Introduction to the Special Issue on Automotive CPS Safety & Security: Part 2

SAMARJIT CHAKRABORTY, University of North Carolina at Chapel Hill, Chapel Hill, North Carolina, USA
SOMESH JHA, University of Wisconsin–Madison, Madison Wisconsin, USA
SOHEIL SAMII, Linköping University, Linköping, Sweden
PHILIPP MUNDHENK, Robert Bosch GmbH, Renningen, Germany

ACM Reference Format:
Samarjit Chakraborty, Somesh Jha, Soheil Samii, and Philipp Mundhenk. 2024. Introduction to the Special Issue on Automotive CPS Safety & Security: Part 2. *ACM Trans. Cyber-Phys. Syst.* 8, 2, Article 10 (May 2024), 17 pages. https://doi.org/10.1145/3650210

1 INTRODUCTION

This special issue on automotive **Cyber-Physical Systems(CPS)** safety and security is a continuation of the special issue that appeared in *ACM Transactions on Cyber-Physical Systems*, Vol. 7, No. 1, in January 2023. It features a second set of seven articles, spanning across a variety of topics, such as electric and autonomous vehicles, automotive control, and in-vehicle networks, again with a focus on safety and security. To give an impression on how rich the research literature on this domain is, we provided a brief survey in Part 1 of this special issue. In Part 2, we continue that survey—once again, our goal is not to exhaustively list all of the problems that have been addressed in this area but to provide a larger context for the seven articles featured here.

In particular, we would like to highlight that the domain of automotive CPS is currently undergoing a major transition. Not only are we witnessing technological revolutions in **Electric Vehicles (EVs)** [1, 90, 91, 166] and autonomous vehicles [15, 97], both of which have major societal and environmental implications, but also the automotive industry is embracing new technologies and design flows at a very rapid pace. These include changes in in-vehicle **Electrical/Electronic (E/E)** architectures, greater connectivity between vehicles, between vehicles and infrastructure, and reliance on vehicle-to-cloud connectivity [2, 176]. Such changes not only expose modern vehicles to new security threats but also introduce additional safety concerns. The introduction of new

Authors' addresses: S. Chakraborty, University of North Carolina at Chapel Hill, Department of Computer Science, 201 S. Columbia St., Chapel Hill, NC 27599175, USA; e-mail: samarjit@cs.unc.edu; S. Jha, University of Wisconsin-Madison, Department of Computer Sciences, UW-Madison, 1210 W. Dayton Street, Madison, WI 53706-1613, USA; e-mail: jha@cs.wisc.edu; S. Samii, Linköping University, Dept. of Computer and Information Science, Linköping University, Linköping, SE-581 83, Sweden; e-mail: soheil.samii@liu.se; P. Mundhenk, Robert Bosch GmbH, Robert Bosch GmbH Zentrum für Forschung und Vorausentwicklung, Robert-Bosch-Campus 1, Renningen, DE 71272, Germany; e-mail: Philipp.Mundhenk@bosch.com.

ACM 2378-962X/2024/05-ART10
https://doi.org/10.1145/3650210

autonomous features have also resulted in more complex automotive control strategies, the use of **Machine Learning (ML)** and perception/vision processing algorithms, and more powerful electronics/hardware to support these algorithms. These have also dramatically increased both safety concerns and security threats.

Finally, while commercially available vehicles already support powerful autonomous features, fully autonomous vehicles are now a reality, and the sale of EVs is rapidly increasing, the technologies used in all of these cases are far from being fully mature. Safety certification for autonomous vehicles and their reliability are still major open problems today [5, 16, 89]. Batteries used in EVs are not yet sustainably produced [31, 151], and their environmental impact remains unclear. As the adoption of EVs increases, how to tackle retired batteries in an environmentally sustainable and cost-effective manner is also unclear [87]. The cost of batteries, and therefore EVs, also remains too high to enable higher levels of adoption [35, 101]. As a result, there are still enormous research opportunities in this domain. It is our hope that this special issue will help advance work in area and encourage more researchers to join this burgeoning field.

In the rest of this article, we first discuss some representative work on automotive E/E architectures that have been motivated by safety and security concerns (Section 2). Next, we discuss work on **Model-Based Design (MBD)** for safety and security (in Section 3). Literature on formal methods for autonomous vehicles safety is discussed in Section 4, and automotive controller design techniques for safety and for mitigating faults and threats in Section 5. Finally, we focus on automotive security in Section 6, and certification and standardization work in Section 7. We conclude by briefly outlining the topics of the seven articles in this special issue.

2 SAFETY AND SECURITY-ORIENTED AUTOMOTIVE E/E ARCHITECTURES

A number of studies have focused on in-vehicle E/E architectures from the lens of safety and security. These include investigating architecture frameworks, standards, protocols, and interfaces, and classifying them according to various metrics [156]. Modern automotive E/E architectures consist of hundreds of **Electronic Control Units (ECUs)** connected by various communication buses. They support applications from a variety of domains—such as engine and brake control to infotainment [121], comfort functions [138], and driver assistance [120, 122]. Given the large number of ECUs and the different applications that are supported on them, determining which connection topologies are better is an important optimization problem. Work has been done toward this to qualitatively and quantitatively evaluate various in-vehicle architecture topologies, with an emphasis on two common topology variants: *domain-based* and *zone-based* architectures. Here, in addition to metrics like cost, total communication cable length, and communication load distribution, safety metrics like failure probability for the different topologies have also been accounted for [39]. Another line of work has developed simulation-based testing of automotive architectures and *software-defined vehicles* [15], using only virtual and open source tools such as CARLA (http://carla.org), Proxmox (http://www.proxmox.com), and ROS2 (Robot Operating System)-based vehicle functions [51].

Additionally, work has been done on recent transformations in vehicle architectures from the conventional signal-oriented networks, which are reaching their limits, to service-oriented architectures and what their relative pros and cons are in terms of flexibility, safety, and security [139]. Similarly, zone-based architectures are also being considered as a promising alternative to conventional E/E architectures. But being new, there is still a lack of systematic methods for designing them. Methods to design zonal architectures, particularly to optimize their power supply system, have been proposed in the work of Maier and Reuss [96]. Here, electric loads have been clustered to identify suitable positions for zone control units. In addition to determining optimal wire harness designs, the entire power supply system has been integrated using vehicle packaging concepts and safety metrics. Batteries in EVs [27] and architectural and management decisions around them also have important safety implications, and some of the techniques used in this domain extend to other areas like drones [77, 109, 110].

Dynamic reconfiguration of architectures for fail-operational behavior have been studied by Oszwald et al. [108]. Similarly, the use of FPGA-based reconfigurable computing for high-performance automotive architectures have been investigated in the work of Shreejith et al. [146], and Shreejith and Fahmy [147] studied partial reconfiguration support on FPGAs to support security functions. Along similar lines of hardware design, techniques for mitigating manufacturing variabilities, transient faults, and aging issues in automotive hardware and their impact on software executing on them have also been studied [28, 40, 41, 85, 98]. How to automate the mapping of safety-critical applications to hardware resources in an automotive high-performance central computer, by taking into account predefined safety requirements and optimization goals, has been studied by Askaripoor et al. [7]. By contrasting classical automotive architecture design approaches, where functions are mapped onto a set of communicating control units, new data-centric approaches to architecture design have been investigated in the RACE (Reliable Control and Automation Environment) project [79].

Since automotive architectures are never designed from scratch but evolve over time, studies have been done on how architecture refinement can be in accordance with ISO 26262 functional safety standards. Toward this, sensitive parts of the architecture have been identified, along with selecting suitable safety mechanisms to reduce failure rates and improve metrics defined in the ISO 26262 standard [129, 130]. Similarly, Lu and Chen [88] used a fault tree analysis for ASIL (Automotive Safety Integrity Level)-oriented hardware design, again following the ISO 26262 safety standard. Xie et al. [163] describe recent advances in automotive functional safety design methodologies for architecture design following both ISO 26262 and the AUTOSAR adaptive platform standard.

In addition to considering safety, a considerable amount of work has focused on *security*-driven architecture design. Using examples of future in-vehicle E/E architectures, Plappert et al. [117] have shown how security *design patterns* can be used to identify and mitigate security attacks. Similarly, security vulnerabilities stemming from service-oriented architectures, and contrasting them with signal-oriented architectures has been discussed by Rumez et al. [128]. A case for centralized E/E architectures considering safety and security has been made in the work of Bandur et al. [10], and an evaluation of in-vehicle communication network security based on the protection characteristics of individual network components and the topology of the network has been presented by Petho et al. [114]. Security considerations toward adopting in-vehicle Ethernet have been discussed in the work of Ju et al. [65]. Finally, Prasanth et al. [118] provide a tutorial on automotive functional safety and security stemming from the increase in electronics, software content, and connectivity in modern cars.

