۷). محور سوم، امنیت سایبری است که پس از نمایش آسیب‌پذیری‌های عملی توسط کوچر و همکاران، به‌سرعت به یک زمینه‌ی پژوهشی فعال تبدیل شد. پژوهش‌های بعدی مانند مطالعه‌ی میلر و والِک بر راهکارهای تشخیص نفوذ مبتنی‌بر رفتار غیرعادی در شبکه‌ی CAN و همچنین استفاده از ماژول‌های امنیتی سخت‌افزاری (HSM) متمرکز شده‌اند (Miller & Valasek, ۲۰۱۵). محور چهارم، معماری‌های نوین الکترونیکی است. با توجه به محدودیت‌های معماری توزیع‌شده‌ی سنتی (با ده‌ها ECU مجزا)، پژوهش‌های کنونی به‌سمت طراحی معماری‌های متمرکز و مبتنی‌بر دامنه حرکت کرده‌اند. مطالعه‌ی ژنگ و همکاران به بررسی سیستماتیک این معماری‌های در حال ظهور، مزایای آن‌ها در کاهش وزن سیم‌کشی و پیچیدگی و چالش‌های مربوط به یکپارچه‌سازی و تأمین امنیت پرداخته است (Zheng et al., ۲۰۲۰). محور پنجم، کاربرد هوش مصنوعی و یادگیری ماشین بر روی ECU است. این حوزه‌ی نوظهور شامل تحقیقاتی در زمینه‌ی بهینه‌سازی و فشرده‌سازی مدل‌های عصبی برای اجرا بر روی سخت‌افزارهای نهفته با منابع محدود (همانند کار هان و همکاران در مورد فشرده‌سازی عمیق) و نیز تضمین عملکرد ایمن و قابل تفسیر این مدل‌ها در سیستم‌های بحرانی-ایمن است (Han et al., ۲۰۱۶). محور ششم، مدیریت انرژی و قابلیت اطمینان است. پژوهش‌هایی مانند کار ژو و همکاران استراتژی‌های مدیریت توان پویا را برای کل شبکه‌ی الکترونیکی خودرو، با هدف بهینه‌سازی مصرف انرژی بدون قربانی کردن عملکرد، تحلیل کرده‌اند (Zhou et al., ۲۰۲۱). علی‌رغم حجم عظیم پژوهش‌های صورت‌گرفته، شکاف‌های قابل‌توجهی در ادبیات موضوع مشاهده می‌شود. بسیاری از مطالعات به‌صورت جزیره‌ای و متمرکز بر یک لایه (مثلاً فقط شبکه یا فقط نرم‌افزار) انجام شده‌اند. پژوهش‌های جامع چندلایه‌ای که هم‌زمان به بهینه‌سازی و یکپارچه‌سازی سخت‌افزار، نرم‌افزار، شبکه و امنیت در قالب یک چارچوب سیستماتیک برای معماری‌های متمرکز آینده بپردازند، همچنان محدود هستند. به‌علاوه، روش‌های رسمی برای تأییدیه‌ی سیستم‌های هوشمند و خود-تطبیقی که در ECUهای نسل آینده مستقر خواهند شد، در مراحل اولیه‌ی تحقیق قرار دارد.

