XANDAR: A holistic Cybersecurity Engineering Process for Safety-critical and Cyber-physical Systems

Fahad Siddiqui[1], Rafiullah Khan[1], Sakir Sezer[1], Kieran McLaughlin[1], Vahid Garousi[1], Leonard Masing[2]
Tobias Dörr[2], Florian Schade[2], Jürgen Becker[2], Alexander Ahlbrecht[3], Wanja Zaeske[3], Umut Durak[3]
Nico Adler[4], Andreas Sailer[4], Raphael Weber[4], Thomas Wilhelm[4], Geza Nemeth[5], Victor Morales[6]
Paco Gomez[6], Georgios Keramidas[7,9], Christos P. Antonopoulos[7], Michail Mavropoulos[7], Vasilios Kelefouras[7]
Konstantinos Antonopoulos[7], Nikolaos Voros[6], Christos Panagiotou[8] and Dimitris Karadimas[8]
[1]Queen's University Belfast, United Kingdom
Email: f.siddiqui, rafiullah.khan, s.sezer, kieran.mclaughlin, v.garousi@qub.ac.uk
[2]Karlsruhe Institute of Technology (KIT), Germany
[3]German Aerospace Center (DLR), Institute of Flight Systems, Germany
[4]Vector Informatik GmbH, Germany
[5]Bayerische Motoren Werke Aktiengesellschaft (BMW), Germany
[6]Fent Innovative Software Solutions (fentISS), SL, Spain
[7]University of Peloponnese, Greece
[8]AVN Innovative Technology Solutions Limited, Cyprus
[9]Aristotle University of Thessaloniki, Greece

***Abstract*—The integration of connected and autonomous technologies in safety-critical and cyber-physical systems offers great potential in the vital application domains of transportation, manufacturing, energy, defence, and aerospace. These technological advancements are necessary to meet the increasing demand for intelligent services. Because they are opening doors to new business models and improving consumer experience by analysing and sharing the generated data. However, where this sharing of mix-critical data and broader connectivity brings opportunities, it simultaneously presents serious cybersecurity and safety risks due to the cyber-physical nature of these systems. Therefore, delivering these intelligent services securely, safely, and reliably to its consumers is a complex engineering and design problem. One of the ways to approach this engineering problem is to consider both system functional and non-functional properties (safety, security, reliability) and systematically integrate them across system design and operational life cycle. In the XANDAR project, partners from both academia and industry are investigating this approach. The aim is to develop holistic software design methods and architectures for safety-critical and cyber-physical systems that guarantee functional and non-functional properties *"by-construction"*. This paper focuses on the non-functional aspects of the project and discusses the preliminary work. It presents the core cybersecurity principles driven from the guidance of cybersecurity guidance, frameworks, uses them as a baseline to propose a holistic cybersecurity engineering process. The tasks of the proposed cybersecurity engineering process are also map onto relevant clauses of ISO 21434. In future, proposed work will be integrated into the XANDAR software toolchain and validated for an avionics situation perception pilot assistance and automotive autonomous driving use cases.**

***Index Terms*—Cybersecurity Engineering, Cyber-physical, Safety-critical, Cyber Resilience, Secure-by-design, Threat Analysis, Risk Assessment, Runtime Monitoring, ISO 21434.**

I. Introduction

One of the advancements initiated by the *edge computing* paradigm [1] is the realisation of *cyber-physical convergence* [2], [3], where the data-driven control decisions made in the cyber-domain executes in the physical-domain. Mass deployment of cyber-physical systems has been underway in public, private, commercial and non-commercial critical services to optimise business processes and enhance customer experience by analysing and sharing the generated data.

