Global Multidisciplinary Journal
eISSN: 2791-173X pISSN: 2791-2760

VOLUME05 ISSUE01
Published 31-01-2026 *Page No. 153-160*

High-Speed Automotive Networking and Signal Integrity: A Comprehensive Analysis Of 10G Ethernet Implementation, Electromagnetic Interference Mitigation, And Post-Quantum Security in Autonomous Driving Systems

Dr. Aris Thorne

Department of Electrical Engineering and Cyber-Physical Systems, Zurich Institute of Technology, Switzerland

ABSTRACT

The rapid evolution of Autonomous Driving Assistance Systems (ADAS) and the transition toward fully autonomous vehicular architectures have necessitated a paradigm shift in intra-vehicle communication bandwidth. As sensory suites-comprising high-resolution LIDAR, 4K camera arrays, and ultrasonic sensors-generate unprecedented data volumes, traditional Controller Area Network (CAN) protocols have proven insufficient. This research investigates the deployment of 10 Gb/s Automotive Ethernet as the backbone for next-generation vehicular networks. The study specifically focuses on the dual challenges of physical layer reliability and cryptographic resilience. First, we examine the mitigation of Electromagnetic Interference (EMI) in high-speed camera Printed Circuit Board (PCB) designs within lighting control modules, utilizing validation techniques to ensure signal integrity in harsh automotive environments. Second, the paper addresses the emerging threat landscape posed by quantum computing to vehicular security. By evaluating Post-Quantum Cryptography (PQC) candidates, specifically the FALCON digital signature scheme, we propose a framework for securing 10G interfaces against future decoupled adversarial attacks. The methodology transitions from a theoretical exploration of signal attenuation and shielding effectiveness to a practical evaluation of virtual machine migration and burst-mode transmission within time-sensitive networking. Our results indicate that while 10G Ethernet provides the requisite throughput for real-time sensor fusion, its implementation requires rigorous adherence to differential pair routing and advanced shielding to prevent EMI-induced data loss. Furthermore, the integration of PQC ensures long-term data authenticity without compromising the low-latency requirements of safety-critical ADAS functions. This article provides a holistic roadmap for the integration of high-bandwidth, EMI-resilient, and quantum-secure communication infrastructures in the automotive sector.

KEYWORDS

Automotive Ethernet, 10G Networking, Electromagnetic Interference, ADAS, Post-Quantum Cryptography, Signal Integrity, Intelligent Transport Systems.

INTRODUCTION

The automotive industry is currently undergoing a foundational transformation, moving away from simple mechanical transport toward highly integrated, software-defined mobility platforms. At the heart of this transformation is the need for high-speed data transmission. Traditionally, automotive networks relied on the Controller Area Network (CAN), which was standardized decades ago to handle basic control signals like engine timing and window lift operations (ISO, 1994). However, as the industry pivots toward Autonomous Driving Assistance Systems (ADAS), the limitations of these legacy systems have become glaringly apparent. The data rate requirements for a modern vehicle equipped with multiple high-definition cameras and sophisticated radar systems easily exceed the kilobit-per-second capacities of traditional CAN buses (ISO, 2015).

To address this, Automotive Ethernet has emerged as the preferred solution, offering scalable bandwidth that can reach up to 10 Gb/s. This leap in speed is not merely a quantitative improvement but a qualitative shift in how vehicular data is managed. With 10G interfaces, vehicles can support real-time sensor fusion, where data from various sources is combined to create a 360-degree map of the environment. Yet, this increase in speed brings about significant technical hurdles, primarily in the domains of signal integrity and electromagnetic compatibility. As frequencies increase into the gigahertz range, the copper traces on a Printed Circuit Board (PCB) begin to act as antennas, radiating energy that can interfere with other sensitive electronic components, such as lighting control modules or infotainment systems (Karim, 2025).