دیتاها و آنالیزها

پژوهش‌های تجربی و تحلیلی متعددی داده‌های کمّی مهمی را در مورد عملکرد، امنیت و کارایی ECUها و شبکه‌های درون‌خودرویی ارائه کرده‌اند. در یک مطالعه‌ی تجربی پیش‌گامانه در حوزه‌ی امنیت، کُشر و همکاران (۲۰۱۰) با انجام یک حمله‌ی عملی بر روی یک خودروی مدرن، داده‌های مهمی را گردآوری کردند. آن‌ها نشان دادند که با دسترسی به شبکه‌ی داخلی خودرو (از طریق پورت OBD-II یا حتی از راه‌دور)، می‌توان فرامین مخربی را به ECUها تزریق کرد؛ برای مثال، توانستند به‌طور کامل ترمزهای یک خودروی درحال‌حرکت را از کار انداخته یا فرمان را قفل کنند. تحلیل داده‌های ترافیک شبکه در این تحقیق، آسیب‌پذیری ذاتی پروتکل CAN در برابر حملات جعل و تکرار (Spoofing & Replay) را به‌وضوح نشان داد. در حوزه‌ی شبکه، مطالعه‌ی تجربی بِی و همکاران (۲۰۱۸) بر روی تأخیر و قابلیت اطمینان بسترهای ارتباطی مختلف، داده‌های مقایسه‌ای ارزشمندی ارائه کرد. اندازه‌گیری‌های آن‌ها روی یک پلتفرم آزمایشی نشان داد که در حالی که شبکه‌ی CAN با نرخ ۵۰۰ کیلوبیت بر ثانیه برای پیام‌های بحرانی-ایمن (مانند ترمز) تأخیری در حد ۲ تا ۱۰ میلی‌ثانیه دارد، شبکه‌ی اترنت خودرویی BASE-T۱۱۰۰ می‌تواند حجم داده‌های یک جریان ویدیویی با وضوح بالا را با تأخیر کمتر از ۳ میلی‌ثانیه منتقل کند، اما در عین‌حال نوسان تأخیر (Jitter) کم‌تری نیز دارد. این داده‌ها مهاجرت به اترنت را برای دامنه‌های اطلاعات-سرگرمی و ADAS توجیه‌پذیر می‌کند. از سوی دیگر، پژوهش کِی و

همکاران (۲۰۱۹) بر روی بهینه‌سازی مصرف انرژی در ECUها، داده‌های جالبی را از طریق شبیه‌سازی ارائه داد. آن‌ها نشان دادند که با استفاده از یک الگوریتم زمان‌بندی پویای وظایف و انتقال حالت‌های خواب (Sleep States) در یک ECU چندهسته‌ای، می‌توان مصرف انرژی را در یک چرخه‌ی رانندگی ترکیبی تا ۲۳٪ کاهش داد بدون آن‌که تأخیر در انجام وظایف بحرانی از آستانه‌ی مجاز فراتر رود. در زمینه‌ی استقرار یادگیری عمیق، مطالعه‌ی چن و همکاران (۲۰۲۱) داده‌های عملکردی دقیقی از اجرای یک شبکه‌ی عصبی کانولوشنی (CNN) برای تشخیص اشیا بر روی یک SoC خودرویی مجهز به واحد پردازش عصبی (NPU) در مقایسه با یک پردازنده‌ی چند هسته‌ای عمومی (CPU) ارائه کردند. نتایج آن‌ها حاکی از آن بود که NPU توانست زمان استنتاج (Inference Time) را تا ۱۵ برابر کاهش داده و مصرف انرژی را به‌ازای هر فریم تا ۹۴٪ بهبود بخشد. این داده‌ها به‌وضوح مزیت سخت‌افزارهای تخصص‌یافته را برای کاربردهای هوش مصنوعی در لبه نشان می‌دهد. همچنین، آنالیز داده‌های واقعی از سیستم‌های OTA توسط نیلسون و همکاران (۲۰۱۷) بر روی ناوگان خودروهای متصل، نشان داد که طراحی یک معماری امن برای به‌روزرسانی، می‌تواند نرخ موفقیت به‌روزرسانی‌ها را از زیر ۹۰٪ به بیش از ۹۹.۵٪ افزایش دهد و میانگین زمان دانلود و نصب یک به‌روزرسانی مهم را با استفاده از تکنیک‌های دیفرانسیلی (ارسال تنها تفاوت‌ها) تا ۶۰٪ کاهش دهد. این داده‌ها بر اهمیت تحقیقات در زمینه‌ی بهینه‌سازی مکانیزم‌های انتشار نرم‌افزار تأکید می‌کنند. در نهایت، مطالعه‌ی شبیه‌سازی گسترده‌ی پارک و همکاران (۲۰۲۲) بر روی یک معماری مرکزی (Zone-Oriented) نشان داد که این معماری در مقایسه با معماری توزیع‌شده‌ی سنتی، می‌تواند طول کل سیم‌کشی را تا ۴۰٪، وزن سیستم برق‌رسانی را تا ۳۰ کیلوگرم و تعداد اتصالات را تا صدها مورد کاهش دهد. با این حال، داده‌های این شبیه‌سازی همچنین هشدار داد که بار پردازشی و حرارتی روی کامپیوترهای مرکزی منطقه‌ای می‌تواند به‌طور قابل‌توجهی متمرکز شده و نیازمند راهکارهای خنک‌کاری و مدیریت حرارتی پیشرفته‌تری است.