Smart Mobility is one of the leading applications of a cyber-physical system. It offers a great potential to make transport systems autonomous, efficient, reliable and safer. It has been estimated that by 2030, the number of autonomous vehicles will reach 90 million worldwide [4]. The UK department of transport predicts that the autonomous vehicles business would be worth £41.7 billion by 2035 [5]. This market trend has been driven by evolving demands for intelligent features from both consumers and manufacturers. The customers are demanding personalised mobility experience, which requires software-defined system adaptability to enable, disable, update existing or add new intelligent services [6]. The vehicle manufacturers are interested in introducing a capability to fix, update, monitor and maintain system software and services during the operational life cycle of a vehicle *i.e.* after the vehicle leave the factory floor into the real world. It will help manufacturers to avoid expensive vehicle recalls [7], [8] and enable them to tap into the valuable real-world vehicle data. An appropriate use of valuable generated data can help to improve cybersecurity, safety, reliability posture and predictive

maintenance methods to reduce cost and system downtime. It will also facilitate manufacturers to achieve and maintain compliance of their systems with both existing and evolving cybersecurity engineering standards such as ISO 21434.

Though where these advancements and broader connectivity brings benefits, they equally increase the system attack surface, exposing safety-critical and cyber-physical systems to a wide range of cyber attacks [9], [10]. In 2017, researchers from Keen Security Lab were successful to install malware and remotely control Tesla Model S braking, side mirrors and locking system [11]. According to a report published in 2021, remote attacks have consistently outnumbered physical attacks, accounting for 79% of all attacks between 2010 and 2020. Where an alarming 77.8% of all these attacks were launched in 2020 alone [4]. The reported cyber attacks have impacted every segment of a connected vehicle and now rapidly extending towards autonomous vehicles. The existing (known) automotive system vulnerabilities can manipulate an alarming 23% of vehicle control and safety-critical systems [4]. These cybersecurity risks raise concerns about the safety of passengers, pedestrians and the security of critical road infrastructure.

One way to approach this complex engineering problem is considering both functional and non-functional properties (safety, security, reliability), and systematically integrating them across system design and operational life cycle. The XANDAR project proposes an *X-by-Construction* approach [12], [13], which advocates the refinement and adoption of holistic cybersecurity engineering process. It shall allow manufacturers of safety-critical and cyber-physical system manufacturers to scope, identify, analyse and assess the cybersecurity risks and safety hazards [14]. It will provide foundations to systematically define and architect a layered system security architecture, by deploying various system-level defences. Thus allowing to enhance the system's cybersecurity posture by making them resilient against cyber attacks.

This paper focuses solely on the non-functional aspects of the project and builds upon previous publications [12], [13]. It presents the holistic cybersecurity engineering process guided by ISO 21434, as part of the initial project planning stage. Since the project is in the early stages, this paper focuses on the bigger picture and presents the envisaged approach and does not intend to provide technical details.

II. EU-Project: X-by-Construction Design Framework for Autonomous and Distributed Real-time Embedded Systems (XANDAR)

One of the project goals is to improve software development productivity and quality for autonomous and distributed real-time embedded systems [12], [13]. This goal can be achieved by providing holistic software design methods and architectures that guarantee functional and non-functional properties *"by-construction"* defined as [15]:

"A step-wise refinement process from specification to code that automatically generates software implementations that by construction satisfy specific functional and non-functional properties."

One of the non-functional objectives of this project is to design and develop interoperable, trustworthy and adaptive system architecture for safety-critical and cyber-physical systems. From the cybersecurity prospective, this requires a holistic cybersecurity engineering process to identify, analyse and assess the risks, threats and hazards to the system. As a first step to lay down the foundations, the critical guidance from international cybersecurity guidelines and frameworks are considered and discussed in Section III. The project consortium consists of the following eight European academic and industrial partners:

