Introduction to the Special Issue on Automotive CPS Safety & Security: Part 1

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

ACM Reference Format:
Samarjit Chakraborty, Somesh Jha, Soheil Samii, and Philipp Mundhenk. 2023. Introduction to the Special Issue on Automotive CPS Safety & Security: Part 1. 1, 1 (January 2023), 6 pages. https://doi.org/xx.xxxx/xxxxxxx.xxxxxxx

1 BACKGROUND

One might argue that automotive and allied domains like robotics serve as the best possible examples of what "cyber-physical systems" (CPS) are. Here, the correctness of the underlying electronics and software (or *cyber*) components are defined by the dynamics of the vehicle or the robot, *viz.*, the *physical* components of the system. This shift in perspective on how electronics and software should be modeled and synthesized, and how their correctness should be defined, has led to a tremendous volume of research on CPS in recent times [7, 8, 43, 56]. At the same time, the volume electronics and software in modern cars have also grown tremendously. Today, high-end cars have more than 100 control computers or electronic control units (ECUs) embedded in them, that run hundreds of millions of lines of software code implementing a range of diverse functions. These functions span across engine and brake control, to the body and entertainment domains. Cars are also equipped with a variety of cameras, radars, and lidar sensors that are used to perceive the external world and take the appropriate control actions as a part of driver assistance features that are common today. As such features continue to accelerate the evolution and adoption of fully autonomous vehicles, the role of electronics and software in the automotive domain is increasing at an unprecedented pace, and modern automobiles are now aptly referred to as "computers on wheels." These developments raise important questions about the *safety* and *security* of modern cars, which led to this special issue on Automotive CPS Safety & Security.

This special issue invited papers on a variety of topics at the intersection of automotive embedded systems, cyber-physical systems, and associated safety and security challenges and their solutions. In particular, the goal was to bring together perspectives from multiple research communities such as machine learning, formal verification, control theory, software engineering, security, fault tolerance, embedded systems and software,

Authors' addresses: Samarjit Chakraborty, samarjit@cs.unc.edu, University of North Carolina at Chapel Hill , Department of Computer Science, 201 S. Columbia St., Chapel Hill, NC 27599-3175, USA; Somesh Jha, University of Wisconsin-Madison, Department of Computer Sciences, UW-Madison, 1210 W. Dayton Street, Madison, WI 53706-1613, USA, jha@cs.wisc.edu; Soheil Samii, Linköping University, Dept. of Computer and Information Science, Linköping University, Linköping, SE-581 83, Sweden, soheil.samii@liu.se; Philipp Mundhenk, Robert Bosch GmbH, Robert Bosch GmbH Zentrum fÜr Forschung und Vorausentwicklung, Robert-Bosch-Campus 1, Renningen, DE 71272, Germany, Philipp.Mundhenk@bosch.com.

XXXX-XXXX/2023/1-ART $15.00
https://doi.org/xx.xxxx/xxxxxxx.xxxxxxx

vision processing, and real-time systems — all of whom are going to play an important role in shaping how future automobiles can be made more safe and secure. We received an overwhelming response to our call for submissions, which shows the importance and timeliness of this topic. As a result, this special issue will be divided into two parts – this Part 1 features seven quite interdisciplinary papers on different aspects of automotive CPS safety and security. The forthcoming Part 2 will feature the remaining papers. Before we introduce the papers in this Part 1 of the special issue, we briefly review some aspects of automotive safety and security. This review is only to set the context for this special issue, and by no means is meant to be detailed or complete. A more detailed review, to impress upon readers the variety of work that has been done in this area and the rich set of challenges that still remain, will be provided in the Part 2 of this special issue.

2 AUTOMOTIVE CYBER-PHYSICAL SYSTEMS AND THEIR SAFETY & SECURITY

Safety has always been an important engineering concern for the automotive domain. But with increased software volumes and electronics in cars, and automotive OEMs relying on many suppliers providing different electronics and software components, safety concerns are no longer restricted to the mechanical engineering domain. Automotive ECUs are also not simple microcontrollers any more, but are heterogeneous multicore processors with decreasing semiconductor geometries. Hence, these are susceptible to a variety of manufacturing variabilities, transient faults and aging issues, that might impact the software execution and the results they produce [9, 12, 13, 28]. Such concerns are amplified by the lack of cooling possibilities, more extreme temperature exposures and increased electromagnetic interferences that semiconductors in cars are subjected to, compared to their counterparts in regular computers.