3 MBD AND VERIFICATION FOR AUTOMOTIVE SAFETY AND SECURITY

MBD is routinely used for automotive software development [29], particularly for safety-critical components. Work in this area is also closely related to recent research on formal methods and MBD for CPS [20, 24, 144, 178]. Among the different tools used for MBD, Simulink/Stateflow for automotive control optimization [102] and control software development are perhaps the most common. The work of Jaskolka et al. [64] shows how to analyze changes in Simulink/Stateflow models to understand how particular model changes impact system evolution. A well-known challenge in MBD is the incompatibility between the tools and models used for different engineering tasks. Toward this, the problem of bridging the gap between SysML system architecture models and AUTOSAR software architecture models have been addressed by Siavashi et al. [148]. Along similar lines, a framework for transforming system requirements to code generation for safety-critical systems has been proposed by Singh et al. [149]. The compatibility between ROS2 and Adaptive AUTOSAR has been studied by Henle et al. [57].

In general, different techniques have been studied to address the problems of model-model mismatch and model-implementation mismatch. With the growing volume of software in the automotive domain, there is a necessity to share computation/communication resources. This has resulted in a variety of task modeling [22, 115], scheduling [133], and management techniques [19, 23, 84, 176], whose impact is typically not accounted for in high-level models from which the software is synthesized. Such policies can be both time triggered [46, 92, 175]and event triggered, as well as hybrid in nature, and a variety of automotive-specific scheduling techniques for these paradigms have been proposed [132]. Efforts to account for this mismatch have led to work on both testing [11, 155] and verification [17, 53, 67, 160], including reachability analysis techniques for safety verification [58, 59, 76, 165, 169].

A review of research and practice in automotive cybersecurity testing, verification, and validation, particularly from the perspective of cybersecurity standards and regulations such as ISO/SAE 21434 and UNECE WP.29, has been presented in the work of Luo et al. [93]. Verification in this domain is not restricted to functional correctness but also involves non-functional properties like *drivability*. The research reported in the work of Formica et al. [36] presents an automated search-based software testing framework for generating failure-revealing test cases for functional and drivability requirements. Formal methods to derive ISO 26262-compliant certificates for service-oriented automotive architecture have been discussed in the work of Krauter et al. [81]. To test motion planning algorithms in autonomous vehicles, critical scenarios have been automatically generated using evolutionary algorithms to tackle the highly non-linear optimization problems involved in the process [78]. Similarly, MBD and formal verification techniques have been extensively studied for automotive security, and more on this is discussed later. For example, formal security analysis of SOME/IP (Scalable service-Oriented MiddlewarE over IP), which is an Ethernet-based service-oriented communication middleware, has been studied in the work of Zelle et al. [173]. Here, multiple security extensions for authentication and authorization of service provisioning and usage have been proposed. How to ensure safety and security using formal verification, in the case of over-the-air protocols for firmware updates of in-car control units, has been studied in the work of Pedroza et al. [112].

3.1 Methods for Ensuring Timing Safety

There is a substantial volume of literature on timing analysis for automotive architectures [43], software, and communication protocols, from the perspective of timing safety [125]. How to use assurance cases to provide timing guarantees in automotive TSN (Time-Sensitive Networking) Ethernet networks has been shown in the work of Kapinski et al. [75]. As mentioned previously, there is now a move from signal-oriented to service-oriented in-vehicle architectures [82]. Here, techniques for bounding service discovery times in in-vehicle networks have been presented by Fraccoroli et al. [37].

One of the primary causes for model-implementation mismatch and safety violation stems from timing issues. Toward this, techniques to account for delays in control loops have been studied in several works [50, 69, 94]. Along the same lines, delay-tolerant controllers [33, 49, 103], controllers that support multiple sampling rates [25, 47, 134], and the co-synthesis of controllers and control task schedules have been studied as well [13, 48, 95, 126, 141, 172]. The problem of verifying whether automotive control safety properties are satisfied in the presence of timing uncertainties has been addressed [42], and the related problem of synthesizing schedules to satisfy control safety has been explored [167]. Finally, timing isolation techniques for critical control software have been proposed [38, 44, 99, 100], as well as the scheduling of mixed-criticality tasks [140].

4 FORMAL METHODS FOR *AUTONOMOUS* VEHICLE SAFETY

The use of formal methods has been particularly relevant to ensure safety in *autonomous* vehicles [60, 72, 135, 159], and recent years have witnessed a tremendous volume of work in this domain. Here, we sample a variety of work in this area. Checking whether safely driving automated vehicles would harmonize well with regular traffic flows has been studied by Althoff and Lösch [3]. Formal methods to derive what a safe driving distance for autonomous vehicles should be, along with checkers for it, have been presented by Rizaldi et al. [124].

Considerations when studying the safety of autonomous vehicles pertain to (a) controllers implementing autonomous functions and (b) ML algorithms for perception processing. Formal verification has been applied to both of these. The verification of neural network controllers that process LiDAR images to produce control actions has been presented in the work of Sun et al. [154]. Similarly, Habeeb et al. [54] studied the safety of trajectories of a camera-based autonomous vehicle that navigates a 3D scene. Formal verification of autonomous vehicles in arbitrary urban traffic situations, by focusing on its motion planning component, has been described in the work of Pek et al. [113]. How to check that the software used in an autonomous vehicle conforms to specified functional requirements has been presented in the work of Yasmine et al. [168]. Computationally efficient verification of neural network controllers for non-linear continuous-time dynamical systems has been proposed by Jafarpour et al. [63].

The correctness of any control system behind an autonomous feature depends also on the correctness of the perception system feeding the controller. Hsieh et al. [61] construct approximations of perception models from system-level safety requirements, data, and program analysis of the modules that are downstream from perception. Since such approximations are more analyzable, they are used in conjunction with closed-loop control strategies to provide correctness guarantees. Similarly, formal probabilistic analysis techniques have been applied to compact abstractions of neural network based perception models in the work of Păsăreanu et al. [111]. A concept of *perception contracts* has been proposed by Astorga et al. [8] to reason about the safety of controllers. Finding closed-loop vision failures has been formulated as a Hamilton-Jacobi reachability analysis problem for vision-based controllers in the work of Chakraborty and Bansal [18].

5 CONTROLLER DESIGN TECHNIQUES FOR SAFETY AND MITIGATING FAULTS AND THREATS

Instead of verifying a given controller, a different line of work pursues the problem of *designing* controllers to ensure safety and mitigating faults and security threats. Toward this, how (a) sensing and communication technologies, (b) human factors, and (c) information-aware controller design impact the correctness of autonomous vehicles have been surveyed by Sarker et al. [137]. The work of Dey et al. [34] argues for the rethinking of basic CPS design methods, and migrating from a safety-aware and resource-level approach to making security a first-class design constraint. Toward this, new security-aware CPS design techniques for the automotive domain were proposed.

How to mitigate security attacks launched onto the perception sensors and communication channels of autonomous vehicles has been studied by Ju et al. [68]. Work on mitigating denial of service attacks in autonomous vehicles by relying on techniques from switched control systems has been presented by Sun et al. [153]. Kang et al. [74] address the problem that control policies in autonomous vehicles are not publicly available and therefore cannot be trusted. Hence, a data-driven control policy based driving safety analysis has been proposed to identify potentially hazardous driving scenarios. Kang et al. [71] proposed velocity optimization techniques for EVs to optimize energy consumption while ensuring safety at traffic lights (i.e., green lights can be passed without braking, and rear-end collisions are avoided at red lights). Cybersecurity assessment of lane-keeping control in an autonomous vehicle has been studied in the work of Wang et al. [157], along with experimental evaluations using hardware-in-the-loop simulation. Different detection mechanisms for cyber-attacks have been experimentally studied in the work of Stabili et al. [150] using an internal combustion engine and a speed controller communicating via a **Controller Area Network (CAN)** bus.

5.1 Security and Fault Monitoring and Fault Tolerance in Automotive CPS

In addition to controller design and verification, various techniques for fault monitoring and fault tolerance for automotive CPS have also been proposed. For example, monitoring of in-vehicle traffic [73, 104, 161] to detect out-of-order behavior [177] and potential security breaches have been studied. A ROS2-based architecture for collecting and filtering cybersecurity information from multiple sources within the vehicle has been proposed in the work of Grimm et al. [52]. Methods to recognize mistimed and/or unintended deactivation of vehicle functions have been outlined by Segler et al. [142]. An intrusion detection system to monitor CAN network activities and detect suspicious behavior has been presented by Mansourian et al. [97]. Management of safety assurance and using it as a basis for runtime monitoring has been proposed in the work of Hawkins and Conmy [56].

6 AUTOMOTIVE SECURITY THREATS, THEIR MODELING, AND MITIGATION

The two areas that have witnessed the maximum activity in this research space are perhaps verification of autonomous vehicles [4, 9] and automotive security [86, 123, 131]. Formal verification techniques like model checking [62, 105, 106, 116] have also been proposed for automotive security. In a landmark paper, it was shown how to experimentally evaluate the vulnerability of the electronics and software in a modern car and infiltrate virtually any ECU to completely circumvent a broad array of safety-critical systems [80]. This paper triggered a considerable volume of work on automotive security for more than a decade, which still continues to be an active area of research. Soon afterward, it was shown that even physical access to vehicle components is not necessary; vehicles are susceptible to remote compromise and even control, for example, via wireless communication channels [30]. The use of ML techniques [158] in autonomous vehicles, especially for perception processing, also introduces new safety and security vulnerabilities.