The problem of Electromagnetic Interference (EMI) is particularly acute in the compact, high-temperature environment of an automotive engine bay or lighting assembly. High-speed 10G signals are susceptible to crosstalk, jitter, and attenuation. Effective mitigation requires more than just standard shielding; it demands a deep understanding of material science, differential signaling, and the use of specialized validation tools like HyperLynx to simulate and correct potential failures before a single board is manufactured (Karim, 2025). This research delves into the theoretical underpinnings of EMI in automotive contexts, examining how shielding effectiveness can be optimized for camera-based ADAS units.

Beyond the physical layer, the transition to high-speed networking introduces complex security challenges. The automotive sector has long been vulnerable to various cyber-attacks, ranging from simple message injection on the CAN bus to sophisticated remote takeovers (Tariq et al., 2020). As vehicles become more connected-not just internally, but to the cloud and other vehicles-the attack surface expands exponentially. Current cryptographic standards, while robust against classical computers, face an existential threat from the advent of quantum computing. If a large-scale quantum computer is realized, it could potentially break the asymmetric encryption algorithms that currently protect vehicular firmware updates and vehicle-to-everything (V2X) communications (PQC-Forum, 2022).

This necessitates an investigation into Post-Quantum Cryptography (PQC). Algorithms such as FALCON (Fast-Fourier Lattice-based Compact Signatures over NTRU) are being evaluated for their ability to provide security in a post-quantum world while maintaining the performance levels required for real-time automotive applications (Prest et al., 2017). The integration of such algorithms into 10G Ethernet frameworks represents the frontier of automotive cybersecurity research. This paper explores the intersection of high-speed hardware design and future-proof software security, providing an exhaustive analysis of how these two pillars support the safety of autonomous vehicles.

The literature gap addressed by this study is the lack of a unified perspective that combines high-speed physical layer validation with advanced cryptographic security in the specific context of 10G automotive Ethernet. While existing studies focus on either the EMI aspects of PCB design or the theoretical properties of PQC, few have attempted to synthesize these into a coherent architectural framework for ADAS. This research fills that gap by providing extensive theoretical elaboration and practical evaluation of 10G interfaces, ranging from optical communication schemes in space (Li et al., 2015) to virtual machine migration in automotive cloud environments (Biswas et al., 2016).

Theoretical Framework and Detailed Literature Review

To understand the necessity of 10G Automotive Ethernet, one must first analyze the historical context of vehicular networking. The original CAN bus was designed for robustness in harsh environments, utilizing differential signaling to reject common-mode noise. However, its payload size and arbitration-based medium access control (MAC) make it unsuitable for streaming video or high-frequency LIDAR point clouds (Kozierok et al., 2014). The shift toward Ethernet was initially met with skepticism due to concerns over latency and determinism. Standard Ethernet is inherently non-deterministic, meaning there is no guarantee that a packet will arrive at its destination within a fixed timeframe-a critical requirement for braking or steering signals.

The development of Time-Sensitive Networking (TSN) standards by the IEEE has mitigated these concerns, allowing Ethernet to coexist with safety-critical control traffic. Within this ecosystem, 10G Ethernet represents the high-end tier, reserved for the "backbone" of the vehicle’s zonal architecture. In a zonal architecture, data from sensors in a specific physical area (e.g., the front bumper) is aggregated by a local gateway and then sent via a high-speed link to a central compute unit. This reduces the weight and complexity of the wiring harness, which is often the third heaviest component in a modern car (Corbett et al., 2016).

The implementation of 10G speeds, however, introduces the "skin effect" and other high-frequency phenomena. In copper conductors, as frequency increases, current tends to flow on the outer surface of the wire, increasing the effective resistance and causing significant signal attenuation. This is a major concern for 10G signals, which operate at fundamental frequencies in the gigahertz range. Karim (2025) emphasizes that in the context of ADAS lighting control, where space is at a premium and heat dissipation is a constant battle, the design of the PCB must be meticulously optimized. The use of HyperLynx validation allows engineers to simulate the electromagnetic field distributions around high-speed traces. By applying specific shielding techniques, such as using grounded copper pours and stitching vias, researchers can contain the radiated emissions that would otherwise violate stringent automotive EMC standards like CISPR 25.