تحلیل داده‌های عمیق‌تر در حوزه‌ی امنیت سایبری نشان می‌دهد که حملات پیشرفته‌تر، لایه‌های جدیدی از آسیب‌پذیری را آشکار می‌کنند. مطالعه‌ی تجربی و تحلیل داده‌های واقعی توسط پچ و همکاران (۲۰۲۰) بر روی حملات کانال جانبی (Side-Channel Attacks) به ماژول‌های امنیتی سخت‌افزاری (HSM) در ECUها نشان داد که با اندازه‌گیری دقیق مصرف برق یا انتشار الکترومغناطیسی در حین اجرای عملیات رمزنگاری، می‌توان کلیدهای رمزنگاری را با دقت بیش از ۹۵٪ در کمتر از ۱۰۰۰ نمونه‌برداری استخراج کرد. این داده‌ها به‌وضوح نشان می‌دهد که پیاده‌سازی امن‌سازی صرفاً در سطح منطقی و نرم‌افزاری کافی نیست و به محافظت‌های فیزیکی پیشرفته‌تری نیاز است. از منظر قابلیت اطمینان، جمع‌آوری و تحلیل داده‌های میدانی از خرابی‌های ECU در ناوگان واقعی توسط ژانگ و همکاران (۲۰۲۱) بینش مهمی ارائه کرد. داده‌های آن‌ها از بیش از ۱۰۰۰۰۰ خودرو در یک بازه‌ی ۵ ساله نشان داد که نرخ خرابی زودهنگام (Early Failure Rate) ECUها با دمای کاری متوسط موتور و تعداد چرخه‌های روشن/خاموش شدن (Power Cycles) همبستگی مثبت قوی دارد. به‌طور مشخص، ECUهای نصب‌شده در محفظه‌ی موتور (با دمای کاری متوسط بالای ۱۰۵ درجه سانتی‌گراد) نرخ خرابی ۲.۳ برابری نسبت به ECUهای نصب‌شده در کابین داشتند. این داده‌ها لزوم طراحی مکانیزم‌های خنک‌کاری مؤثر و انتخاب قطعات با درجه‌ی کیفی مناسب برای محیط‌های خشن را تأیید می‌کند. در زمینه‌ی شبکه، آنالیز داده‌های ترافیک واقعی شبکه‌های CAN توسط مِیر و همکاران (۲۰۱۹) برای توسعه‌ی سیستم‌های تشخیص نفوذ مبتنی‌بر یادگیری ماشین مورد استفاده قرار گرفت. آن‌ها با ثبت بیش از ۵۰۰ ساعت داده‌ی ترافیک طبیعی و تزریق حملات شبیه‌سازی‌شده، مجموعه‌داده‌ای ایجاد کردند و نشان دادند که مدل‌های مبتنی‌بر جنگل تصادفی (Random Forest) می‌توانند حملات انکار سرویس (DoS) و تزریق فریم (Frame Injection) را با دقت ۹۹.۲٪ و نرخ هشدار کاذب کمتر از ۰.۱٪ تشخیص دهند. این داده‌ها پتانسیل بالای هوش مصنوعی را برای نظارت امنیتی بلادرنگ نشان می‌دهد. در حوزه‌ی عملکرد سخت‌افزار، بنچمارک‌های دقیق انجام‌شده توسط گومز و همکاران (۲۰۲۲) بر روی نسل جدید پردازنده‌های چند هسته‌ای مبتنی‌بر معماری ARM Cortex-R۵۲+که برای کاربردهای ایمنی-حیاتی طراحی شده‌اند، داده‌های ارزشمندی ارائه کردند. نتایج نشان داد که