1) ***The Queen's University of Belfast*** is leading the cybersecurity for safety-critical system, focusing on cybersecurity engineering processes and platform security.
2) ***Karlsruhe Institute of Technology*** is coordinating the project, leading the design and development of dynamic modelling extension and automatic software generation.
3) ***The University of the Peloponnese*** is leading the design and development of a reliable safety-critical software architecture focusing on compiler-level transformations.
4) ***Bayerische Motoren Werke (BMW)*** is the world leader in automotive, providing domain-specific technical support, guidance and the automotive use case.
5) ***German Aerospace Center (DLR)*** is the world leader in avionics, providing domain-specific technical support, guidance and the avionics use case.
6) ***Vector Informatik GmbH*** is the leading automotive software tool supplier, providing technical support in design and development of model-based system software.
7) ***fent Innovative Software Solutions (fentISS)*** is a leading supplier of software solutions specifically designed for critical real-time embedded partitioned systems using virtualization techniques, providing XtratuM hypervisor.
8) ***AVN Innovative Technology Solutions Limited*** is providing and maintaining the continuous integration and deployment platform for the project.

III. Cybersecurity Guidelines & Frameworks

A. Guiding principles for designing Secure Cyber-Physical Systems (NCSC, United Kingdom)

National Cyber Security Centre (NCSC) has developed a set of principles (Fig. 1) to guide system security designers in the design and development of cyber-physical systems [16]:

1) **Establish the context before designing a system** - Before you can create a secure system design, you need to have a good understanding of the fundamentals and take action to address any identified shortcomings.
2) **Make compromise difficult** - Designing systems with security in mind means applying concepts and techniques that make it harder for attackers to compromise a system and its data.
3) **Make disruption difficult** - When critical services rely on technology for delivery, it becomes essential that the technology is always available. The acceptable percentage of 'down time' can be effectively zero.

4) **Make compromise detection easier** - Even if you take all available precautions, there's still a chance your system will be compromised by a new or unknown attack. Therefore to spot these attacks, you should be well-positioned to detect compromise.
5) **Reduce the impact of compromise** - Design to naturally minimise the severity of any compromise.

B. Cybersecurity Framework (NIST, United States)

National Institute of Standards and Technology (NIST) Cybersecurity Framework [17] aims to improve the security of the critical infrastructure. This cybersecurity framework provides a uniform set of rules, guidelines, and standards for organizations to use across industries vital to national and economic security, including transportation, energy, banking, communication, and industrial base. It provides a set of guidelines for technology manufacturers to follow and better prepare to handle cyber attacks, particularly where a lack of security standardisation exists. The framework defines five core security functions (*identify*, *detect*, *protect*, *respond* and *recover*) as illustrated in Fig. 1, to establish, maintain and improve cyber resilience [18].

C. Security Pillars (Elektrobit, Germany)

Elektrobit provides comprehensive and proven solutions and services to protect connected cars and commercial vehicles against cyber attacks. Elektrobit has published their security philosophy [19] to approach the complex cybersecurity challenges of the automotive industry. This security philosophy is based on three critical pillars which are *prevent*, *understand* and *respond* as shown in Fig. 1. Elektrobit advocates the adoption of these critical pillars in the automotive systems design process such that car makers should always be able to prevent, understand and respond to cyber threats.

After going through these cybersecurity guidelines (Fig. 1), it can be inferred that there is a need for a holistic cybersecurity engineering process. A process that helps to scope, identify, analyse and assess the cybersecurity risks and safety hazards. But also encompass both the system design and the operational life cycle of a system. For this purpose, the gained knowledge (from the discussed cybersecurity standards, frameworks and guidelines) is synthesised and used to derive the core cybersecurity principles in Section IV.

IV. Core Cybersecurity Principles

To secure the life cycle of a safety-critical and cyber-physical system, the security shall be built, baked into the system from the ground-up [20], [21] rather than an afterthought. To design such a secure-by-design system requires an engineering process that allow a capability to:

- Identify system critical assets, services to define the cybersecurity requirements during the concept phase.
- Assess the threats to these system's assets, and hazards to critical services by conducting a detailed use-case driven threat, hazard analysis and risk assessment.