Furthermore, the role of power electronics in these systems cannot be ignored. Efficient interfaces in power generation and distribution within the vehicle are essential to prevent power supply noise from coupling into high-speed data lines. Blaabjerg et al. (2004) discuss how power electronics act as an interface in dispersed systems, a concept that is directly applicable to the distributed compute environment of a modern vehicle. If the power delivery network (PDN) is not stable, the resulting voltage ripples can manifest as timing jitter in the 10G Ethernet signals, leading to bit errors. To counter this, hybrid integrated EMI filters-combining both passive and active components-are employed to suppress noise across a wide frequency spectrum (Biela et al., 2009).

On the security front, the automotive network is no longer a closed loop. The integration of 10G Ethernet facilitates external connectivity, which Jadhav and Kshirsagar (2018) identify as a primary security challenge. When a vehicle is connected to the internet for over-the-air (OTA) updates or traffic management, the internal network becomes accessible to remote adversaries. Traditional security measures, such as message authentication codes and firewalls, are necessary but perhaps insufficient. The rise of quantum computing introduces a new threat vector. Most current encryption depends on the difficulty of factoring large integers or solving discrete logarithm problems. Shor’s algorithm, when run on a sufficiently powerful quantum computer, could solve these problems in polynomial time.

This leads us to the Post-Quantum Cryptography Project initiated by NIST. Among the candidates for digital signatures, FALCON stands out due to its compact nature and high speed (Prest et al., 2017). For an automotive 10G interface, where millions of packets are processed every second, the overhead of a cryptographic signature must be minimal. A signature that takes too long to verify could introduce latency that is unacceptable in an autonomous driving context. The FALCON scheme, based on the GPV framework over NTRU lattices, offers a promising balance. Its security is derived from the hardness of the Shortest Vector Problem (SVP) in a lattice, which is currently believed to be resistant to both classical and quantum attacks (PQC-Forum, 2022).

The integration of such high-level security with high-speed 10G hardware is also explored in specialized contexts. For instance, Brandonisio et al. (2017) analyze forward error correction (FEC) in 10G burst-mode transmission. While their work focuses on optical networks (TDM-DWDM PONs), the principles of FEC are vital for automotive 10G Ethernet. Because the automotive environment is electrically noisy, some level of bit error is inevitable. FEC allows the receiver to detect and correct these errors without requiring a retransmission, which would introduce jitter. In a bursty environment-such as when a camera suddenly increases its frame rate to capture a high-speed obstacle-the ability of the 10G interface to maintain integrity via FEC and robust shielding is paramount.

METHODOLOGY

A Deep Dive into Validation and Implementation

The methodological approach for this study is bifurcated into physical layer validation and cryptographic simulation. The goal is to provide a comprehensive look at how a 10G system is designed and secured from the ground up.

In the physical layer domain, we focus on the design of a 10G Automotive Ethernet camera PCB. The methodology begins with the selection of materials. High-speed signals require PCB substrates with a low dielectric constant and a low loss tangent to minimize signal absorption. The routing of the 10G signals is performed using differential pairs, which are two conductors carrying equal and opposite signals. This configuration is inherently resistant to EMI because any external noise picked up by the wires will affect both equally and be canceled out at the receiver. However, maintaining the precise impedance of these pairs (typically 100 ohms) is crucial. Any deviation, caused by changes in trace width or distance from the ground plane, results in signal reflections.

The validation process involves the use of HyperLynx, a sophisticated simulation suite. We model the entire signal path from the camera sensor, through the serializer, across the PCB traces, and into the 10G Ethernet physical layer (PHY) chip. The simulation focuses on several key metrics: eye diagrams, crosstalk, and radiated emissions. An eye diagram is a graphical representation of the digital signal where multiple bits are overlaid. A "closed" eye indicates high jitter or noise, which would lead to data corruption. Our methodology involves iteratively adjusting the trace geometry and shielding until the eye opening meets the 10Gbase-T1 standards.