استفاده از قفل‌قدم سخت‌افزاری (Lockstep) با پیکربندی Dual-Core Lockstep، نرخ تشخیص خطای واحد (Single Event Upset) ناشی از تشعشعات را به بیش از ۹۹.۹۹٪ می‌رساند، اما این افزونگی، مصرف توان پردازنده را تا ۴۰٪ افزایش می‌دهد و فرکانس کاری آن را حدود ۲۰٪ محدود می‌کند. این داده‌ها تجسم ملموسی از بهای دستیابی به سطح بالای ایمنی (ASIL-D) ارائه می‌دهند. همچنین، شبیه‌سازی‌های پیش‌بین در مطالعه‌ی لیو و همکاران (۲۰۲۳) درباره‌ی معماری‌های کاملاً متمرکز (Vehicle Computer) حاکی از آن است که پردازنده‌های مرکزی نسل آینده برای پشتیبانی از خودران سطح ۴، ممکن است به توان پردازشی بیش از ۱۰۰۰ TOPS و پهنای باند حافظه‌ای بیش از ۲۰۰ گیگابایت بر ثانیه نیاز داشته باشند. داده‌های این پژوهش بر شکاف فناورانه‌ی کنونی بین سخت‌افزارهای موجود و نیازهای آتی تأکید دارد و لزوم نوآوری در معماری‌های محاسباتی ناهمگن و حافظه‌های پهن‌باند را برجسته می‌سازد.

نتیجه‌گیری و پیشنهادها

نتیجه‌گیری

واحد کنترل الکترونیکی (ECU) از یک کنترل‌کننده‌ی تخصصی و منفرد به هسته‌ی مرکزی یک سیستم سایبر-فیزیکی فوق‌پیچیده تحول یافته است که تعیین‌کننده‌ی عملکرد، ایمنی، امنیت و تجربه‌ی کاربری خودروی مدرن است. این مقاله نشان داد که سیر تکامل ECUها در پاسخ به سه محرک اصلی قوانین سخت‌گیرانه‌ی زیست‌محیطی و ایمنی، تقاضای بازار برای قابلیت‌های نوین و انقلاب دیجیتال صورت گرفته و اکنون در آستانه‌ی یک گذار پارادایمی دیگر قرار دارد. معماری توزیع‌شده‌ی مبتنی‌بر ده‌ها ECU ناهمگن و شبکه‌های ارتباطی سنتی مانند CAN، با وجود خدمت‌رسانی قابل‌توجه، به‌دلیل پیچیدگی فزاینده، محدودیت‌های امنیتی و موانع توسعه‌ی نرم‌افزاری، به مرزهای خود نزدیک شده‌اند. داده‌های تجربی و تحلیلی بررسی‌شده به‌وضوح مزایای کمّی حرکت به سمت معماری‌های متمرکز با کامپیوترهای مرکزی قدرتمند و شبکه‌های اترنت پهن‌باند را در کاهش وزن، پیچیدگی سیم‌کشی و بهبود قابلیت توسعه نشان می‌دهند. با این حال، این انتقال چالش‌های بنیادین جدیدی را در زمینه‌های امنیت سایبری چندلایه، مدیریت انرژی و حرارتی سامانه‌های محاسباتی فشرده، تضمین قابلیت اطمینان زیرسیستم‌های بحرانی-ایمن در یک محیط یکپارچه‌شده، و استقرار ایمن و کارآمد الگوریتم‌های هوش مصنوعی به‌وجود آورده است. به‌علاوه، وابستگی روزافزون به نرم‌افزار و اتصال‌پذیری، خودرو را به یک موجودیت زنده‌ی دیجیتال تبدیل کرده که نیازمند چرخه‌ی عمر کامل توسعه، استقرار و نگهداری مبتنی‌بر DevOps و مداوم‌سازی یکپارچه (CI/CD) است. بنابراین، آینده‌ی صنعت خودرو در گرو توانایی در مدیریت این پیچیدگی ذاتی از طریق رویکردهای میان‌رشته‌ای نوآورانه است.

پیشنهادها برای پژوهش‌ها و کاربردهای آینده

۱. توسعه‌ی چارچوب‌های طراحی و اعتبارسنجی مبتنی‌بر دوقلوهای دیجیتال (Digital Twins) برای کل معماری E/E: پیشنهاد می‌شود یک مدل دینامیک و همه‌جانبه از سخت‌افزار، نرم‌افزار و ارتباطات خودرو ایجاد شود که امکان شبیه‌سازی، پیش‌بینی رفتار، بهینه‌سازی و عیب‌یابی را در طول چرخه‌ی عمر کامل، از مرحله‌ی طراحی مفهومی تا بازنشستگی، فراهم کند.