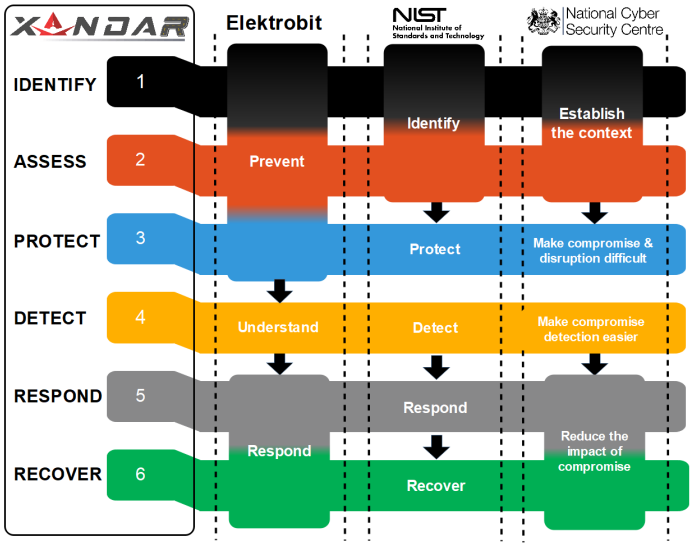

Fig. 1. Core cybersecurity principles driven from the discussed cybersecurity guidelines and frameworks.

- Define necessary system cybersecurity defences (based on the decisions of threat and hazard assessments) to harden system security posture.
- Update and maintain system cybersecurity posture during the operational life cycle of the system. It is necessary for handling threats posed by the discovery of new system vulnerabilities and attack vectors.
- Comply all stages of system life cycle with both existing and evolving national and international cybersecurity standards (ISO 21434, ISO 24089, NIST SP 800-160), guidelines, and best practices.

After identifying the high-level cybersecurity engineering requirements and reviewing the cybersecurity guidelines, the six core cybersecurity principles have been derived as shown in Fig. 1. These principles are ① *Identify*, ② *Assess*, ③ *Protect*, ④ *Detect*, ⑤ *Respond*, ⑥ *Recover*, which encompass and complement the international cybersecurity frameworks. These principles will serve as cornerstones for the proposed cybersecurity engineering process presented in Section V.

V. Holistic Cybersecurity Engineering Process

To approach the discussed cybersecurity engineering challenges of cyber-physical systems, this section proposes a holistic risk-oriented cybersecurity engineering process and its relevant tasks as illustrated in Fig. 2. It presents the necessary design and development activities, maps them onto the driven core cybersecurity principles (Section IV) as well as on to the identified system phases i.e. *scoping, assessment, modelling, generation, runtime* as illustrated in Fig. 2. Furthermore to establish a cybersecurity baseline, the proposed tasks are map onto the relevant clauses of ISO 21434 cybersecurity engineering standard. This cyberseurity engineering process can help manufacturers and suppliers of safety-critical and cyber-physical systems to effectively realise and manage cy-

