Journal of Electronic Research and Application, 2025, Volume 9, Issue 2
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

A Collaborative Protection Mechanism for System-on-Chip Functional Safety and Information Security in Autonomous Driving

Zhongyi Xu*, Lei Xin, Zhongbai Huang, Deguang Wei

Shandong Vocational and Technical University of International Studies, Rizhao 276800, Shandong, China

****Corresponding author:*** Zhongyi Xu, shuanqiangbr8@163.com

Abstract: This article takes the current autonomous driving technology as the research background and studies the collaborative protection mechanism between its system-on-chip (SoC) functional safety and information security. It includes an introduction to the functions and information security of autonomous driving SoCs, as well as the main design strategies for the collaborative prevention and control mechanism of SoC functional safety and information security in autonomous driving. The research shows that in the field of autonomous driving, there is a close connection between the functional safety of SoCs and their information security. In the design of the safety collaborative protection mechanism, the overall collaborative protection architecture, SoC functional safety protection mechanism, information security protection mechanism, the workflow of the collaborative protection mechanism, and its strategies are all key design elements. It is hoped that this analysis can provide some references for the collaborative protection of SoC functional safety and information security in the field of autonomous driving, so as to improve the safety of autonomous driving technology and meet its practical application requirements.

Keywords: Autonomous driving; SoC functional safety; Information security; Collaborative protection mechanism; Collaborative protection architecture

Online publication: April 3, 2025

1. Introduction

In the current field of autonomous driving, the functions of the system-on-chip (SoC) are a core component, and its security directly affects the safe use of autonomous driving technology. In addition, information security also directly impacts the safety of autonomous driving. Therefore, in the practical application research of modern autonomous driving technology, the collaborative protection mechanism between SoC functional safety and information security has become the focus of attention for researchers in this field. In specific research, researchers need to clarify the functional safety of autonomous driving SoCs and their information security and design a collaborative protection mechanism with reasonable strategies to achieve the collaborative guarantee of the security of both, providing strong support for the good application and development of autonomous driving technology.

2. Introduction to the functions and information security of autonomous driving SoCs

2.1. Functions of autonomous driving SoCs

System-on-chip is a core integration platform in the modern autonomous driving field and an integrated platform for various functions and capabilities in autonomous vehicles. In the current autonomous driving field, the main components and functions of SoCs include the following aspects. First is the computing and processing function, which involves functions such as sensor data processing, complex algorithm operations, multitasking processing, and scheduling in autonomous driving. Second is the communication and interface function, including sensor interfaces, vehicle bus communication, and external communication interfaces in autonomous driving. Third is the safety and reliability function, covering hardware safety mechanisms, fault detection and tolerance, security authentication, and encryption in autonomous driving. Fourth is the graphics processing and display function, including high-definition image rendering and 3D environment modeling display in autonomous driving. Fifth is the power management function, which includes power consumption control, power management, and power distribution in autonomous driving. In practical applications, secure SoC functions can strongly support the sensor data analysis and obstacle position judgment of autonomous vehicles, ensuring the timely issuance of braking, evasion, and other commands, and providing a good guarantee for the safety of autonomous driving.

2.2. Introduction to information security in autonomous driving

In the field of autonomous driving, information security means that all kinds of information and systems during the autonomous driving process of vehicles are not subject to security attacks, and there is no risk of data tampering, loss, or leakage. Only in this way can it guarantee the safe driving of autonomous vehicles and effectively prevent the leakage of important or private information of passengers. In the current autonomous driving field, the importance of information security is mainly reflected in the following aspects. First, the autonomous driving system highly depends on sensors, electronic control units, and software algorithms. If the information in these systems is lost, tampered with, or interfered with, the autonomous vehicle is likely to get out of control, and in severe cases, even lead to safety accidents [1]. Second, autonomous vehicles often collect a large amount of user data during operation, including driving habits and location information. If the security of this information cannot be effectively guaranteed, important or private user information is likely to be leaked, causing unnecessary disturbances to their normal work and life and even economic losses. Third, in the practical application of autonomous driving technology, if information security problems occur frequently, users' trust in this technology will gradually decrease, which will pose many obstacles to the subsequent application and development of this technology and the automation transformation and development of the automotive driving field.