۲. پژوهش در زمینه‌ی سخت‌افزارهای محاسباتی امن، ناهمگن و قابل‌اطمینان: تمرکز بر طراحی سیستم‌های روی تراشه (SoC) با بخش‌های پردازشی تخصصی (CPU, GPU, NPU, FPGA) که از نظر فیزیکی از یکدیگر جداسازی شده‌اند، مجهز به مکانیزم‌های مقاوم در برابر حملات کانال جانبی بوده و از معماری‌های تحمل‌پذیر خطا برای دستیابی به سطوح بالای ASIL پشتیبانی می‌کنند.

۳. ایجاد استانداردها و پروتکل‌های ارتباطی یکپارچه و ذاتاً امن برای معماری‌های متمرکز: ضرورت دارد پروتکل‌های جدیدی توسعه یابند که به‌طور ذاتی و در لایه‌ی فیزیکی/پیونددادهه، ویژگی‌های امنیتی مانند احراز هویت، محرمانگی و جامعیت را برای ارتباط بین واحدهای مرکزی، ECUهای منطقه‌ای و حسگرها/عملگرها تضمین کنند.

۴. تدوین روش‌های رسمی (Formal Methods) برای تأیید و تصدیق سیستم‌های خود-تطبیق و مبتنی‌بر یادگیری ماشین: با توجه به غیرقطعی بودن رفتار برخی الگوریتم‌های هوش مصنوعی، پیشنهاد می‌گردد روش‌های ریاضیاتی برای اثبات رفتار ایمن این سیستم‌ها تحت تمامی سناریوهای ممکن (یا یک زیرمجموعه‌ی قابل‌اثبات) توسعه و در چارچوبی مانند ISO ۲۱٤٤۸ (SOTIF) ادغام شوند.

۵. معماری‌های نرم‌افزاری مبتنی‌بر میکروسرویس و کانتینر برای خودرو: تحقیق بر روی امکان‌سنجی و پیاده‌سازی معماری‌های نرم‌افزاری بسیار ماژولار و مستقل از سخت‌افزار که امکان به‌روزرسانی، گسترش و مدیریت چابک قابلیت‌های نرم‌افزاری را حتی پس از تحویل خودرو به مشتری فراهم می‌آورد.

۶. راهکارهای مدیریت حرارت و انرژی در سطح سیستم برای مراکز داده‌ی متحرک (Vehicle Data Centers): پژوهش‌های کاربردی بر روی سیستم‌های خنک‌کاری پیشرفته (مانند خنک‌کاری مایع مستقیم تراشه)، تکنیک‌های کاهش توان پویا و معماری‌های تأمین توان بهینه‌شده برای محاسبات مرکزی پرتوان ضروری است.

۷. ایجاد اکوسیستم‌های آزمایش و ارزیابی مجازی مشترک (Shared Virtual Proving Grounds): پیشنهاد می‌شود پلتفرم‌های شبیه‌سازی استانداردشده‌ای ایجاد شوند که در آن سازندگان خودرو، تأمین‌کنندگان و محققان بتوانند عملکرد، امنیت و قابلیت همکاری راه‌حل‌های نرم‌افزاری و سخت‌افزاری نوین را در یک محیط مجازی غنی و مبتنی‌بر سناریوهای واقعی ارزیابی کنند.

مراجع

[۱] Broy, M., et al. (۲۰۱۲). Engineering Automotive Software. Proceedings of the IEEE, ۱۰۰(۲), ٤٥۸-٤٧٤.

[۲] Macher, G., et al. (۲۰۱۷). A Systematic Review of Automotive Software Engineering Frameworks. Journal of Systems and Software, ۱۲۸, ۲٥-٤۲.

[۳] Navet, N., et al. (۲۰۱۷). Vehicle Electronics and Architectures: Automotive Networks. In Handbook of Automotive Electronics (pp. ٤٥-۸۹). CRC Press.

[٤] Robert Bosch GmbH. (۲۰۱۸). Automotive Handbook (۱۰th ed.). Wiley..

[٥] AUTOSAR Partnership. (۲۰۲۱). *AUTOSAR Classic Platform Release ۲۱-۱۱*. https://www.autosar.org

[٦] Freescale Semiconductor. (۲۰۱٥). Automotive Microcontrollers and Processors: Technical Reference Manual.

[۷] Heywood, J. B. (۲۰۱۸). Internal Combustion Engine Fundamentals (۲nd ed.). McGraw-Hill Education.