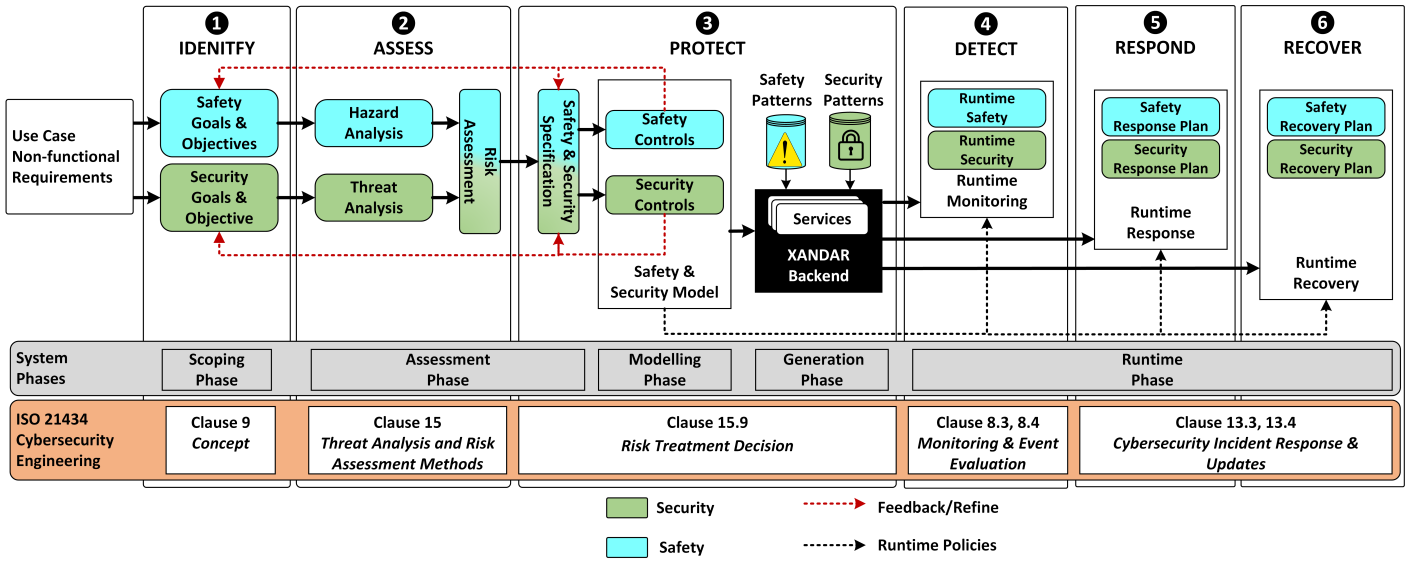

Fig. 2. Block diagram of the proposed cybersecurity engineering process, guided by ISO 21434 standard. It shows both the safety and security engineering activities, and their required interactions during different phases of the system design and development life cycle.

bersecurity risks across the system life cycle. The following are the salient details of each task:

① **IDENTIFY –** during scoping phase, gather/capture the use case non-functional requirements to identify the appropriate security and safety requirements under the given context. These requirements allow to define security, safety goals and objectives (Fig. 2), and to establish necessary system management policies. This task can be used to define cybersecurity concept *(Clause 9)* of ISO 21434.

② **ASSESS –** analyse and assess the risks to the system assets and safety-critical services of the application use case. This activity includes considering system deployment scenarios to establish the right context, which plays a critical role during the assessment phase of the system as illustrated in Fig. 2. This risk-oriented approach helps to determine and assess the business's safety and security risks, generally defined, and regulated by the certification authorities and domain-specific standards. This can be determined first by identifying the system's assets. Second identifying threats to these system's assets. Third identifying hazards to system-critical services. Fourth estimating the likelihood that identified threats/hazards will be materialised. Lastly the impact of each threat/hazard on the system's safety and security operations. The activities defined in this task shall facilitate realisation of threat analysis and risk assessment *(Clause 15)* of ISO 21434. The outcome of this process is the quantitative analysis of security threats and safety hazards that facilitates system security architect to make informed decisions and choose appropriate risk mitigation strategy i.e., accept, avoid, control or transfer the risk.

③ **PROTECT –** based on the chosen risk mitigation strategy, the system security architect methodically defines the system safety and security model during the modelling phase of the system. This task takes the assessed conditions, i.e., the results of quantitative analysis (hazard and threat analysis) on system operations, use them to define appropriate system safety and security specification, and choose a suitable safety and security control to mitigate/minimise the probability and damage caused by each considered risks and hazards. In the system generation phase, the defined safety and security model shall be realised by deploying these safety and security controls. In XANDAR project, safety and security controls will be automatically generated by the XANDAR software backend. A pattern-based approach will be used to harden security and enhance safety of the system software services. This task shall facilitate the process of choosing an appropriate risk treatment decision *(Clause 15.9)* of ISO 21434.