2.3. Correlation between SoC functional safety and information security in autonomous driving

In the current autonomous driving field, SoC functional safety and information security are not independent of each other but are interdependent and mutually influential. There is a close correlation between them, and both play a crucial role in the operation of the autonomous driving system. First, there is some redundant design in the SoC functions of autonomous driving, that is, some spare parts identical or similar to the operating hardware are equipped. When a component fails, the spare component can promptly detect the fault and replace it to continue normal operation. In this case, if a piece of hardware is hacked and the data or permissions in it are tampered with, the redundant component can promptly discover the fault and replace it to continue normal operation [2,3]. This not only ensures the security of autonomous driving information but also reduces the probability of unnecessary safety accidents. Second, the information security protection technology in autonomous driving can effectively prevent various data from being attacked during storage or transmission, thus ensuring the integrity and security of data. In this mode, the realization of SoC functions in autonomous driving will be more secure, providing a good guarantee for the safe and stable operation of autonomous vehicles. It can be seen that in the field of autonomous driving, the connection between SoC functional safety and information security is very close. Only by ensuring the security of both SoC functions and information can the safety of autonomous vehicle driving be ensured. Based on this, the collaborative protection mechanism for SoC functional safety and information security has become a key focus and research area in the field of autonomous driving in recent years [4].

3. Main design strategies for the collaborative protection mechanism of SoC functional safety and information security in autonomous driving

3.1. Design of the overall collaborative protection architecture

In the collaborative protection mechanism for SoC functional safety and information security in autonomous driving, the rational design of the overall collaborative protection architecture is of great significance. According to the collaborative protection requirements for SoC safety and information security in the autonomous driving field, this architecture mainly includes the following components.

The first is the SoC functional safety protection module. This module is the key defense line to ensure the healthy and normal operation of SoC functions and the safe and stable operation of SoC hardware. The most critical safety protection links include fault detection, tolerance, and safe state switching. Through the collaborative operation of these links, the probability of SoC hardware failures can be effectively reduced, avoiding autonomous driving risks caused by SoC failures and making the operation state of autonomous vehicles safer and more reliable [5-7].

The second is the information security protection module. This module is the key defense line to prevent autonomous driving systems from being attacked by the network and ensure data security. The most critical security protection technologies include data encryption technology, identity authentication technology, access control technology, and intrusion detection technology. Through the coordinated cooperation of these technologies, various information security risks can be effectively prevented, guaranteeing the data security of the autonomous driving system, preventing the adverse effects of data security risks on system operation, and maintaining the safe and stable operation state of the overall system.

The third is the collaborative protection mechanism implementation module. This module is the key link to ensure the collaborative protection of SoC functions and information security in autonomous driving [8]. It can establish a close connection between SoC function and information security protection, enabling all links to maintain coordinated cooperation and orderly operation. The three most critical collaborative operation processes are safety monitoring, collaborative decision-making, and response execution. Through the effective control and realization of these three processes, the orderly operation of the overall collaborative protection mechanism can be ensured, meeting the collaborative protection requirements for SoC functional safety and information security in autonomous driving.

3.2. Design of the SoC functional safety protection mechanism

As an important protection module to ensure the functional safety of autonomous driving SoCs, this protection mechanism mainly consists of three functions: fault detection, tolerance, and safe state switching.