Security threats in cars have grown considerably because of their increased connectivity. In addition to connectivity between vehicles, between vehicles and the infrastructure, and because of communication between charging stations and battery management systems [152] in EVs, security risks have increased. Yoshizawa et al. [171] have studied protocols and standards for emerging V2X (Vehicle-to-Everything) communication and identified multiple security- and privacy-related shortcomings and inconsistencies in them. Some solutions to address these, particularly for pseudonym certificate management in V2X communication, was proposed by Yoshizawa and Preneel [170]. Han et al. [55] have investigated security threats stemming from collaborative interaction and decision making in connected and autonomous vehicles.

In recent years, there has been an enormous amount of work on security vulnerabilities in the CAN bus, which is widely used in automotive in-vehicle architectures [70] but still lacks suitable security mechanisms such as message authentication and encryption, primarily because of resource constraints. Here, we sample some recent work in this area. Several intrusion detection techniques for CAN use generative adversarial networks to detect out-of-distribution traffic [177] and generate usable attacked samples to supplement training samples [164]. The research of Xie et al. [162] developed security-aware obfuscated priority assignment for CAN-FD (which is CAN with flexible data rates). A survey on artificial intelligence based intrusion detection systems for attacks on CAN has been presented in the work of Rajapaksha et al. [119]. Recently, using graph neural networks, Zhang et al. [174] propose an anomaly detection mechanism that can detect all—message injection, suspension, and falsification—attacks in real time, whereas most other anomaly detection methods can detect only one or two of these attacks. Other recent anomaly detection mechanisms include those in the work of Shahriar et al. [145] that use a deep learning based signal-level intrusion detection framework. It performs better than anomaly detection methods that either monitor sequences of CAN messages IDs or the binary payload data.

Basing an ECU's hardware characteristics to create its voltage fingerprint has been used as an authentication mechanism on the CAN bus. But a technique has been proposed by Bhatia et al. [14] to corrupt the bus voltages in such an authentication mechanism and launch an attack. In fact, several papers have shown that even a single compromised ECU on a CAN bus can launch many different types of attacks. As an attempt to address resource constraints, and especially the limited bandwidth of the CAN bus, Serag et al. [143] propose an authentication mechanism that uses the spacing between CAN frames instead of any space *in* the frame for authentication information.

Other lines of work focus on attacks on an autonomous vehicle's CAN bus, as they have more external interfaces and sensors then regular vehicles. Toward this, a lightweight encryption and authentication scheme for the CAN bus was proposed in the work of Cui et al. [32]. Finally, examples of attack detection and mitigation mechanisms that use a vehicle's dynamics include the work of Kang and Shen [73]. Here, a vehicle state space model that incorporates features like real-time road friction coefficients are used. When the predicted values of these model parameters based on historical measurements differ too much from currently measured values, such differences are attributed to potential attacks. Such changes are then subtracted away from measured vehicle states to generate correct state estimates.

7 CERTIFICATION AND STANDARDIZATION FOR AUTOMOTIVE SAFETY AND SECURITY

A considerable volume of literature also exists on the topic of standardization and certification for safety and security in the automotive domain; a literature review on this may be found in the work of Sanguino et al. [136]. Ardila and Gallina [6] show how to prove compliance with automotive standards such as ISO 26262 and SAE J3061. How to establish compliance with standards by considering an autonomous vehicle's full ecosystem has has studied in the work of Benyahya et al. [12].

While certification in other safety-critical domains like avionics is more well established, the automotive domain is significantly more cost and, hence, resource sensitive. As a result, it is not possible to over-provision resources to meet safety constraints [45]. To address this issue, both formal verification [21, 83] and systematic testing has been used for the purpose of certification [107]. Optimization techniques [26] to address resource constraints have also been designed with verification and certification in view [26], and model-based techniques have been used for certification [66]. But a remaining open challenge is to translate verification certificates derived at the model level to corresponding certificates for implementations generated from the models [127].

8 ARTICLES IN THIS SPECIAL ISSUE

As in Part 1 of this special issue, Part 2 also features seven articles. The first article, entitled "EVScout2.0: Electric Vehicle Profiling Through Charging Profile" by Brighente et al., discusses techniques for profiling exchanges that EVs have with charging stations and use the resulting information to identify them. Such information leakage during charging is a privacy threat, and the goal of this work is to use the proposed profiling and associated benchmarks to help develop future techniques to plug such vehicle identity leakage. The second article, entitled “Control Performance Analysis of Automotive Cyber-Physical Systems: A Study on Efficient Formal Verification” by Panahi et al., proposes verification techniques to ensure that automotive controllers meet their performance and safety requirements even when the resources available to them vary over time. These variations might stem from schedulers that manage multiple software tasks sharing common resources. Such verification techniques are usually not scalable, and one of the main contributions of this work is to suitably prune the state space to improve scalability while ensuring the soundness of the verification process.

As our review illustrated, security for the CAN bus has attracted a lot of attention, and the third article, entitled “CANOA: CAN Origin Authentication Through Power Side-Channel Monitoring” by Thakur et al., uses an ECU’s power consumption to authenticate it. The fourth article, “Remote Perception Attacks against Camera-Based Object Recognition Systems and Countermeasures” by Man et al., is also on automotive security and shows how camera-based perception systems, such as in autonomous vehicles, can be attacked using lens flare and auto-exposure control to manipulate what its vision system perceives. The work also proposes countermeasures for such attacks.

The fifth article, entitled “Performance Comparison of Timing-Based Anomaly Detectors for Controller Area Network: A Reproducible Study” by Pollicino et al., is again on CAN security, for which several anomaly detection techniques have been proposed in the past. This work presents a systematic comparison of eight different CAN anomaly detection algorithms. It releases their implementations and labeled datasets, thereby allowing a fair comparison of different algorithms. The sixth article of this special issue, entitled “Towards Safe Autonomy in Hybrid Traffic: Detecting Unpredictable Abnormal Behaviors of Human Drivers via Information Sharing” by Wang et al., studies safety in hybrid traffic scenarios, where roads are shared by human-driven and autonomous vehicles. The work proposes algorithms for autonomous vehicles to improve their trajectories by fusing information from surrounding autonomous vehicles, along with detecting abnormal behaviors of human-driven vehicles. Finally, the seventh and the last article, entitled “A Deep Time Delay Filter for Cooperative Adaptive Cruise Control” by Hsueh et al., studies the stability of cooperative adaptive cruise control in the presence of delays. In particular, it proposes to use a neural network to reconstruct state signals that would otherwise not be available—because of delays–to compute control inputs and maintain system performance.

It is our hope that this second set of articles, along with those that appeared in Part 1 of this special issue, will push the envelope in automotive CPS research, particularly on safety and security. We again thank all of the reviewers, Editor-in-Chief Chenyang Lu of ACM TCPS, and all members of the TCPS editorial team, especially Rebecca Malone and Gita Delsing, without whom this special issue would not have been possible.

REFERENCES

[1] Ryan Aalund, Weiping Diao, Lingxi Kong, and Michael G. Pecht. 2021. Understanding the non-collision related battery safety risks in electric vehicles a case study in electric vehicle recalls and the LG chem battery. *IEEE Access* 9 (2021), 89527–89532.

[2] Arun Adiththan, S. Ramesh, and Soheil Samii. 2018. Cloud-assisted control of ground vehicles using adaptive computation offloading techniques. In *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition (DATE’18).*

[3] Matthias Althoff and Robert Lösch. 2016. Can automated road vehicles harmonize with traffic flow while guaranteeing a safe distance? In *Proceedings of the 19th IEEE International Conference on Intelligent Transportation Systems (ITSC’16).* IEEE.

[4] Tanya Amert, Michael Balszun, Martin Geier, F. Donelson Smith, James H. Anderson, and Samarjit Chakraborty. 2021. Timing-predictable vision processing for autonomous systems. In *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition (DATE’21).*

[5] Julia Angwin. 2023. Autonomous vehicles are driving blind. *The New York Times*. Retrieved March 14, 2024 from https://www.nytimes.com/2023/10/11/opinion/driverless-cars-san-francisco.html

[6] Julieth Patricia Castellanos Ardila and Barbara Gallina. 2017. Towards efficiently checking compliance against automotive security and safety standards. In *Proceedings of the IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW'17)*.

[7] Hadi Askaripoor, Morteza Hashemi Farzaneh, and Alois C. Knoll. 2021. A platform to configure and monitor safety-critical applications for automotive central computers. In *Proceedings of the 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'21)*.

[8] Angello Astorga, Chiao Hsieh, P. Madhusudan, and Sayan Mitra. 2023. Perception contracts for safety of ML-enabled systems. *Proceedings of the ACM on Programming Languages* 7, OOPSLA 2 (2023), 2196–2223.

[9] Michael Balszun, Martin Geier, and Samarjit Chakraborty. 2020. Predictable vision for autonomous systems. In *Proceedings of the 23rd IEEE International Symposium on Real-Time Distributed Computing (ISORC'20)*.

[10] Victor Bandur, Gehan M. K. Selim, Vera Pantelic, and Mark Lawford. 2021. Making the case for centralized automotive E/E architectures. *IEEE Transactions on Vehicular Technology* 70, 2 (2021), 1230–1245.

[11] Peter Baumann, Martin Krammer, Mario Driussi, Lars Mikelsons, Josef Zehetner, Werner Mair, and Dieter Schramm. 2019. Using the distributed co-simulation protocol for a mixed real-virtual prototype. In *Proceedings of the IEEE International Conference on Mechatronics (ICM'19)*.