④ **DETECT –** adopt runtime system monitoring approach to monitor activities of a software services. This enables a capability to check whether the execution of a software services is in-line with the defined safety and security specification, which helps detection of software malfunctions, errors, faults, and adversarial activities. This task shall leverage the well-established runtime technologies to ensure spatial and temporal partitioning among mix-critical systems services and resources, and to detect policy violation. This task can facilitate runtime cybersecurity monitoring, an essential continual cybersecurity activity *(Clause 8.3, 8.4)* of ISO 21434.

⑤ **RESPOND –** formulate appropriate safety and security response plan for each security and safety violation for the system runtime phase. This task shall involve the selection of appropriate corrective control for each risk in accordance with the chosen risk mitigation strategy in task ②. The integration of these corrective controls shall facilitate a system-level capability to continuously monitor system activities, confine software faults/errors and curtail the impact of security and safety policy violation enforced by the runtime system. This task can facilitate an essential continual cybersecurity activity *(Clause 13.3, 13.4)* of ISO 21434.

⑥ **RECOVER –** initiate appropriate safety and security recovery plan during the runtime phase to ensure safety and security, maintain availability and reliability of the system operations. This includes the selection of appropriate recovery strategy i.e. (fail-open, fail-close, fail-safe, fail-secure) for each or group of safety and security violations. This will allow to confine encountered accidental software errors, faults and manage unintended malicious attacks, by maintaining a secure and safe system state/operation. It can facilitate operations and maintenance activities *(Clause 13.3, 13.4)* of ISO 21434.

In the XANDAR project, the tasks ③,④,⑤,⑥ initially will be focused on data confidentiality, data integrity and data authentication functions as required by the automotive and avionics application use cases [13]. It will involve:

- Use of data encryption methods at-rest and in-motion to protect confidentiality of system software and data communication interfaces.
- Use of data integrity methods to detect data tampering.
- Use of digital signature methods to authenticate and verify integrity of the software and detect compromise.
- Use of secure boot, on-boarding and off-boarding of software services to maintain secure life cycle management.
- Use of runtime technology to isolate, segregate and enforce appropriate system security policies.
- Leverage platform's built-in safety and security features to respond and recover the system to its safe state.

VI. Conclusion & Future Work

The XANDAR project aims to investigate software design methods and architectures for safety-critical and cyber-physical systems, that guarantee both functional and non-functional properties *"by-construction"*. This paper has introduced the six core cybersecurity principles to lay down the foundation for the proposed holistic cybersecurity engineering process. To establish a cybersecurity baseline for safety-critical and cyber-physical systems, the proposed tasks are mapped on the ISO 21434 clauses. This process allow hardening of cybersecurity posture aligned with ISO 21434, by choosing appropriate defence methods to detect, respond and recover the system's safety-critical functions against malicious attacks. To realise the proposed cybersecurity engineering process the first step is to identify the XANDAR use case security requirements and then conduct threat analysis and risk assessment to define the security model. The future project publications will realise the proposed work by implementing avionics situation perception pilot assistance and automotive autonomous driving use cases.

Acknowledgement

This research work was funded by the European Union's Horizon 2020 Research and Innovation Programme under Grant 957210 (XANDAR).

References

[1] P. Garcia Lopez, A. Montresor, D. Epema, A. Datta *et al.*, "Edge-Centric Computing: Vision and Challenges," *SIGCOMM Comput. Comm. Rev.*, vol. 45, no. 5, p. 37–42, Sep. 2015.

[2] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Design Automation Conference*, Anaheim, USA, 2010, pp. 731–736.

[3] M. Conti, S. K. Das, C. Bisdikian, M. Kumar *et al.*, "Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber–physical convergence," *Pervasive and Mobile Computing*, vol. 8, no. 1, pp. 2–21, 2012.