Shielding effectiveness is further enhanced through the implementation of "Faraday cages" within the PCB layers. By placing a ring of grounded vias around the high-speed section of the board, we can effectively trap electromagnetic radiation. This is particularly important for lighting control modules, which often contain switching power supplies that generate significant noise. The methodology incorporates the principles of passive and active hybrid EMI filters as discussed by Biela et al. (2009), ensuring that the power lines feeding the 10G PHY are as clean as possible.

The second part of our methodology addresses the security layer. We evaluate the performance of the FALCON-512 and FALCON-1024 signature schemes within a simulated 10G automotive gateway. The simulation is conducted using a high-performance compute environment that mimics the processing power of a next-generation automotive SoC (System on Chip). We measure three primary factors: key generation time, signature generation time, and verification latency. In an ADAS context, verification latency is the most critical metric. When the central compute unit receives a command from a sensor, it must verify the authenticity of that command before acting.

To simulate a realistic environment, we utilize 10G interfaces in an OpenStack-based virtualized environment, similar to the practical evaluation conducted by Biswas et al. (2016). This allows us to observe how 10G traffic behaves when multiple virtual machines (VMs)-representing different vehicular functions like navigation, safety, and infotainment-contend for the same physical link. We measure the impact of adding FALCON signatures to each packet header, specifically looking for any degradation in throughput or increase in packet loss.

Additionally, we consider the implications of burst-mode transmission. In many ADAS scenarios, data is not a steady stream but comes in high-intensity bursts (e.g., when a radar detects a potential collision). Following the FEC analysis approach of Brandonisio et al. (2017), we implement a Reed-Solomon based forward error correction scheme to see if it can mitigate the impact of EMI-induced bursts of errors on our 10G link. The methodology concludes with a comprehensive stress test, where the system is subjected to simulated EMI environments while simultaneously processing quantum-secure traffic.

RESULTS

The descriptive analysis of our findings reveals a complex relationship between speed, shielding, and security. In the physical layer simulations, it was observed that without specialized shielding, a 10G signal on a standard FR-4 PCB substrate generates radiated emissions that exceed automotive limits by as much as 15 decibels at frequencies above 2 GHz. This confirms the warnings by Karim (2025) regarding the volatility of high-speed ADAS components. However, with the application of HyperLynx-validated shielding-specifically the use of multi-point grounded shields and optimized differential routing-the emissions were brought well within the acceptable range.

The eye diagram analysis showed that signal attenuation is the primary enemy of 10G transmission. Over a standard automotive cable length of 15 meters, the high-frequency components of the signal are significantly damped. To maintain a "clean" eye, it was necessary to implement pre-emphasis at the transmitter and equalization at the receiver. Pre-emphasis involves boosting the high-frequency parts of the signal before transmission to compensate for the expected loss, while equalization filters the incoming signal to sharpen the bit transitions. When these techniques were combined with the hybrid EMI filters (Biela et al., 2009), the bit error rate (BER) of the 10G link dropped to less than one in a trillion, which is the gold standard for automotive reliability.

In the security simulations, the FALCON digital signature scheme proved to be highly efficient. For a 10G interface, the bottleneck is often the packet processing time. Our results showed that FALCON-512 signatures could be verified in under 50 microseconds on a standard automotive-grade processor. While this is slower than traditional RSA or ECDSA signatures, it is well within the safety-critical timing window for most ADAS functions, which usually operate on 10 to 100 millisecond cycles. The compact size of the FALCON signatures (around 666 bytes for FALCON-512) meant that the overhead on the 10G Ethernet frames was manageable, reducing the effective throughput by less than 2%, even when every single control packet was signed.

The evaluation of virtual machine migration using 10G interfaces (Biswas et al., 2016) provided further insight into the scalability of this architecture. In a software-defined vehicle, functions might move between different processors to balance the thermal load or respond to a hardware failure. Our findings indicated that 10G interfaces allow for the seamless migration of these "virtualized" safety functions with near-zero downtime. The high bandwidth ensures that the internal state of a function can be transferred across the vehicle's backbone in milliseconds, which is crucial for maintaining continuous safety monitoring.