[12] Meriem Benyahya, Anastasija Collen, and Niels Alexander Nijdam. 2023. Cybersecurity and data privacy certification gaps of connected and automated vehicles. *Transportation Research Procedia* 72 (2023), 783–790.

[13] Laksh Bhatia, Ivana Tomic, Anqi Fu, Michael Breza, and Julie A. McCann. 2021. Control communication co-design for wide area cyber-physical systems. *ACM Transactions on Cyber-Physical Systems* 5, 2 (2021), Article 18, 27 pages.

[14] Rohit Bhatia, Vireshwar Kumar, Khaled Serag, Z. Berkay Celik, Mathias Payer, and Dongyan Xu. 2021. Evading voltage-based intrusion detection on automotive CAN. In *Proceedings of the 28th Annual Network and Distributed System Security Symposium (NDSS'21)*. .

[15] Unmesh D. Bordoloi, Samarjit Chakraborty, Markus Jochim, Prachi Joshi, Arvind Raghuraman, and S. Ramesh. 2023. Autonomy-driven emerging directions in software-defined vehicles. In *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition (DATE'23)*.

[16] Neal E. Boudette, Cade Metz, and Jack Ewing. 2022. Tesla Autopilot and other driver-assist systems linked to hundreds of crashes. *The New York Times*. Retrieved March 14, 2024 from https://www.nytimes.com/2022/06/15/business/self-driving-car-nhtsa-crash-data.html

[17] Manfred Broy, Samarjit Chakraborty, Dip Goswami, S. Ramesh, Manoranjan Satpathy, Stefan Resmerita, and Wolfgang Pree. 2011. Cross-layer analysis, testing and verification of automotive control software. In *Proceedings of the 11th International Conference on Embedded Software (EMSOFT'11)*.

[18] Kaustav Chakraborty and Somil Bansal. 2023. Discovering closed-loop failures of vision-based controllers via reachability analysis. *IEEE Robotics and Automation Letters* 8, 5 (2023), 2692–2699.

[19] Samarjit Chakraborty, Thomas Erlebach, and Lothar Thiele. 2001. On the complexity of scheduling conditional real-time code. In *Algorithms and Data Structures*. Lecture Notes in Computer Science, Vol. 2125. Springer, 38–49.

[20] Samarjit Chakraborty, Mohammad Abdullah Al Faruque, Wanli Chang, Dip Goswami, Marilyn Wolf, and Qi Zhu. 2016. Automotive cyber-physical systems: A tutorial introduction. *IEEE Design & Test* 33, 4 (2016), 92–108.

[21] Samarjit Chakraborty, Yanhong Liu, Nikolay Stoimenov, Lothar Thiele, and Ernesto Wandeler. 2006. Interface-based rate analysis of embedded systems. In *Proceedings of the 27th IEEE Real-Time Systems Symposium (RTSS'06)*.

[22] Samarjit Chakraborty, Linh T. X. Phan, and P. S. Thiagarajan. 2005. Event count automata: A state-based model for stream processing systems. In *Proceedings of the 26th IEEE Real-Time Systems Symposium (RTSS'05)*.

[23] Samarjit Chakraborty and Lothar Thiele. 2005. A new task model for streaming applications and its schedulability analysis. In *Proceedings of the Design, Automation, and Test in Europe Conference and Exposition (DATE'05)*.

[24] Wanli Chang and Samarjit Chakraborty. 2016. Resource-aware automotive control systems design: A cyber-physical systems approach. *Foundations and Trends in Electronic Design Automation* 10, 4 (2016), 249–369.

[25] Wanli Chang, Dip Goswami, Samarjit Chakraborty, and Arne Hamann. 2018. OS-aware automotive controller design using non-uniform sampling. *ACM Transactions on Cyber-Physical Systems* 2, 4 (2018), Article 26, 22 pages.

[26] Wanli Chang, Dip Goswami, Samarjit Chakraborty, Lei Ju, Chun Jason Xue, and Sidharta Andalam. 2017. Memory-aware embedded control systems design. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 36, 4 (2017), 586–599.

[27] Wanli Chang, Martin Lukasiewycz, Sebastian Steinhorst, and Samarjit Chakraborty. 2013. Dimensioning and configuration of EES systems for electric vehicles with boundary-conditioned adaptive scalarization. In *Proceedings of the International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS'13)*.

[28] Wanli Chang, Alma Pröbstl, Dip Goswami, Majid Zamani, and Samarjit Chakraborty. 2014. Battery- and aging-aware embedded control systems for electric vehicles. In *Proceedings of the 35th IEEE Real-Time Systems Symposium (RTSS'14)*.

[29] Wanli Chang, Debayan Roy, Licong Zhang, and Samarjit Chakraborty. 2016. Model-based design of resource-efficient automotive control software. In *Proceedings of the 35th International Conference on Computer-Aided Design (ICCAD'16).*

[30] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. 2011. Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of the 20th USENIX Security Symposium.*

[31] Michael J. Coren. 2023. Are electric cars really better for the environment? *The Washington Post.* Retrieved March 14, 2024 from https://www.washingtonpost.com/climate-environment/2023/09/19/electric-cars-better-environment-fossil-fuels/

[32] Jie Cui, Yaning Chen, Hong Zhong, Debiao He, Lu Wei, Irina Bolodurina, and Lu Liu. 2023. Lightweight encryption and authentication for controller area network of autonomous vehicles. *IEEE Transactions on Vehicular Technology* 72, 11 (2023), 14756–14770.

[33] Sayandip De, Sajid Mohamed, Dip Goswami, and Henk Corporaal. 2020. Approximation-aware design of an image-based control system. *IEEE Access* 8 (2020), 174568–174586.

[34] Soumyajit Dey, Ipsita Koley, and Sunandan Adhikary. 2023. Resource aware synthesis of automotive security primitives. In *Machine Learning and Optimization Techniques for Automotive Cyber-Physical Systems.* Springer, 189–224.

[35] Jack Ewing. 2023. Automakers delay electric vehicle spending as demand slows. *The New York Times.* Retrieved March 14, 2024 from https://www.nytimes.com/2023/11/07/business/energy-environment/electric-vehicles-sales.html

[36] Federico Formica, Nicholas Petrunti, Lucas Bruck, Vera Pantelic, Mark Lawford, and Claudio Menghi. 2023. Test case generation for drivability requirements of an automotive cruise controller: An experience with an industrial simulator. In *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE'23).*

[37] Enrico Fraccaroli, Parchi Joshi, Shengjie Xu, Khaja Shazzad, Markus Jochim, and Samarjit Chakraborty. 2023. Timing predictability for SOME/IP-based service-oriented automotive in-vehicle networks. In *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition (DATE'23).*

[38] Johannes Freitag, Sascha Uhrig, and Theo Ungerer. 2018. Virtual timing isolation for mixed-criticality systems. In *Proceedings of the 30th Euromicro Conference on Real-Time Systems (ECRTS'18).*

[39] Alessandro Frigerio, Bart Vermeulen, and Kees G. W. Goossens. 2021. Automotive architecture topologies: Analysis for safety-critical autonomous vehicle applications. *IEEE Access* 9 (2021), 62837–62846.

[40] Foad Haidari Gandoman, Abdollah Ahmadi, Peter Van den Bossche, Joeri Van Mierlo, Noshin Omar, Ali Esmaeel Nezhad, Hani Mavalizadeh, and Clement Mayet. 2019. Status and future perspectives of reliability assessment for electric vehicles. *Reliability Engineering & System Safety* 183 (2019), 1–16.

[41] Georg Georgakos, Ulf Schlichtmann, Reinhard Schneider, and Samarjit Chakraborty. 2013. Reliability challenges for electric vehicles: From devices to architecture and systems software. In *Proceedings of the 50th Annual Design Automation Conference (DAC'13).*

[42] Bineet Ghosh, Clara Hobbs, Shengjie Xu, Parasara Sridhar Duggirala, James H. Anderson, P. S. Thiagarajan, and Samarjit Chakraborty. 2022. Statistical hypothesis testing of controller implementations under timing uncertainties. In *Proceedings of the 28th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'22).*

[43] Michael Glaß, Martin Lukasiewycz, Jürgen Teich, Unmesh D. Bordoloi, and Samarjit Chakraborty. 2009. Designing heterogeneous ECU networks via compact architecture encoding and hybrid timing analysis. In *Proceedings of the 46th Design Automation Conference (DAC'09).*

[44] Kees Goossens, Arnaldo Azevedo, Karthik Chandrasekar, Manil Dev Gomony, Sven Goossens, Martijn Koedam, Yonghui Li, Davit Mirzoyan, Anca Mariana Molnos, Ashkan Beyranvand Nejad, Andrew Nelson, and Shubhendu Sinha. 2013. Virtual execution platforms for mixed-time-criticality systems: The CompSOC architecture and design flow. *ACM SIGBED Review* 10, 3 (2013), 23–34.