[4] (2021) Upstream Security's 2021 Global Automotive Cybersecurity Report. [Online]. Available: https://upstream.auto/2021report/

[5] (2021) UK on the cusp of a transport revolution, as self-driving vehicles set to be worth nearly £42 billion by 2035. [Online]. Available: https://www.gov.uk/government/news/uk-on-the-cusp-of-a-transport-revolution-as-self-driving-vehicles-set-to-be-worth-nearly-42-billion-by-2035

[6] B. Kim and S. Park, "ECU Software Updating Scenario Using OTA Technology through Mobile Communication Network," in *IEEE 3rd International Conference on Communication and Information Systems (ICCIS)*, Singapore, 2018, pp. 67–72.

[7] (2021) Volkswagen recalls Audi A3s on passenger air bag concerns. [Online]. Available: https://eu.usatoday.com/story/money/2021/03/27/vehicle-recall-check-volkswagen-recalls-audi-a-3-s-air-bag-concerns/7028190002/

[8] (2021) Daimler will recall 2.6M Mercedes cars in China. [Online]. Available: https://europe.autonews.com/automakers/daimler-will-recall-26m-mercedes-cars-china

[9] K. Kim, J. S. Kim, S. Jeong, J.-H. Park *et al.*, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Computers & Security*, vol. 103, p. 102150, 2021.

[10] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam *et al.*, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.

[11] (2017) Keen Lab hackers managed to take control of Tesla vehicles again. [Online]. Available: https://electrek.co/2017/07/28/tesla-hack-keen-lab/

[12] J. Becker, L. Masing, T. Dörr, F. Schade *et al.*, "XANDAR: X-by-Construction Design framework for Engineering Autonomous & Distributed Real-time Embedded Software Systems," in *31st International Conference on Field-Programmable Logic and Applications (FPL)*, Dresden, Germany, 2021, pp. 382–383.

[13] L. Masing, T. Dörr, F. Schade, J. Becker *et al.*, "XANDAR: Exploiting the X-by-Construction Paradigm in Model-based Development of Safety-critical Systems," in *Design, Automation and Test in Europe Conference (DATE)*, 2022. *(In press)*.

[14] F. Siddiqui, R. Khan, and S. Sezer, "Bird's-eye view on the Automotive Cybersecurity Landscape & Challenges in adopting AI/ML," in *4th IEEE International Symposium on Future Cyber Security Technologies*, Nov. 2021. *(In press)*.

[15] M. ter Beek, L. Cleophas, I. Schaefer, and B. Watson, "X-by-construction," in *8th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation, (ISoLA)*, Limassol, Cyprus, Jan. 2018, pp. 359–364.

[16] "Secure design principles: Guides for the design of cyber secure systems," National Cyber Security Centre (NCSC), Tech. Rep., May 2019. [Online]. Available: https://www.ncsc.gov.uk/collection/cyber-security-design-principles

[17] "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology (NIST), Tech. Rep., Apr. 2018. [Online]. Available: https://www.nist.gov/cyberframework/framework

[18] F. Siddiqui, M. Hagan, and S. Sezer, "Establishing Cyber Resilience in Embedded Systems for Securing Next-Generation Critical Infrastructure," in *32nd IEEE International System-on-Chip Conference (SOCC)*, Singapore, 2019, pp. 218–223.

[19] Martin Böhner, "Security for connected vehicles throughout the entire life cycle," Elecktrobit, Germany, Tech. Rep., 2015. [Online]. Available: https://www.elektrobit.com/tech-corner/security-for-connected-vehicles-throughout-the-entire-life-cycle/

[20] A. Chattopadhyay, K.-Y. Lam, and Y. Tavva, "Autonomous Vehicle: Security by Design," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 11, pp. 7015–7029, 2021.

[21] M. Scalas and G. Giacinto, "Automotive Cybersecurity: Foundations for Next-Generation Vehicles," in *2nd International Conference on new Trends in Computing Sciences (ICTCS)*, Amman, Jordan, 2019, pp. 1–6.