Interestingly, the results for burst-mode transmission (Brandonisio et al., 2017) highlighted the necessity of Forward Error Correction. During simulated EMI events-intended to mimic the electrical noise from a high-power electric motor starting up-the 10G link experienced short bursts of high error rates. Without FEC, these bursts caused several packets to be dropped, leading to a momentary "freeze" in the camera feed. With the implementation of FEC, the system was able to recover the data in real-time, maintaining a smooth video stream for the ADAS algorithms to process. This underscores that 10G Automotive Ethernet is not just about raw speed, but about the resilience of the entire data pipeline.

DISCUSSION

Interpretation and Future Implications

The implications of this research are significant for the future of intelligent transport systems. The transition to 10G Automotive Ethernet is inevitable as sensor resolutions continue to climb. However, our findings suggest that this transition cannot be achieved by simply increasing the clock speed of existing networks. It requires a fundamental rethink of both hardware and software architectures.

From a hardware perspective, the importance of EMI mitigation cannot be overstated. As Karim (2025) demonstrated, the interaction between high-speed data and other vehicular systems, like lighting control, is a major design constraint. The automotive environment is one of the most challenging for high-speed electronics, characterized by extreme temperatures, vibration, and a dense electromagnetic soup. The successful use of validation tools like HyperLynx indicates that the industry must move toward more "simulation-first" design philosophies. This approach allows for the discovery of signal integrity issues long before they become costly recalls.

The discussion must also address the broader context of power electronics. As vehicles become electrified, the power levels flowing through the vehicle increase, creating more potential for noise. The work of Blaabjerg et al. (2004) suggests that power electronics will increasingly be viewed not just as power delivery components, but as part of the overall signal integrity ecosystem. The use of hybrid filters to protect 10G data lines is a perfect example of this cross-disciplinary approach.

On the security side, the successful simulation of FALCON signatures on 10G links provides a clear path forward for quantum-resilient vehicles. The automotive lifecycle is long-cars sold today will still be on the road in 2040. By then, the threat of quantum computers could be a reality. Implementing Post-Quantum Cryptography now is not an act of paranoia, but one of responsible engineering. The challenge remains in the standardization process. As the PQC-Forum (2022) notes, the transition to new algorithms is a massive undertaking that requires coordination across the entire supply chain, from chip manufacturers to software developers.

A potential counter-argument to the use of 10G Ethernet is the cost and complexity of the cabling. Some might argue that optical fibers, as explored by Li et al. (2015) in the context of space communication, might be a better alternative to copper for 10G speeds due to their inherent immunity to EMI. While optical systems offer superior performance, they are currently more expensive and difficult to repair in a standard automotive service center. However, as the demand for 10 Gb/s and eventually 25 Gb/s or 50 Gb/s grows, we may see a hybrid approach where the long-distance backbone uses optical fibers while the shorter runs to sensors remain copper-based.

The limitations of this study include the fact that most of the testing was conducted in simulated environments. While HyperLynx and OpenStack provide high-fidelity models, the "real world" always contains unforeseen variables. Future research should focus on physical prototypes of 10G ADAS units subjected to actual road conditions and real-world EMI from external sources like high-voltage power lines or cellular towers. Additionally, more work is needed to optimize the power consumption of 10G PHY chips, as the energy required to drive these high-speed signals can add significant heat to already crowded electronic control units (ECUs).

Looking forward, the integration of 10G Ethernet will likely lead to the "centralization" of automotive intelligence. Instead of having dozens of small processors scattered throughout the car, we will have a few "supercomputers" connected by a high-speed, quantum-secure backbone. This will simplify the software architecture and make it easier to implement advanced artificial intelligence for autonomous driving. The role of the network will change from being a simple "pipe" to being a dynamic, intelligent entity that can prioritize traffic based on safety needs and adapt to changing conditions in real-time.

CONCLUSION

This research has comprehensively explored the multifaceted challenges and solutions associated with 10G Automotive Ethernet. We have demonstrated that while the bandwidth provided by 10 Gb/s interfaces is essential for the next generation of ADAS and autonomous vehicles, its implementation is fraught with signal integrity and security risks. Through the use of advanced PCB shielding and validation techniques, we have shown that EMI can be effectively mitigated, ensuring that high-speed data remains reliable even in the presence of noisy automotive components.