In this safety protection mechanism, fault detection is the primary link. Its core operation goal is to detect various potential hardware abnormalities or software errors in the SoC system during operation in a timely and accurate manner. There are many detection methods for hardware abnormalities. First is the real-time monitoring technology of hardware circuits, that is, using sensors to monitor the current, voltage, temperature, etc. of hardware circuits in real time. If the values exceed the specified range, the system will immediately issue an alarm and activate the corresponding protection mechanism [9,10]. Second is the hardware redundancy-based fault detection and hardware switching. On the basis of the operation of the main hardware, pre-installed identical or similar hardware is added as a backup. Once the main hardware fails or malfunctions, the backup hardware will immediately replace the main hardware to continue maintaining the safe and stable operation of the overall system, providing support for subsequent fault detection, operation, and maintenance of the main hardware. There are also many detection methods for software errors. For example, through static analysis methods, the logic, semantics, and syntax of software code can be analyzed to check for potential problems, including memory leaks, null pointer references, etc. Through dynamic testing methods, the software operation scenarios can be simulated, and the software performance and function can be comprehensively tested in the simulated scenarios to verify whether they meet the design requirements. Through unit testing, integration testing, and system testing methods, the functions and operation effects of the software under various conditions can be comprehensively verified to discover software errors in a timely manner [11]. To ensure the system operation effect under software error conditions, the system also has a software redundancy design, that is, the backup system replaces the main system to run, reserving sufficient time for the repair of software errors in the main system.

The fault-tolerance protection mechanism is a key component of this module. Its main goal is to implement fault-tolerance processing on the detected faults through effective means to keep the key functions of the system operating normally. In addition to hardware and software redundancy designs, the system also needs to introduce error-correcting code technology supported by automation and intelligence. That is, the system data is verified through CRC (Cyclic Redundancy Check). If data errors are found, the error-correcting code can automatically correct the wrong data to ensure the accuracy of system operation parameters and prevent operation errors [12].

Safe state switching is the last line of defense for SoC functional safety. Its main goal is to automatically switch the SoC function to a safe state when a fault or abnormality occurs, ensuring the safe and stable operation of the overall system. In the specific design, this function needs to be realized with the help of intelligent fault assessment and automated control logic. Methods such as fault tree analysis are used to assess the SoC function faults or abnormalities, and the assessment results are fed back to the control logic. The control logic then executes the corresponding safe state switching operations according to the assessment results. In this way, the rapid isolation of SoC system hardware and software faults can be achieved, and the operation state of the overall system can always be kept safe and stable.

3.3. Design of the information security protection mechanism

As the key defense mechanism for the information security of the SoC system, this module's main supporting technologies include data authentication and encryption technology, identity authentication technology, access control technology, and intrusion detection technology.

Data encryption technology is the basic technology for information security protection. Its main goal is to encrypt the data stored or transmitted in the system, converting readable plaintext into unreadable ciphertext. Only authorized users can decrypt and read the data. With the support of SSL (Secure Socket Layer) and TLS (Transport Layer Security), the data transmitted between autonomous vehicles and cloud servers, other vehicles, and infrastructure is encrypted. When data starts to be transmitted, SSL/TLS will encrypt it to prevent attacks during data transmission. With the support of AES (Advanced Encryption Standard), various data encryption algorithms can be adopted according to the actual situation to encrypt all sensitive or important data stored in the system, including passengers' location information and personal information, to prevent illegal use [13,14].

Identity authentication technology is a key means to judge the legitimacy of system access. With the help of this technology, information such as usernames, passwords, faces, or fingerprints can be identified. Only users who pass the identification are allowed to access the system, and those who fail cannot.

Permission control technology is a security protection technology superimposed on the basis of identity authentication technology. Its basic goal is to identify the access permissions of users to the system according to their identity information. For example, ordinary users can only view data within their permission range, while administrative users can manage system configurations, update software, or set security policies. Users cannot operate functions outside their permission range to prevent malicious access and tampering with system resources.

Intrusion detection technology is an important technology for the system to resist external attacks. Its basic goal is to monitor the system operation state and network traffic in real time to detect potential network attack behaviors in a timely manner and issue alarms. In the specific design, this function should be realized with the support of machine learning technology and big data technology. The machine learning model is trained with massive data to enable it to accurately identify and block various network attack behaviors in a timely manner, ensuring system security.