[45] Dip Goswami, Reinhard Schneider, Alejandro Masrur, Martin Lukasiewycz, Samarjit Chakraborty, Harald Voit, and Anuradha Annaswamy. 2012. Challenges in automotive cyber-physical systems design. In *Proceedings of the International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS'12).*

[46] Dip Goswami, Martin Lukasiewycz, Reinhard Schneider, and Samarjit Chakraborty. 2012. Time-triggered implementations of mixed-criticality automotive software. In *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition (DATE'12).*

[47] Dip Goswami, Alejandro Masrur, Reinhard Schneider, Chun Jason Xue, and Samarjit Chakraborty. 2013. Multirate controller design for resource- and schedule-constrained automotive ECUs. In *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition (DATE'13).*

[48] Dip Goswami, Reinhard Schneider, and Samarjit Chakraborty. 2011. Co-design of cyber-physical systems via controllers with flexible delay constraints. In *Proceedings of the 16th Asia South Pacific Design Automation Conference (ASP-DAC'11).*

[49] Dip Goswami, Reinhard Schneider, and Samarjit Chakraborty. 2011. Re-engineering cyber-physical control applications for hybrid communication protocols. In *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition (DATE'11)*.

[50] Dip Goswami, Reinhard Schneider, and Samarjit Chakraborty. 2014. Relaxing signal delay constraints in distributed embedded controllers. *IEEE Transactions on Control Systems Technology* 22, 6 (2014), 2337–2345.

[51] Daniel Grimm, Marc Schindewolf, and Eric Sax. 2023. Fleet in the loop: An open source approach for design and test of resilient vehicle architectures. In *Proceedings of the 15th IEEE International Symposium on Autonomous Decentralized Systems (ISADS'23)*.

[52] Daniel Grimm, Moritz Zink, Marc Schindewolf, and Eric Sax. 2023. Adaptive cybersecurity monitoring for resilient vehicular architectures. In *Proceedings of the IEEE Vehicular Networking Conference (VNC'23)*. IEEE, 41–48.

[53] Liangpeng Guo, Qi Zhu, Pierluigi Nuzzo, Roberto Passerone, Alberto L. Sangiovanni-Vincentelli, and Edward A. Lee. 2014. Metronomy: A function-architecture co-simulation framework for timing verification of cyber-physical systems. In *Proceedings of the International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS'14)*.

[54] P. Habeeb, Nabarun Deka, Deepak D'Souza, Kamal Lodaya, and Pavithra Prabhakar. 2023. Verification of camera-based autonomous systems. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 42, 10 (2023), 3450–3463.

[55] Jinpeng Han, Zhiyang Ju, Xiaoguang Chen, Manzhi Yang, Hui Zhang, and Rouxing Huai. 2023. Secure operations of connected and autonomous vehicles. *IEEE Transactions on Intelligent Vehicles* 8, 11 (2023), 4484–4497. https://doi.org/10.1109/TIV.2023.3304762

[56] Richard Hawkins and Philippa Ryan Conmy. 2023. Identifying run-time monitoring requirements for autonomous systems through the analysis of safety arguments. In *Computer Safety, Reliability, and Security*. Lecture Notes in Computer Science, Vol. 14181. Springer, 11–24.

[57] Jacqueline Henle, Martin Stoffel, Marc Schindewolf, Ann-Therese Nägele, and Eric Sax. 2022. Architecture platforms for future vehicles: A comparison of ROS2 and Adaptive AUTOSAR. In *Proceedings of the 25th IEEE International Conference on Intelligent Transportation Systems (ITSC'22)*.

[58] Jens Henriksson, Markus Borg, and Cristofer Englund. 2018. Automotive safety and machine learning: Initial results from a study on how to adapt the ISO 26262 safety standard. In *Proceedings of the 1st IEEE/ACM International Workshop on Software Engineering for AI in Autonomous Systems (SEFAIAS@ICSE'18)*.

[59] Clara Hobbs, Bineet Ghosh, Shengjie Xu, Parasara Sridhar Duggirala, and Samarjit Chakraborty. 2022. Safety analysis of embedded controllers under implementation platform timing uncertainties. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 41, 11 (2022), 4016–4027.

[60] Clara Hobbs, Debayan Roy, Parasara Sridhar Duggirala, F. Donelson Smith, Soheil Samii, James H. Anderson, and Samarjit Chakraborty. 2021. Perception computing-aware controller synthesis for autonomous systems. In *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition (DATE'21)*.

[61] Chiao Hsieh, Yangge Li, Dawei Sun, Keyur Joshi, Sasa Misailovic, and Sayan Mitra. 2022. Verifying controllers with vision-based perception using safe approximate abstractions. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 41, 11 (2022), 4205–4216.

[62] Li Huang and Eun-Young Kang. 2019. In *Fundamental Approaches to Software Engineering*. Lecture Notes in Computer Science, Vol. 11424. Springer, 210–227. .

[63] Saber Jafarpour, Akash Harapanahalli, and Samuel Coogan. 2023. Interval reachability of nonlinear dynamical systems with neural network controllers. In *Proceedings of the Learning for Dynamics and Control Conference*. 12–25.

[64] Monika Jaskolka, Vera Pantelic, Alan Wassyng, Richard F. Paige, and Mark Lawford. 2023. Repository mining for changes in Simulink and Stateflow models. *Software and Systems Modeling* 22, 5 (2023), 1713–1732.

[65] Hongil Ju, Boosun Jeon, Daewon Kim, Boheung Jung, and Kyudong Jung. 2019. Security considerations for in-vehicle secure communication. In *Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC'19)*.

[66] Lei Ju, Bach Khoa Huynh, Samarjit Chakraborty, and Abhik Roychoudhury. 2009. Context-sensitive timing analysis of Esterel programs. In *Proceedings of the 46th Design Automation Conference (DAC'09)*.

[67] Lei Ju, Bach Khoa Huynh, Abhik Roychoudhury, and Samarjit Chakraborty. 2008. Performance debugging of Esterel specifications. In *Proceedings of the 6th International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS'08)*.

[68] Zhiyang Ju, Hui Zhang, Xiang Li, Xiaoguang Chen, Jinpeng Han, and Manzhi Yang. 2022. A survey on attack detection and resilience for connected and automated vehicles: From vehicle dynamics and control perspective. *IEEE Transactions on Intelligent Vehicles* 7, 4 (2022), 815–837.

[69] Chaitanya Jugade, Daniel Hartgers, Phan Dúc Anh, Sajid Mohamed, Mojtaba Haghi, Dip Goswami, Andrew Nelson, Gijs van der Veen, and Kees Goossens. 2022. An evaluation framework for vision-in-the-loop motion control systems. In *Proceedings of the 27th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'22)*.

[70] Harsha Kumara Kalutarage, M. Omar Al-Kadri, Madeline Cheah, and Garikayi Madzudzo. 2019. Context-aware anomaly detector for monitoring cyber attacks on automotive CAN bus. In *Proceedings of the ACM Symposium on Computer Science in Cars*. Article 7, 8 pages.

[71] Liuwang Kang, Ankur Sarker, and Haiying Shen. 2020. Velocity optimization of pure electric vehicles with traffic dynamics and driving safety considerations. *ACM Transactions on Internet of Things* 2, 1 (2020), Article 7, 24 pages.

[72] Liuwang Kang and Haiying Shen. 2021. A control policy based driving safety system for autonomous vehicles. In *Proceedings of the IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS'21)*.

[73] Liuwang Kang and Haiying Shen. 2022. Detection and mitigation of sensor and CAN bus attacks in vehicle anti-lock braking systems. *ACM Transactions on Cyber-Physical Systems* 6, 1 (2022), Article 9, 24 pages.

[74] Liuwang Kang, Haiying Shen, Yezhuo Li, and Shiwei Xu. 2023. A data-driven control-policy-based driving safety analysis system for autonomous vehicles. *IEEE Internet of Things Journal* 10, 16 (2023), 14058–14070.

[75] Ryan Kapinski, Vera Pantelic, Victor Bandur, Alan Wassyng, and Mark Lawford. 2023. Assurance cases for timing properties of automotive TSN networks. In *Computer Safety, Reliability, and Security: SAFECOMP 2023 Workshops*. Lecture Notes in Computer Science, Vol. 14182. Springer, 26–31.

[76] Matthias Kauer, Damoon Soudbakhsh, Dip Goswami, Samarjit Chakraborty, and Anuradha M. Annaswamy. 2014. Fault-tolerant control synthesis and verification of distributed embedded systems. In *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition (DATE'14)*.

[77] Jiwon Kim, Yonghun Choi, Seunghyeok Jeon, Jaeyun Kang, and Hojung Cha. 2020. Optrone: Maximizing performance and energy resources of drone batteries. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 39, 11 (2020), 3931–3943.

[78] Moritz Klischat and Matthias Althoff. 2019. Generating critical test scenarios for automated vehicles with evolutionary algorithms. In *Proceedings of the IEEE Intelligent Vehicles Symposium (IV'19)*. IEEE, 2352–2358.

[79] Alois C. Knoll, Christian Buckl, Karl-Josef Kuhn, and Gernot Spiegelberg. 2019. The RACE project: An informatics-driven Greenfield approach to future E/E architectures for cars. In *Automotive Systems and Software Engineering: State of the Art and Future Trends*, Yanja Dajsuren and Mark van den Brand (Eds.). Springer, 171–195.

[80] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak N. Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. 2010. Experimental security analysis of a modern automobile. In *Proceedings of the 31st IEEE Symposium on Security and Privacy (SP'10)*.