The increasing complexity of software in cars and the associated scheduling [6, 27, 54] and management of such software also contributes to growing safety concerns. Unlike in regular computers, the correctness of the software – and in particular software responsible for critical functionality – is of crucial importance in the automotive domain. This has led to a variety of work on testing [3, 45] and formal verification of automotive control software [5, 17, 22, 48]. At the heart of most automotive control software lies feedback control loops, and as a result there are close ties between safety analysis and control theory in this domain. Towards this, control-theoretic techniques and reachability analysis have been used for safety verification [18, 19, 26, 50, 52]. Since modern automotive in-vehicle architectures are highly distributed and use multiple different communication buses, control signals are subject to varying delays that might additionally compromise the safety of the closed-loop system, even if the control strategy is functionally correct. Several publications have addressed this issue [16, 23, 31], including how to synthesize delay-tolerant controllers [10, 15, 34] and how to co-synthesize controllers and their underlying task schedules [4, 32, 39, 42, 53]. This is also related to providing timing isolation to critical control software [11, 14, 33] and the scheduling of mixed-criticality tasks [41]. Finally, a significant volume of recent work has been on emerging topics like electric [1, 29, 30, 51] and autonomous vehicles [20, 24, 40, 47] and safety issues arising in them.

In addition to these safety issues, security in the automotive domain is a growing concern [38]. Cars are increasingly becoming “connected” and communicate with the external world using a variety of mechanisms. These include communication between charging stations and battery management systems [44] in an electric vehicle, to over-the-air software updates, various vehicle-to-vehicle and vehicle-to-infrastructure communication mechanisms for autonomous and semi-autonomous vehicles, as well as infotainment connectivity options where passengers might wirelessly connect their smartphones to a vehicle’s electronics in order to control the air conditioner or heating or for streaming their music. In the future, software in cars will become more “dynamic” and will use external infrastructure such as the cloud [2, 54] for various computation tasks. The number of sensors on autonomous vehicles will also continue to grow. Each of these developments and connections with the external world will introduce new attack vectors and new possibilities for the vehicle’s safety to be compromised.

In order to mitigate these challenges, several different solutions have been proposed. These include using formal verification techniques like model checking [21, 36, 37] to establish security guarantees, and monitoring of in-vehicle traffic [25, 35, 49] to detect out of order behavior [55] and potential security breaches. Finally, the use of machine learning (ML) techniques [46] in autonomous vehicles, especially for perception processing introduce new safety and security vulnerabilities that have attracted considerable attention from the research community.

3 PAPERS IN THIS SPECIAL ISSUE

This Part 1 of the special issue features seven papers. The first paper, entitled "*$S\mathcal{L}_1$-Simplex: Safe Velocity Regulation of Self-Driving Vehicles in Dynamic and Unforeseen Environments* by Mao *et al.* augments the well-known Simplex architecture – that allows safe mode changes and component replacements at run time – with online model learning within the context of $\mathcal{L}_1$ adaptive controllers. This integration of $\mathcal{L}_1$ adaptive controllers, safe controller switching, and finite-time model learning allows tracking in self-driving vehicles in dynamic and unforeseen environments. The second paper, entitled "*CASCADE: An Asset-driven Approach to Build Security Assurance Cases for Automotive Systems*" by Mohamad *et al.* proposes a methodology for building security assurance cases, where assurance cases are structured sets of arguments and evidence that establish certain properties of a system. The proposed methodology was used to validate ISO/SAE-21434 requirements in an industrial automotive case study.

While machine learning techniques for intrusion detection by identifying anomalies in traffic patterns have been well-studied in the past, the third paper "*DT-DS: CAN Intrusion Detection with Decision Tree Ensembles*" by Mehta *et al.* shows that decision tree-based learning ensembles can outperform anomaly-based intrusion detection techniques. The paper also studies optimal parameterizations of tree-based learning ensembles. Similarly, known architectural patterns are often used to provide guarantees on security and fault tolerance. But such patterns might also introduce new security threats or faults. The fourth paper, entitled "*Automating Safety and Security Co-Design through Semantically-Rich Architecture Patterns*" by Dantas and Nigam proposes a domain specific language for specifying architectural patterns, and a method for checking whether an introduced pattern attains the targeted safety goal. This is done co-designing safety and security reasoning rules and using automated reasoning techniques.