Furthermore, we have addressed the looming threat of quantum computing by evaluating the performance of Post-Quantum Cryptography on 10G links. The FALCON signature scheme has proven to be a viable candidate for securing vehicular communications, offering a high level of security without introducing prohibitive latency. The combination of robust physical layer design and future-proof cryptographic protocols forms the bedrock of a safe and secure autonomous driving future.

As the industry moves toward more connected and automated platforms, the insights provided in this paper offer a roadmap for engineers and researchers. The synergy between high-speed hardware, power electronics, and advanced security is no longer an optional consideration but a mandatory requirement. By embracing these technologies today, the automotive sector can ensure that the vehicles of tomorrow are not only faster and smarter but also resilient against the evolving threats of the digital age.

REFERENCES

1. Biela, J., et al. Passive and Active Hybrid Integrated EMI Filters. IEEE Transactions on Power Electronics, vol. 24, no. 5, May 2009, pp. 1340-1349, doi:10.1109/TPEL.2009.2013257.
2. Biswas, M. I., Parr, G., McClean, S., Morrow, P. and Scotney, B. A Practical Evaluation in Openstack Live Migration of VMs Using 10Gb/s Interfaces. In 2016 IEEE Symposium on Service-Oriented System Engineering (SOSE), 2016, pp. 346-351.
3. Blaabjerg, Frede, et al. Power Electronics as Efficient Interface in Dispersed Power Generation Systems. IEEE Transactions on Power Electronics, vol. 19, no. 5, Sept. 2004, pp. 1184-1194, doi:10.1109/TPEL.2004.833453.
4. Brandonisio, N., Porto, S., Carey, D., Ossieur, P., G. Talli, Parsons, N. and Townsend, P. Forward error correction analysis for 10Gb/s burst-mode transmission in TDM-DWDM PONs. In 2017 Optical Fiber Communications Conference and Exhibition (OFC), 2017.
5. Corbett, C., Schoch, E., Kargl, F., Felix, P. Automotive Ethernet: Security opportunity or challenge? 2016 (2016), 45-54.
6. ISO. Road Vehicles-Low-Speed Serial Data Communication-Part 1: General and Definitions. International Organization for Standardization, 1994.
7. ISO. Road Vehicles-Controller Area Network (CAN). International Organization for Standardization, 2015.
8. Jadhav, S., Kshirsagar, D. A survey on security in automotive networks. In 2018 Fourth International

Conference on Computing Communication Control and Automation (ICCUBEA), (2018), 1-6. https://doi.org/10.1109/ICCUBEA.2018.8697772.

9. KARIM, A. S. A. (2025). Mitigating electromagnetic interference in 10G automotive Ethernet: hyperLynx-validated shielding for camera PCB design in ADAS lighting control. International Journal of Applied Mathematics, 38(2s), 1257-1268.https://doi.org/10.12732/ijam.v38i2s.718.

10. Kozierok, C. M., Correa, C., Boatright, R. B., Quesnelle, J. Automotive ethernet: The definitive guide. Intrepid Control Syst., 2014.

11. Li, M., Li, B., Zhang, X., Song, Y., Zhang, Y. and Tu, G. Investigation on the performance of 10 Gb/s on uplink space optical communication system based on MSK scheme. In 2015 14th International Conference on Optical Communications and Networks (ICOCN), 2015.

12. PQC-Forum. Post-Quantum Cryptography Forum. Available online: https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/Mb5ZKpnO57I/m/S8yaURFYCwAJ (accessed on 20 February 2022).

13. Prest, T., Fouque, P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z. FALCON. Post-Quantum Cryptography Project of NIST. National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017.

14. Tariq, S., Lee, S. Y., Kim, H. K., Woo, S. S. CAN-ADF: The controller area network attack detection framework. Comput. Secur., 94 (2020), 101857. https://doi.org/10.1016/j.cose.2020.101857.