[81] Felix Krauter, Marc Schindewolf, and Eric Sax. 2022. Certificate-based safety concept for future dynamic automotive electric/electronic architectures. In *22. Internationales Stuttgarter Symposium*, Michael Bargende, Hans-Christian Reuss, and Andreas Wagner (Eds.). Springer Fachmedien Wiesbaden, 487–500.

[82] Stefan Kugele, Philipp Obergfell, and Eric Sax. 2021. Model-based resource analysis and synthesis of service-oriented automotive software architectures. *Software and Systems Modeling* 20, 6 (2021), 1945–1975.

[83] Pratyush Kumar, Dip Goswami, Samarjit Chakraborty, Anuradha Annaswamy, Kai Lampka, and Lothar Thiele. 2012. A hybrid approach to cyber-physical systems verification. In *Proceedings of the 49th Annual Design Automation Conference (DAC'12)*.

[84] Zhaojian Li, Tianshu Chu, Ilya V. Kolmanovsky, Xiang Yin, and Xunyuan Yin. 2017. Cloud resource allocation for cloud-based automotive applications. *CoRR abs/1701.04537* (2017). http://arxiv.org/abs/1701.04537

[85] Zhao Li, Chengcheng Huang, Xiaoxiao Dong, and Chongguang Ren. 2020. Resource-efficient cyber-physical systems design: A survey. *Microprocessors and Microsystems* 77 (2020), 103183.

[86] Hengyi Liang, Zhilu Wang, Debayan Roy, Soumyajit Dey, Samarjit Chakraborty, and Qi Zhu. 2019. Security-driven codesign with weakly-hard constraints for real-time embedded systems. In *Proceedings of the 37th IEEE International Conference on Computer Design (ICCD'19)*.

[87] XiaoZhi Lim. 2021. Millions of electric car batteries will retire in the next decade. What happens to them? *The Guardian*. Retrieved March 14, 2024 from https://www.theguardian.com/environment/2021/aug/20/electric-car-batteries-what-happens-to-them

[88] Kuen-Long Lu and Yung-Yuan Chen. 2019. ISO 26262 ASIL-oriented hardware design framework for safety-critical automotive systems. In *Proceedings of the IEEE International Conference on Connected Vehicles and Expo (ICCVE'19)*.

[89] Yiwen Lu. 2023. 'Lost time for no reason': How driverless taxis are stressing cities. *The New York Times*. Retrieved March 14, 2024 from https://www.nytimes.com/2023/11/20/technology/driverless-taxis-cars-cities.html.

[90] Martin Lukasiewycz, Sebastian Steinhorst, Florian Sagstetter, Wanli Chang, Peter Waszecki, Matthias Kauer, and Samarjit Chakraborty. 2012. Cyber-physical systems design for electric vehicles. In *Proceedings of the 15th Euromicro Conference on Digital System Design (DSD'12)*.

[91] Martin Lukasiewycz, Sebastian Steinhorst, Sidharta Andalam, Florian Sagstetter, Peter Waszecki, Wanli Chang, Matthias Kauer, Philipp Mundhenk, Shreejith Shanker, Suhaib A. Fahmy, and Samarjit Chakraborty. 2013. System architecture and software design for electric vehicles. In *Proceedings of the 50th Annual Design Automation Conference (DAC'13)*.

[92] Martin Lukasiewycz, Reinhard Schneider, Dip Goswami, and Samarjit Chakraborty. 2012. Modular scheduling of distributed heterogeneous time-triggered automotive systems. In *Proceedings of the 17th Asia and South Pacific Design Automation Conference (ASP-DAC'12)*.

[93] Feng Luo, Xuan Zhang, Zhenyu Yang, Yifan Jiang, Jiajia Wang, Mingzhi Wu, and Wanqiang Feng. 2022. Cybersecurity testing for automotive domain: A survey. *Sensors* 22, 23 (2022), 9211.

[94] Martina Maggio, Arne Hamann, Eckart Mayer-John, and Dirk Ziegenbein. 2020. Control-system stability under consecutive deadline misses constraints. In *32nd Euromicro Conference on Real-Time Systems (ECRTS'20).* Leibniz International Proceedings in Informatics, Vol. 165. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Article 21, 24 pages.

[95] Rouhollah Mahfouzi, Amir Aminifar, Soheil Samii, Ahmed Rezine, Petru Eles, and Zebo Peng. 2021. Breaking silos to guarantee control stability with communication over ethernet TSN. *IEEE Design & Test* 38, 5 (2021), 48–56.

[96] Jonas Maier and Hans-Christian Reuss. 2023. Handling system complexity in zonal E/E architectures. *Transportation Engineering* 13 (2023), 100195. https://doi.org/10.1016/j.treng.2023.100195

[97] Pegah Mansourian, Ning Zhang, Arunita Jaekel, and Marc Kneppers. 2023. Deep learning-based anomaly detection for connected autonomous vehicles using spatiotemporal information. *IEEE Transactions on Intelligent Transportation Systems* 24, 12 (2023), 16006–16017.

[98] Alejandro Masrur, Philipp Kindt, Martin Becker, Samarjit Chakraborty, Veit Kleeberger, Martin Barke, and Ulf Schlichtmann. 2012. Schedulability analysis for processors with aging-aware autonomic frequency scaling. In *Proceedings of the IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'12)*.

[99] Alejandro Masrur, Sebastian Drössler, Thomas Pfeuffer, and Samarjit Chakraborty. 2010. VM-based real-time services for automotive control applications. In *Proceedings of the 16th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'10)*.

[100] Alejandro Masrur, Thomas Pfeuffer, Martin Geier, Sebastian Drössler, and Samarjit Chakraborty. 2011. Designing VM schedulers for embedded real-time applications. In *Proceedings of the 9th International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS'11)*.

[101] Sean McLain and Nate Rattner. 2023. How electric vehicles are losing momentum with U.S. buyers, in charts. *The Wall Street Journal*. Retrieved March 14, 2024 from https://www.wsj.com/business/autos/electric-vehicle-demand-charts-7d3089c7

[102] Anna Minaeva, Debayan Roy, Benny Akesson, Zdenek Hanzálek, and Samarjit Chakraborty. 2021. Control performance optimization for application integration on automotive architectures. *IEEE Transactions on Computers* 70, 7 (2021), 1059–1073.

[103] Sajid Mohamed, Dip Goswami, Vishak Nathan, Raghu Rajappa, and Twan Basten. 2020. A scenario- and platform-aware design flow for image-based control systems. *Microprocessors and Microsystems* 75 (2020), 103037.

[104] Hyeran Mun, Kyusuk Han, and Dong Hoon Lee. 2020. Ensuring safety and security in CAN-based automotive embedded systems: A combination of design optimization and secure communication. *IEEE Transactions on Vehicular Technology* 69, 7 (2020), 7078–7091.

[105] Philipp Mundhenk, Andrew Paverd, Artur Mrowca, Sebastian Steinhorst, Martin Lukasiewycz, Suhaib A. Fahmy, and Samarjit Chakraborty. 2017. Security in automotive networks: Lightweight authentication and authorization. *ACM Transactions on Design Automation of Electronic Systems* 22, 2 (2017), Article 25, 27 pages.

[106] Philipp Mundhenk, Sebastian Steinhorst, Martin Lukasiewycz, Suhaib A. Fahmy, and Samarjit Chakraborty. 2015. Security analysis of automotive architectures using probabilistic model checking. In *Proceedings of the 52nd Annual Design Automation Conference (DAC'15)*.

[107] Jan-Hendrik Oetjens, N. Bannow, M. Becker, O. Bringmann, A. Burger, M. Chaari, S. Chakraborty, R. Dreschler, W. Ecker, K. Gruttner, Th. Kruse, C. Kuznik, H. M. Le, A. Mauderer, W. Muller, D. Muller-Gritschneder, F. Poppen, H. Post, S. Reiter, W. Rosenstiel, S. Roth, U. Schlichtmann, A. von Schwerin, B.-A. Tabacaru, and A. Viehl. 2014. Safety evaluation of automotive electronics using virtual prototypes: State of the art and research challenges. In *Proceedings of the 51st Annual Design Automation Conference (DAC'14).* ACM, Article 113, 6 pages.

[108] Florian Oszwald, Philipp Obergfell, Matthias Traub, and Jürgen Becker. 2019. Reliable fail-operational automotive E/E-architectures by dynamic redundancy and reconfiguration. In *Proceedings of the 32nd IEEE International System-on-Chip Conference (SOCC'19)*.

[109] Sangyoung Park, Licong Zhang, and Samarjit Chakraborty. 2016. Design space exploration of drone infrastructure for large-scale delivery services. In *Proceedings of the 35th International Conference on Computer-Aided Design (ICCAD'16)*.

[110] Sangyoung Park, Licong Zhang, and Samarjit Chakraborty. 2017. Battery assignment and scheduling for drone delivery businesses. In *Proceedings of the IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED'17)*.

[111] Corina S Păsăreanu, Ravi Mangal, Divya Gopinath, Sinem Getir Yaman, Calum Imrie, Radu Calinescu, and Huafeng Yu. 2023. Closed-loop analysis of vision-based autonomous systems: A case study. In *Proceedings of the International Conference on Computer Aided Verification (CAV'23)*. 289–303.