The fifth paper, entitled "*SchedGuard++: Protecting against Schedule Leaks Using Linux Containers On Multi-core Processors*" by Chen *et al.* studies methods for mitigating timing attacks in autonomous driving systems by proposing a temporal protection framework for Linux-based real-time systems. This framework works on multi-core platforms and uses Linux containers and a customized real-time scheduler. Security has traditionally not been a first class citizen in the design of automotive software. Security mechanisms have been added as an afterthought after most of the design is frozen. However, as outlined earlier in this introduction, as modern vehicles are becoming more connected, their security vulnerabilities are also significantly increasing, thereby necessitating mechanisms for estimating their security vulnerability. The sixth paper of this special issue, entitled "*CAD support for Security and Robustness Analysis of Safety-Critical Automotive Software*" by Koley *et al.* studies formal models of automotive controllers and determines their safety and robustness by injecting different attacks, and identifying which sensor and actuation signals are vulnerable. Finally, the seventh and the last paper, entitled "*Security Risk Assessments: Modeling and Risk-Level Propagation*" by Angermeier *et al.* proposes modeling techniques to bridge the gap between software development models and those used for security assessment. This allows automotive systems and security engineers to jointly develop and assess models, where security-specific requirements can be traced back to modules relevant for systems development. This can then trigger extensions or refinements in functional modeling, thereby enabling a more holistic development process.

We believe that this special issue will further enrich the already active and interdisciplinary areas of safety and security in automotive cyber-physical systems. We further hope that our readers will not only find these articles to be interesting, but through them will be able to gain new insights into this fast evolving area. We would also

like to thank all the reviewers, the EiC of ACM TCPS – Chenyang Lu – and all members of the TCPS editorial team, especially Rebecca Malone and Gita Delsing, without whose help and continuous support this special issue would not have been possible.

REFERENCES

[1] R. Aalund, W. Diao, L. Kong, and M. G. Pecht. 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*, 9:89527–89532, 2021.

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

[3] P. Baumann, M. Krammer, M. Driussi, L. Mikelsons, J. Zehetner, W. Mair, and D. Schramm. Using the distributed co-simulation protocol for a mixed real-virtual prototype. In *IEEE International Conference on Mechatronics (ICM)*, 2019.

[4] L. Bhatia, I. Tomic, A. Fu, M. Breza, and J. A. McCann. Control communication co-design for wide area cyber-physical systems. *ACM Trans. Cyber Phys. Syst.*, 5(2):18:1–18:27, 2021.

[5] M. Broy, S. Chakraborty, D. Goswami, S. Ramesh, M. Satpathy, S. Resmerita, and W. Pree. Cross-layer analysis, testing and verification of automotive control software. In *11th International Conference on Embedded Software (EMSOFT)*, 2011.

[6] S. Chakraborty, T. Erlebach, and L. Thiele. On the complexity of scheduling conditional real-time code. In *7th International Workshop on Algorithms and Data Structures (WADS)*, volume 2125 of *Lecture Notes in Computer Science*. Springer, 2001.

[7] S. Chakraborty, M. A. A. Faruque, W. Chang, D. Goswami, M. Wolf, and Q. Zhu. Automotive cyber-physical systems: A tutorial introduction. *IEEE Des. Test*, 33(4):92–108, 2016.

[8] W. Chang and S. Chakraborty. Resource-aware automotive control systems design: A cyber-physical systems approach. *Found. Trends Electron. Des. Autom.*, 10(4):249–369, 2016.

[9] W. Chang, A. Pröbstl, D. Goswami, M. Zamani, and S. Chakraborty. Battery- and aging-aware embedded control systems for electric vehicles. In *35th IEEE Real-Time Systems Symposium (RTSS)*, 2014.

[10] S. De, S. Mohamed, D. Goswami, and H. Corporaal. Approximation-aware design of an image-based control system. *IEEE Access*, 8:174568–174586, 2020.

[11] J. Freitag, S. Uhrig, and T. Ungerer. Virtual timing isolation for mixed-criticality systems. In *30th Euromicro Conference on Real-Time Systems (ECRTS)*, 2018.

[12] F. H. Gandoman, A. Ahmadi, P. V. den Bossche, J. V. Mierlo, N. Omar, A. E. Nezhad, H. Mavalizadeh, and C. Mayet. Status and future perspectives of reliability assessment for electric vehicles. *Reliab. Eng. Syst. Saf.*, 183:1–16, 2019.

[13] G. Georgakos, U. Schlichtmann, R. Schneider, and S. Chakraborty. Reliability challenges for electric vehicles: from devices to architecture and systems software. In *50th Annual Design Automation Conference (DAC)*, 2013.