3.4. Design of the workflow and strategies of the collaborative protection mechanism

In the operation of the collaborative protection mechanism, its basic workflow includes three steps: safety monitoring, collaborative decision-making, and response execution. Safety monitoring is the first step in discovering SoC function or information security problems [15]. After detecting various security problems through the above-mentioned safety protection technical measures, this module will continue to use the intelligent algorithm model to accurately predict the types of security threats, their severity, and their impact scope. According to the security prediction results, the intelligent algorithm model will, with the support of big data technology, quickly and effectively decide on subsequent security protection and governance measures and send the corresponding security control instructions to the response execution module. After receiving the system instructions, the response execution module will immediately isolate the faulty hardware or software according to the instructions or immediately block the corresponding network security attack behaviors. In this way, effective collaborative protection of SoC functions and information security in autonomous driving can be achieved, maximizing the security of the autonomous driving SoC system and avoiding various unnecessary security problems or accidents.

4. Conclusion

In summary, in the practical application of autonomous driving technology, the collaborative protection of SoC functional safety and information security is of great importance. Based on this, researchers need to establish a scientific, reasonable, and complete collaborative protection mechanism according to their internal connections and security protection requirements to ensure the safe and stable operation of the overall system and provide a good guarantee for the safety of autonomous vehicles.

Disclosure statement

The authors declare no conflict of interest.

References

[1] Chen M, Yang Z, Qiu J, et al., 2025, Analysis of the Information Security Platform for the Commercialization of Autonomous Driving. Network Security Technology & Application, 2025(01): 111–113.

[2] Duan W, Wang G, 2024, Analysis of Traffic Safety Management for Autonomous Driving from the Perspective of Security. Auto & Safety, 2024(08): 83–93.

[3] Wang M, Tu H, Xue D, et al., 2024, Optimization of Autonomous Driving Adaptive Cruise Control Based on Safety Risk Prediction. Journal of Tongji University (Natural Science), 2024(04): 512–519.

[4] Zhang X, Chen H, Yang S, et al., 2024, Research on Cybersecurity Policies and Standardization for Autonomous Driving. China Information Security, 2024(02): 26–29.

[5] Wang Y, 2022, Development of On-Board Controllers for Autonomous Vehicles, dissertation, Tianjin University of Technology and Education.

[6] Mao X, Shang S, Cui H, 2018, Research on the Analysis and Countermeasures of Safety-Related Factors for Autonomous Vehicles. Shanghai Auto, 2018(1): 5.

[7] Wang K, Dong Z, Yang F, et al., 2023, Key Technologies and Applications of Vehicle-to-Everything Cooperative Autonomous Driving Based on C-V2X. Telecommunications Science, 39(3): 16.

[8] Xu X, 2024, Research on the Functional Safety Strategy for Multisource Vehicle Body Information in Autonomous Driving. Journal of Information Security Research, 10(11): 1020–1026.

[9] Feng J, 2023, Research and Application of 3D Object Detection Algorithms for Autonomous Driving Scenarios, dissertation, Taiyuan University of Technology.

[10] Han J, 2006, Research on the Attack-Defense Technology of Information Security Chips, dissertation, Fudan University.

[11] Zhang A, Qiao G, 2006, Development of High-Performance Information Security SoC Chips. China Integrated Circuit, 2006(01): 29–31.

[12] Zhang L, Chang C, Dong J, 2012, External Program Secure Access Architecture Based on SoC Chips, CN202102449U.

[13] Wen S, 2009, Design and Implementation of a Dedicated Security Chip Based on SoC, dissertation, The PLA Information Engineering University.

[14] Fang J, Wu P, Ai Y, 2023, Implementation of the Off-line Loading System for Secure SoC Chips. Journal of Engineering Technology (Citation Edition), 2023(4): 4.

[15] Yang T, 2022, Research on the Functional Safety of Vehicle Brake-by-Wire Systems for Autonomous Driving, dissertation, Jilin University.

Publisher's note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.