[۸] Koscher, K., et al. (۲۰۱۰). Experimental Security Analysis of a Modern Automobile. IEEE Symposium on Security and Privacy, ٤٤۷-٤٦۲.

[۹] Navet, N., et al. (۲۰۱۷). Vehicle Electronics and Architectures: Automotive Networks. In Handbook of Automotive Electronics (pp. ٤٥-۸۹). CRC Press.

[۱۰] Winner, H., et al. (Eds.). (۲۰۱٦). Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort. Springer.

[۱۱] Zheng, Y., et al. (۲۰۲۰). A Survey on In-Vehicle Network Architecture for Connected and Automated Vehicles. IEEE Transactions on Intelligent Transportation Systems, ۲۱(۷), ۲۷۹٤-۲۸۰۸.

[۱۲] AUTOSAR Partnership. (۲۰۲۱). *AUTOSAR Classic Platform Release ۲۱-۱۱*. https://www.autosar.org

[۱۳] ISO ۲۶۲۶۲. (۲۰۱۸). Road vehicles – Functional safety (۲nd ed.). International Organization for Standardization.

[۱٤] Koscher, K., et al. (۲۰۱۰). Experimental Security Analysis of a Modern Automobile. IEEE Symposium on Security and Privacy, ٤٤٧-٤٦٢.

[۱٥] Macher, G., et al. (۲۰۱۷). A Systematic Review of Automotive Software Engineering Frameworks. Journal of Systems and Software, ۱۲۸, ۲٥-٤۲.

[۱٦] Navet, N., et al. (۲۰۱۷). Vehicle Electronics and Architectures: Automotive Networks. In Handbook of Automotive Electronics (pp. ٤٥-۸۹). CRC Press.

[۱۷] Zheng, Y., et al. (۲۰۲۰). A Survey on In-Vehicle Network Architecture for Connected and Automated Vehicles. IEEE Transactions on Intelligent Transportation Systems, ۲۱(۷), ۲۷۹٤-۲۸۰۸.

[۱۸] Han, S., et al. (۲۰۱٦). Deep Compression: Compressing Deep Neural Networks with Pruning, Trained Quantization and Huffman Coding. International Conference on Learning Representations (ICLR).

[۱۹] Nilsson, D. K., et al. (۲۰۱۷). A Framework for Over-the-Air Software Updates in Vehicles. IEEE Vehicular Networking Conference (VNC), ۸۳-۹۰.

[۲۰] Zhou, Y., et al. (۲۰۲۱). A Comprehensive Review of Energy Management Strategies for Electric Vehicles. Renewable and Sustainable Energy Reviews, ۱٤۷, ۱۱۱۱۹۰.

[۲۱] Alur, R. (۲۰۱٥). Principles of Cyber-Physical Systems. The MIT Press.

[۲۲] Chen, X., et al. (۲۰۲۲). Task Allocation for Collaborative Edge Computing in Autonomous Vehicles: A Survey. IEEE Transactions on Intelligent Vehicles, ۷(۲), ٤۷۲-٤۸۹.

[۲۳] AUTOSAR Partnership. (۲۰۲۱). *AUTOSAR Classic Platform Release ۲۱-۱۱*. https://www.autosar.org

[۲٤] Broy, M., et al. (۲۰۱۲). Engineering Automotive Software. Proceedings of the IEEE, ۱۰۰(۲), ٤٥۸-٤۷٤.

[۲٥] Koscher, K., et al. (۲۰۱۰). Experimental Security Analysis of a Modern Automobile. IEEE Symposium on Security and Privacy, ٤٤٧-٤٦۲.

[۲٦] Leen, G., & Heffernan, D. (۲۰۰۲). Expanding Automotive Electronic Systems. Computer, ۳٥(۱), ۸۸-۹۳.

[۲۷] Navet, N., et al. (۲۰۱۷). Vehicle Electronics and Architectures: Automotive Networks. In Handbook of Automotive Electronics (pp. ٤٥-۸۹). CRC Press.

[۲۸] Robert Bosch GmbH. (۲۰۱۸). Automotive Handbook (۱۰th ed.). Wiley.

[۲۹] Zheng, Y., et al. (۲۰۲۰). A Survey on In-Vehicle Network Architecture for Connected and Automated Vehicles. IEEE Transactions on Intelligent Transportation Systems, ۲۱(۷), ۲۷۹٤-۲۸۰۸.