[14] K. Goossens, A. Azevedo, K. Chandrasekar, M. D. Gomony, S. Goossens, M. Koedam, Y. Li, D. Mirzoyan, A. M. Molnos, A. B. Nejad, A. Nelson, and S. Sinha. Virtual execution platforms for mixed-time-criticality systems: the compsoc architecture and design flow. *SIGBED Rev.*, 10(3):23–34, 2013.

[15] D. Goswami, R. Schneider, and S. Chakraborty. Re-engineering cyber-physical control applications for hybrid communication protocols. In *Design, Automation and Test in Europe (DATE)*, 2011.

[16] D. Goswami, R. Schneider, and S. Chakraborty. Relaxing signal delay constraints in distributed embedded controllers. *IEEE Trans. Control. Syst. Technol.*, 22(6):2337–2345, 2014.

[17] L. Guo, Q. Zhu, P. Nuzzo, R. Passerone, A. L. Sangiovanni-Vincentelli, and E. A. Lee. Metronomy: A function-architecture co-simulation framework for timing verification of cyber-physical systems. In *International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)*, 2014.

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

[19] C. Hobbs, B. Ghosh, S. Xu, P. S. Duggirala, and S. Chakraborty. Safety analysis of embedded controllers under implementation platform timing uncertainties. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, 41(11):4016–4027, 2022.

[20] C. Hobbs, D. Roy, P. S. Duggirala, F. D. Smith, S. Samii, J. H. Anderson, and S. Chakraborty. Perception computing-aware controller synthesis for autonomous systems. In *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2021.

[21] L. Huang and E. Kang. Formal verification of safety & security related timing constraints for a cooperative automotive system. In *22nd International Conference on Fundamental Approaches to Software Engineering (FASE)*, volume 11424 of *Lecture Notes in Computer Science*. Springer, 2019.

[22] L. Ju, B. K. Huynh, A. Roychoudhury, and S. Chakraborty. Performance debugging of Esterel specifications. In *6th International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)*, 2008.

[23] C. Jugade, D. Hartgers, P. D. Anh, S. Mohamed, M. Haghi, D. Goswami, A. Nelson, G. van der Veen, and K. Goossens. An evaluation framework for vision-in-the-loop motion control systems. In *27th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2022.

[24] L. Kang and H. Shen. A control policy based driving safety system for autonomous vehicles. In *IEEE 18th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, 2021.

[25] L. Kang and H. Shen. Detection and mitigation of sensor and CAN bus attacks in vehicle anti-lock braking systems. *ACM Trans. Cyber Phys. Syst.*, 6(1):9:1–9:24, 2022.

[26] M. Kauer, D. Soudbakhsh, D. Goswami, S. Chakraborty, and A. M. Annaswamy. Fault-tolerant control synthesis and verification of distributed embedded systems. In *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2014.

[27] Z. Li, T. Chu, I. V. Kolmanovsky, X. Yin, and X. Yin. Cloud resource allocation for cloud-based automotive applications. *CoRR*, abs/1701.04537, 2017.

[28] Z. Li, C. Huang, X. Dong, and C. Ren. Resource-efficient cyber-physical systems design: A survey. *Microprocess. Microsystems*, 77:103183, 2020.

[29] M. Lukasiewycz et al. Cyber-physical systems design for electric vehicles. In *15th Euromicro Conference on Digital System Design (DSD)*, 2012.

[30] M. Lukasiewycz et al. System architecture and software design for electric vehicles. In *50th Annual Design Automation Conference (DAC)*, 2013.

[31] M. Maggio, A. Hamann, E. Mayer-John, and D. Ziegenbein. Control-system stability under consecutive deadline misses constraints. In *32nd Euromicro Conference on Real-Time Systems (ECRTS)*, volume 165 of *LIPIcs*, pages 21:1–21:24. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[32] R. Mahfouzi, A. Aminifar, S. Samii, A. Rezine, P. Eles, and Z. Peng. Breaking silos to guarantee control stability with communication over ethernet TSN. *IEEE Des. Test*, 38(5):48–56, 2021.

[33] A. Masrur, S. Drössler, T. Pfeuffer, and S. Chakraborty. VM-based real-time services for automotive control applications. In *16th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA)*, 2010.

[34] S. Mohamed, D. Goswami, V. Nathan, R. Rajappa, and T. Basten. A scenario- and platform-aware design flow for image-based control systems. *Microprocess. Microsystems*, 75:103037, 2020.

[35] H. Mun, K. Han, and D. H. Lee. Ensuring safety and security in can-based automotive embedded systems: A combination of design optimization and secure communication. *IEEE Trans. Veh. Technol.*, 69(7):7078–7091, 2020.