[112] Gabriel Pedroza, Muhammad Sabir Idrees, Ludovic Apvrille, and Yves Roudier. 2011. A formal methodology applied to secure over-the-air automotive applications. In *Proceedings of the 74th IEEE Vehicular Technology Conference (VTC'11)*. IEEE, 1–5.

[113] Christian Pek, Stefanie Manzinger, Markus Koschi, and Matthias Althoff. 2020. Using online verification to prevent autonomous vehicles from causing accidents. *Nature Machine Intelligence* 2, 9 (2020), 518–528.

[114] Zsombor Petho, Intiyaz Khan, and Árpád Török. 2021. Analysis of security vulnerability levels of in-vehicle network topologies applying graph representations. *Journal of Electronic Testing* 37, 5 (2021), 613–621.

[115] Linh T. X. Phan, Samarjit Chakraborty, P. S. Thiagarajan, and Lothar Thiele. 2007. Composing functional and state-based performance models for analyzing heterogeneous real-time systems. In *Proceedings of the 28th IEEE Real-Time Systems Symposium (RTSS'07)*.

[116] Lee Pike, Jamey Sharp, Mark Tullsen, Patrick C. Hickey, and James Bielman. 2017. Secure automotive software: The next steps. *IEEE Software* 34, 3 (2017), 49–55.

[117] Christian Plappert, Florian Fenzl, Roland Rieke, Ilaria Matteucci, Gianpiero Costantino, and Marco De Vincenzi. 2022. SECPAT: Security patterns for resilient automotive E/E architectures. In *Proceedings of the 30th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP'22)*. IEEE, 255–264.

[118] V. Prasanth, David Foley, and Srivaths Ravi. 2017. Demystifying automotive safety and security for semiconductor developer. In *Proceedings of the 2017 IEEE International Test Conference (ITC'17)*.

[119] Sampath Rajapaksha, Harsha K. Kalutarage, M. Omar Al-Kadri, Andrei Petrovski, Garikayi Madzudzo, and Madeline Cheah. 2023. AI-based intrusion detection systems for in-vehicle networks: A survey. *ACM Computing Surveys* 55, 11 (2023), Article 237, 40 pages.

[120] Qing Rao and Samarjit Chakraborty. 2021. In-vehicle object-level 3D reconstruction of traffic scenes. *IEEE Transactions on Intelligent Transportation Systems* 22, 12 (2021), 7747–7759.

[121] Qing Rao, Christian Grünler, Markus Hammori, and Samarjit Chakraborty. 2014. Design methods for augmented reality in-vehicle infotainment systems. In *Proceedings of the 51st Annual Design Automation Conference (DAC'14)*.

[122] Qing Rao, Tobias Tropper, Christian Grünler, Markus Hammori, and Samarjit Chakraborty. 2014. —Implementation of in-vehicle augmented reality. In *Proceedings of the IEEE International Symposium on Mixed and Augmented Reality (ISMAR'14)*.

[123] Sandip Ray, Ahmad-Reza Sadeghi, and Mohammad Abdullah Al Faruque. 2019. Guest editors' introduction: Secure automotive systems. *IEEE Design & Test* 36, 6 (2019), 5–6.

[124] Albert Rizaldi, Fabian Immler, and Matthias Althoff. 2016. A formally verified checker of the safe distance traffic rules for autonomous vehicles. In *NASA Formal Methods*. Lecture Notes in Computer Science, Vol. 9690. Springer, 175–190.

[125] Debayan Roy, Clara Hobbs, James H. Anderson, Marco Caccamo, and Samarjit Chakraborty. 2021. Timing debugging for cyber-physical systems. In *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition (DATE'21)*.

[126] Debayan Roy, Licong Zhang, Wanli Chang, Dip Goswami, and Samarjit Chakraborty. 2016. Multi-objective co-optimization of FlexRay-based distributed control systems. In *Proceedings of the IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS'16)*.

[127] Debayan Roy, Licong Zhang, Wanli Chang, Sanjoy K. Mitter, and Samarjit Chakraborty. 2018. Semantics-preserving cosynthesis of cyber-physical systems. *Proceedings of the IEEE* 106, 1 (2018), 171–200.

[128] Marcel Rumez, Daniel Grimm, Reiner Kriesten, and Eric Sax. 2020. An overview of automotive service-oriented architectures and implications for security countermeasures. *IEEE Access* 8 (2020), 221852–221870.

[129] Vladimir Rupanov, Christian Buckl, Ludger Fiege, Michael Armbruster, Alois C. Knoll, and Gernot Spiegelberg. 2012. Early safety evaluation of design decisions in E/E architecture according to ISO 26262. In *Proceedings of the 3rd International ACM SIGSOFT Symposium on Architecting Critical Systems (ISARCS'12)*. ACM, 1–10.

[130] Vladimir Rupanov, Christian Buckl, Ludger Fiege, Michael Armbruster, Alois C. Knoll, and Gernot Spiegelberg. 2014. Employing early model-based safety evaluation to iteratively derive E/E architecture design. *Science of Computer Programming* 90 (2014), 161–179.

[131] Florian Sagstetter, Martin Lukasiewycz, Sebastian Steinhorst, and Marko Wolf. 2013. Security challenges in automotive hardware/software architecture design. In *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition (DATE'13)*.

[132] Florian Sagstetter, Sidharta Andalam, Peter Waszecki, Martin Lukasiewycz, Hauke Stähle, Samarjit Chakraborty, and Alois C. Knoll. 2014. Schedule integration framework for time-triggered automotive architectures. In *Proceedings of the 51st Annual Design Automation Conference (DAC'14)*.

[133] Florian Sagstetter, Martin Lukasiewycz, and Samarjit Chakraborty. 2017. Generalized asynchronous time-triggered scheduling for FlexRay. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 36, 2 (2017), 214–226.

[134] Florian Sagstetter, Peter Waszecki, Sebastian Steinhorst, Martin Lukasiewycz, and Samarjit Chakraborty. 2016. Multischedule synthesis for variant management in automotive time-triggered systems. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 35, 4 (2016), 637–650.

[135] Kruttidipta Samal, Marilyn Wolf, and Saibal Mukhopadhyay. 2021. Closed-loop approach to perception in autonomous system. In *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition (DATE'21)*.

[136] Tomás de J. Mateo Sanguino, José M. Lozano Domínguez, and Patrícia de Carvalho Baptista. 2020. Cybersecurity certification and auditing of automotive industry. In *Advances in Transport Policy and Planning*. Vol. 5. Elsevier, 95–124.

[137] Ankur Sarker, Haiying Shen, Mizanur Rahman, Mashrur Chowdhury, Kakan C. Dey, Fangjian Li, Yue Wang, and Husnu S. Narman. 2020. A review of sensing and communication, human factors, and controller aspects for information-aware connected and automated vehicles. *IEEE Transactions on Intelligent Transportation Systems* 21, 1 (2020), 7–29.

[138] Christian Scharfenberger, Samarjit Chakraborty, and Georg Färber. 2012. Robust image processing for an omnidirectional camera-based smart car door. *ACM Transactions on Embedded Computing Systems* 11, 4 (2012), Article 87, 28 pages.

[139] Marc Schindewolf, Hannes Stoll, Houssem Guissouma, Andreas Puder, Eric Sax, Andreas Vetter, Marcel Rumez, and Jacqueline Henle. 2022. A comparison of architecture paradigms for dynamic reconfigurable automotive networks. In *Proceedings of the International Conference on Connected Vehicles and Expo (ICCVE'22)*. IEEE.

[140] Reinhard Schneider, Dip Goswami, Alejandro Masrur, Martin Becker, and Samarjit Chakraborty. 2013. Multi-layered scheduling of mixed-criticality cyber-physical systems. *Journal of Systems Architecture* 59, 10-D (2013), 1215–1230.

[141] Reinhard Schneider, Dip Goswami, Sohaib Zafar, Martin Lukasiewycz, and Samarjit Chakraborty. 2011. Constraint-driven synthesis and tool-support for FlexRay-based automotive control systems. In *Proceedings of the 9th International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS'11)*.

[142] Christoph Segler, Stefan Kugele, Philipp Obergfell, Mohd Hafeez Osman, Sina Shafaei, Eric Sax, and Alois C. Knoll. 2019. Evaluation of feature selection for anomaly detection in automotive E/E architectures. In *Proceedings of the 41st International Conference on Software Engineering: Companion Proceedings (ICSE'19)*. IEEE, 260–261.

[143] Khaled Serag, Rohit Bhatia, Akram Faqih, Muslum Ozgur Ozmen, Vireshwar Kumar, Z. Berkay Celik, and Dongyan Xu. 2023. ZBCAN: A zero-byte CAN defense system. In *Proceedings of the 32nd USENIX Security Symposium*. 6893–6910.

[144] Sanjit A. Seshia, Shiyan Hu, Wenchao Li, and Qi Zhu. 2017. Design automation of cyber-physical systems: Challenges, advances, and opportunities. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 36, 9 (2017), 1421–1434.

[145] Md. Hasan Shahriar, Yang Xiao, Pablo Moriano, Wenjing Lou, and Y. Thomas Hou. 2023. CANShield: Deep-learning-based intrusion detection framework for controller area networks at the signal level. *IEEE Internet of Things Journal* 10, 24 (2023), 22111–22127.