[۳۰] Broy, M., et al. (۲۰۱۲). Engineering Automotive Software. Proceedings of the IEEE, ۱۰۰(۲), ٤٥۸-٤۷٤.

[۳۱] Han, S., et al. (۲۰۱٦). Deep Compression: Compressing Deep Neural Networks with Pruning, Trained Quantization and Huffman Coding. International Conference on Learning Representations (ICLR).

[۳۲] Macher, G., et al. (۲۰۱۷). A Systematic Review of Automotive Software Engineering Frameworks. Journal of Systems and Software, ۱۲۸, ۲۵-٤۲.

[۳۳] Miller, C., & Valasek, C. (۲۰۱۵). Remote Exploitation of an Unaltered Passenger Vehicle. Black Hat USA.

[۳٤] Navet, N., et al. (۲۰۱۷). Vehicle Electronics and Architectures: Automotive Networks. In Handbook of Automotive Electronics (pp. ٤٥-۸۹). CRC Press.

[۳٥] Zheng, Y., et al. (۲۰۲۰). A Survey on In-Vehicle Network Architecture for Connected and Automated Vehicles. IEEE Transactions on Intelligent Transportation Systems, ۲۱(۷), ۲۷۹٤-۲۸۰۸.

[۳٦] Zhou, Y., et al. (۲۰۲۱). A Comprehensive Review of Energy Management Strategies for Electric Vehicles. Renewable and Sustainable Energy Reviews, ۱٤۷, ۱۱۱۱۹۰.

[۳۷] Baye, M., et al. (۲۰۱۸). Performance evaluation of CAN FD and automotive Ethernet for in-vehicle networks. IEEE Transactions on Vehicular Technology, ٦۷(۱۰), ۹۲٤٥-۹۲٥٦.

[۳۸] Chen, X., et al. (۲۰۲۱). Performance and Energy Evaluation of Embedded Deep Learning on Automotive Platforms. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, ٤۰(٥), ۹۳۷-۹٥۰.

[۳۹] Kay, S., et al. (۲۰۱۹). Dynamic Power Management for Multicore ECUs in Automotive Systems. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, ۲۷(٦), ۱٤۳۷-۱٤٤٦.

[٤۰] Koscher, K., et al. (۲۰۱۰). Experimental Security Analysis of a Modern Automobile. IEEE Symposium on Security and Privacy, ٤٤۷-٤٦۲.

[٤۱] Nilsson, D. K., et al. (۲۰۱۷). A Framework for Over-the-Air Software Updates in Vehicles. IEEE Vehicular Networking Conference (VNC), ۸۳-۹۰.

[٤۲] Park, J., et al. (۲۰۲۲). A Simulation-Based Study on Weight and Cost Reduction of Vehicle E/E Architecture Using Zonal Controllers. SAE International Journal of Connected and Automated Vehicles, ٥(۲), ۱۲۳-۱۳٥.

[٤۳] Gomez, A., et al. (۲۰۲۲). Benchmarking and Reliability Analysis of Multicore Lockstep Processors for ASIL-D Automotive Applications. IEEE Transactions on Device and Materials Reliability, ۲۲(۱), ۷۸-۸۹.

[٤٤] Liu, Y., et al. (۲۰۲۳). Computational Requirements Analysis for Level ٤ Autonomous Vehicle Central Computers: A Projection Study. IEEE Access, ۱۱, ۲۳٤٥٦-۲۳٤۷۰.

[٤٥] Meier, D., et al. (۲۰۱۹). CANet: An Intrusion Detection System for CAN Bus Based on Machine Learning. IEEE Transactions on Intelligent Transportation Systems, ۲۰(۹), ۳۳۳۷-۳۳٤٦.

[٤٦] Pech, L., et al. (۲۰۲۰). Practical Side-Channel Attacks on Automotive Hardware Security Modules. Proceedings of the USENIX Security Symposium, ۱٤٥۷-۱٤۷٤.

[٤۷] Zhang, H., et al. (۲۰۲۱). Field Failure Data Analysis of Automotive Electronic Control Units: A Large-Scale Fleet Study. Microelectronics Reliability, ۱۲٦, ۱۱٤۲٦۸.