[36] P. Mundhenk, S. Steinhorst, M. Lukasiewycz, S. A. Fahmy, and S. Chakraborty. Security analysis of automotive architectures using probabilistic model checking. In *52nd Annual Design Automation Conference (DAC)*, 2015.

[37] L. Pike, J. Sharp, M. Tullsen, P. C. Hickey, and J. Bielman. Secure automotive software: The next steps. *IEEE Softw.*, 34(3):49–55, 2017.

[38] S. Ray, A. Sadeghi, and M. A. A. Faruque. Guest editors' introduction: Secure automotive systems. *IEEE Des. Test*, 36(6):5–6, 2019.

[39] D. Roy, L. Zhang, W. Chang, D. Goswami, and S. Chakraborty. Multi-objective co-optimization of flexray-based distributed control systems. In *IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)*, 2016.

[40] K. Samal, M. Wolf, and S. Mukhopadhyay. Closed-loop approach to perception in autonomous system. In *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2021.

[41] R. Schneider, D. Goswami, A. Masrur, M. Becker, and S. Chakraborty. Multi-layered scheduling of mixed-criticality cyber-physical systems. *J. Syst. Archit.*, 59(10-D):1215–1230, 2013.

[42] R. Schneider, D. Goswami, S. Zafar, M. Lukasiewycz, and S. Chakraborty. Constraint-driven synthesis and tool-support for flexray-based automotive control systems. In *9th International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS)*, 2011.

[43] S. A. Seshia, S. Hu, W. Li, and Q. Zhu. Design automation of cyber-physical systems: Challenges, advances, and opportunities. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, 36(9):1421–1434, 2017.

[44] S. Steinhorst et al. Distributed reconfigurable battery system management architectures. In *21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2016.

[45] G. Tibba, C. Malz, C. Stoermer, N. Nagarajan, L. Zhang, and S. Chakraborty. Testing automotive embedded systems under X-in-the-loop setups. In *35th International Conference on Computer-Aided Design (ICCAD)*, 2016.

[46] Y. Wang, C. Huang, Z. Wang, Z. Wang, and Q. Zhu. Design-while-verify: correct-by-construction control learning with verification in the loop. In *ACM/IEEE Design Automation Conference (DAC)*, 2022.

[47] Z. Wang, C. Huang, Y. Wang, C. Hobbs, S. Chakraborty, and Q. Zhu. Bounding perception neural network uncertainty for safe control of autonomous systems. In *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2021.

[48] Z. Wang, H. Liang, C. Huang, and Q. Zhu. Cross-layer design of automotive systems. *IEEE Des. Test*, 38(5):8–16, 2021.

[49] P. Waszecki, P. Mundhenk, S. Steinhorst, M. Lukasiewycz, R. Karri, and S. Chakraborty. Automotive electrical and electronic architecture security via distributed in-vehicle traffic monitoring. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, 36(11):1790–1803, 2017.

[50] G. Xie, G. Zeng, Y. Liu, J. Zhou, R. Li, and K. Li. Fast functional safety verification for distributed automotive applications during early design phase. *IEEE Trans. Ind. Electron.*, 65(5):4378–4391, 2018.

[51] G. Xu, K. Xu, C. Zheng, X. Zhang, and T. Zahid. Fully electrified regenerative braking control for deep energy recovery and maintaining safety of electric vehicles. *IEEE Trans. Veh. Technol.*, 65(3):1186–1198, 2016.

[52] A. Yeolekar, R. Metta, C. Hobbs, and S. Chakraborty. Checking scheduling-induced violations of control safety properties. In *20th International Symposium on Automated Technology for Verification and Analysis (ATVA)*, volume 13505 of *Lecture Notes in Computer Science*. Springer, 2022.

[53] G. Zardini, A. Censi, and E. Frazzoli. Co-design of autonomous systems: From hardware selection to control synthesis. In *2021 European Control Conference (ECC)*, 2021.

[54] L. Zhang, D. Roy, P. Mundhenk, and S. Chakraborty. Schedule management framework for cloud-based future automotive software systems. In *22nd IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA)*, 2016.

[55] Q. Zhao, M. Chen, Z. Gu, S. Luan, H. Zeng, and S. Chakraborty. CAN bus intrusion detection based on auxiliary classifier GAN and out-of-distribution detection. *ACM Trans. Embed. Comput. Syst.*, 21(4):45:1–45:30, 2022.

[56] Q. Zhu and A. L. Sangiovanni-Vincentelli. Codesign methodologies and tools for cyber-physical systems. *Proc. IEEE*, 106(9):1484–1500, 2018.