[146] Shanker Shreejith, Philipp Mundhenk, Andreas Ettner, Suhaib A. Fahmy, Sebastian Steinhorst, Martin Lukasiewycz, and Samarjit Chakraborty. 2017. VEGa: A high performance vehicular Ethernet gateway on hybrid FPGA. *IEEE Transactions on Computers* 66, 10 (2017), 1790–1803.

[147] Shanker Shreejith and Suhaib A. Fahmy. 2015. Security aware network controllers for next generation automotive embedded systems. In *Proceedings of the 52nd Annual Design Automation Conference (DAC'15)*. ACM, Article 39, 6 pages.

[148] Faezeh Siavashi, Horacio Hoyos Rodriguez, Vera Pantelic, Mark Lawford, Richard F. Paige, Monika Jaskolka, Guanrui Hou, and Alessandro Verde. 2023. Bridging the gap between system architecture and software design using model transformation. In *Proceedings of the 34th IEEE International Symposium on Software Reliability Engineering (ISSRE'23)*.

[149] Neeraj Kumar Singh, Mark Lawford, Thomas Stephen Edward Maibaum, and Alan Wassyng. 2021. A formal approach to rigorous development of critical systems. *Journal of Software: Evolution and Process* 33, 4 (2021), e2334.

[150] Dario Stabili, Raffaele Romagnoli, Mirco Marchetti, Bruno Sinopoli, and Michele Colajanni. 2023. A multidisciplinary detection system for cyber attacks on powertrain cyber physical systems. *Future Generation Computer Systems* 144 (2023), 151–164.

[151] Aaron Steckelberg, Hannah Dormido, Ruby Mellen, Steven Rich, and Cate Brown. 2023. The underbelly of electric vehicles: What goes into making EVs, where it comes from and at what human cost. *The Washington Post*. Retrieved March 14, 2024 from https://www.washingtonpost.com/world/interactive/2023/electric-car-batteries-geography/

[152] Sebastian Steinhorst, Zili Shao, Samarjit Chakraborty, Matthias Kauer, Shuai Li, Martin Lukasiewycz, Swaminathan Narayanaswamy, Muhammad Usman Rafique, and Qixin Wang. 2016. Distributed reconfigurable battery system

management architectures. In *Proceedings of the 21st Asia and South Pacific Design Automation Conference (ASP-DAC'16)*.

[153] Hong-Tao Sun, Chen Peng, and Fei Ding. 2022. Self-discipline predictive control of autonomous vehicles against denial of service attacks. *Asian Journal of Control* 24, 6 (2022), 3538–3551.

[154] Xiaowu Sun, Haitham Khedr, and Yasser Shoukry. 2019. Formal verification of neural network controlled autonomous systems. In *Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control (HSCC'19)*.

[155] Ghizlane Tibba, Christoph Malz, Christoph Stoermer, Natarajan Nagarajan, Licong Zhang, and Samarjit Chakraborty. 2016. Testing automotive embedded systems under X-in-the-loop setups. In *Proceedings of the 35th International Conference on Computer-Aided Design (ICCAD'16)*.

[156] Bram van der Sanden and Alexandr Vasenev. 2020. Architectural guidance in automotive for privacy and security: Survey and classification. In *Proceedings of the IEEE International Systems Conference (SysCon'20)*.

[157] Yulei Wang, An Huang, Fan Yang, Jiazhi Zhang, Ning Bian, and Lulu Guo. 2023. Systematic assessment of cyber-physical security of lane keeping control system for autonomous vehicles. *Security and Safety* 2 (2023), 1–19.

[158] Yixuan Wang, Chao Huang, Zhaoran Wang, Zhilu Wang, and Qi Zhu. 2022. Design-while-verify: Correct-by-construction control learning with verification in the loop. In *Proceedings of the ACM/IEEE Design Automation Conference (DAC'22)*.

[159] Zhilu Wang, Chao Huang, Yixuan Wang, Clara Hobbs, Samarjit Chakraborty, and Qi Zhu. 2021. Bounding perception neural network uncertainty for safe control of autonomous systems. In *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition (DATE'21)*.

[160] Zhilu Wang, Hengyi Liang, Chao Huang, and Qi Zhu. 2021. Cross-layer design of automotive systems. *IEEE Design & Test* 38, 5 (2021), 8–16.

[161] Peter Waszecki, Philipp Mundhenk, Sebastian Steinhorst, Martin Lukasiewycz, Ramesh Karri, and Samarjit Chakraborty. 2017. Automotive electrical and electronic architecture security via distributed in-vehicle traffic monitoring. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 36, 11 (2017), 1790–1803.

[162] Guoqi Xie, Renfa Li, and Shiyan Hu. 2020. Security-aware obfuscated priority assignment for CAN FD messages in real-time parallel automotive applications. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 39, 12 (2020), 4413–4425.

[163] Guoqi Xie, Yanwen Li, Yunbo Han, Yong Xie, Gang Zeng, and Renfa Li. 2020. Recent advances and future trends for automotive functional safety design methodologies. *IEEE Transactions on Industrial Informatics* 16, 9 (2020), 5629–5642.

[164] Guoqi Xie, Laurence T. Yang, Yuanda Yang, Haibo Luo, Renfa Li, and Mamoun Alazab. 2021. Threat analysis for automotive CAN networks: A GAN model-based intrusion detection technique. *IEEE Transactions on Intelligent Transportation Systems* 22, 7 (2021), 4467–4477.

[165] Guoqi Xie, Gang Zeng, Yan Liu, Jia Zhou, Renfa Li, and Keqin Li. 2018. Fast functional safety verification for distributed automotive applications during early design phase. *IEEE Transactions on Industrial Electronics* 65, 5 (2018), 4378–4391.

[166] Guoqing Xu, Kun Xu, Chunhua Zheng, Xinye Zhang, and Taimoor Zahid. 2016. Fully electrified regenerative braking control for deep energy recovery and maintaining safety of electric vehicles. *IEEE Transactions on Vehicular Technology* 65, 3 (2016), 1186–1198.

[167] Shengjie Xu, Bineet Ghosh, Clara Hobbs, P. S. Thiagarajan, and Samarjit Chakraborty. 2023. Safety-aware flexible schedule synthesis for cyber-physical systems using weakly-hard constraints. In *Proceedings of the 28th Asia and South Pacific Design Automation Conference (ASP-DAC'23)*.

[168] Assioua Yasmine, Ameur-Boulifa Rabea, and Guitton-Ouhamou Patricia. 2020. Towards formal verification of autonomous driving supervisor functions. In *Proceedings of the 10th European Congress on Embedded Real Time Software and Systems (ERTS'20)*.

[169] Anand Yeolekar, Ravindra Metta, Clara Hobbs, and Samarjit Chakraborty. 2022. Checking scheduling-induced violations of control safety properties. In *Automated Technology for Verification and Analysis*. Lecture Notes in Computer Science, Vol. 13505. Springer, 100–116.

[170] Takahito Yoshizawa and Bart Preneel. 2023. A new approach to pseudonym certificate management in V2X communication. In *Proceedings of the IEEE Vehicular Networking Conference (VNC'23)*.

[171] Takahito Yoshizawa, Dave Singelée, Jan Tobias Mühlberg, Stéphane Delbruel, Amir Taherkordi, Danny Hughes, and Bart Preneel. 2023. A survey of security and privacy issues in V2X communication systems. *ACM Computin Surveys* 55, 9 (2023), Article 185, 36 pages.

[172] Gioele Zardini, Andrea Censi, and Emilio Frazzoli. 2021. Co-design of autonomous systems: From hardware selection to control synthesis. In *Proceedings of the European Control Conference (ECC'21)*.

[173] Daniel Zelle, Timm Lauser, Dustin Kern, and Christoph Krauß. 2021. Analyzing and securing SOME/IP automotive services with formal and practical methods. In *Proceedings of the 16th International Conference on Availability, Reliability, and Security (ARES'21).* ACM, Article 8, 20 pages.

[174] Hengrun Zhang, Kai Zeng, and Shuai Lin. 2023. Federated graph neural network for fast anomaly detection in controller area networks. *IEEE Transactions on Information Forensics and Security* 18 (2023), 1566–1579.

[175] Licong Zhang, Dip Goswami, Reinhard Schneider, and Samarjit Chakraborty. 2014. Task- and network-level schedule co-synthesis of Ethernet-based time-triggered systems. In *Proceedings of the 19th Asia and South Pacific Design Automation Conference (ASP-DAC'14).*

[176] Licong Zhang, Debayan Roy, Philipp Mundhenk, and Samarjit Chakraborty. 2016. Schedule management framework for cloud-based future automotive software systems. In *Proceedings of the 22nd IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'16).*

[177] Qingling Zhao, Mingqiang Chen, Zonghua Gu, Siyu Luan, Haibo Zeng, and Samarjit Chakraborty. 2022. CAN bus intrusion detection based on auxiliary classifier GAN and out-of-distribution detection. *ACM Transactions on Embedded Computing Systems* 21, 4 (2022), Article 45, 30 pages.

[178] Qi Zhu and Alberto L. Sangiovanni-Vincentelli. 2018. Codesign methodologies and tools for cyber-physical systems. *Proceedings of the IEEE* 106, 9 (2018), 1484–1500.

Received 25 February 2024; accepted 28 February 2024