COLOMBO SCIENTIFIC PUBLISHING

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM
E-ISSN: 2536-7919
P-ISSN: 2536-7900
PAGE NO: 01-06

A Secure and Deterministic Time-Sensitive Networking Architecture for Automotive and Industrial Cyber-Physical Systems: An Integrated Study of Synchronization, Resilience, And Cybersecurity

Dr. Andi Prakoso
Department of Computer Science and Artificial Intelligence, Jakarta Institute of Digital Technology, Jakarta, Indonesia

ARTICLE INFO

Article history:
Submission: May 08, 2026
Accepted: June 06, 2026
Published: July 01, 2026
VOLUME: Vol.11 Issue 07 2026

Keywords:
Time-Sensitive Networking, Automotive Systems, Cyber-Physical Systems, Synchronization, Cybersecurity, Fault Tolerance, Deterministic Communication, IEEE 802.1AS, Real-Time Systems, Industrial Automation

ABSTRACT

Time-Sensitive Networking (TSN) has emerged as a foundational paradigm for enabling deterministic communication in automotive and industrial cyber-physical systems (CPS), where strict timing guarantees, high reliability, and cybersecurity resilience are simultaneously required. However, the integration of synchronization precision, fault tolerance, and security mechanisms into a unified architectural framework remains an open research challenge. Existing industrial and automotive network designs often treat these concerns independently, leading to inefficiencies, timing uncertainties, and increased vulnerability to cyber-attacks.

This research proposes a conceptual and analytical synthesis of secure and deterministic TSN architectures tailored for automotive and industrial CPS environments. The study investigates synchronization mechanisms based on IEEE 802.1AS and IEEE 1588, evaluates fault-tolerant communication strategies, and examines cybersecurity threats targeting time-sensitive protocols. A structured architectural model is derived through comparative synthesis of existing automotive network frameworks and TSN implementations. The analysis further integrates predictability theory to assess real-time guarantees in distributed systems.

Findings indicate that achieving deterministic performance under adversarial conditions requires co-design of synchronization, traffic shaping, and intrusion detection mechanisms. Moreover, automotive-grade architectures demonstrate that centralized platform-based designs improve scalability but introduce new security bottlenecks. The study concludes that a unified TSN framework with built-in security and resilience layers is essential for next-generation automotive and industrial CPS.

1. INTRODUCTION

1.1 Background

Modern automotive and industrial systems are rapidly evolving into complex cyber-physical ecosystems characterized by distributed intelligence, high-speed communication, and strict timing constraints. Traditional in-vehicle networking protocols such as CAN and Ethernet variants are increasingly insufficient to meet emerging requirements for determinism, scalability, and security. Time-Sensitive Networking (TSN), an extension of Ethernet standards, has been proposed as a unifying communication backbone capable of addressing these limitations through bounded latency and synchronized transmission.

The evolution of automotive architectures has also shifted toward centralized and zonal computing models, as highlighted in industrial implementations such as the automotive architecture framework of Volvo Cars, which demonstrates the transition toward platform-based system design (Pelliccione et al., 2017). This architectural shift enables consolidation of computation and communication resources but introduces new challenges in synchronization consistency and cybersecurity exposure across shared networks (Pelliccione et al., 2017).

1.2 Problem Statement

Despite advancements in TSN standards and automotive network design, three fundamental challenges remain unresolved:

1. Lack of unified synchronization and security integration in deterministic networks
2. Insufficient fault tolerance under timing-sensitive and adversarial conditions
3. Limited architectural frameworks that jointly address industrial and automotive CPS requirements

Existing systems often optimize one dimension—such as latency or security—at the expense of others, resulting in fragile system-level performance.

1.3 Research Objectives

This study aims to:

- Develop a conceptual TSN-based architecture for deterministic communication
- Analyze synchronization mechanisms in distributed real-time networks
- Investigate cybersecurity vulnerabilities in time-sensitive protocols
- Evaluate fault tolerance strategies in automotive and industrial CPS
- Synthesize a unified framework supporting resilience, security, and determinism

1.4 Scope and Significance

The scope of this research spans automotive in-vehicle networks and industrial automation systems that rely on TSN standards. The significance lies in bridging the gap between theoretical TSN models and practical deployment constraints in safety-critical environments. The study builds upon established automotive architectural paradigms, particularly platform-based designs that emphasize modularity and scalability (Pelliccione et al., 2017).

2. LITERATURE REVIEW

2.1 Evolution of Automotive and Industrial Network Architectures

Automotive systems have transitioned from distributed ECUs connected via CAN buses to centralized computing platforms with high-bandwidth Ethernet backbones. The Race architecture introduced a centralized platform-based design that consolidates automotive applications into a unified computing environment, enabling improved performance and reduced system complexity (Sommer et al., 2013). However, such centralization increases dependency on deterministic communication infrastructure.

Similarly, Volvo's automotive architecture framework demonstrates the industrial feasibility of modular system design, emphasizing scalability and cross-domain integration (Pelliccione et al., 2017). This framework highlights the importance of structured communication layers and system abstraction for managing complexity in modern vehicles (Pelliccione et al., 2017).

2.2 Time-Sensitive Networking Foundations

TSN standards extend Ethernet by introducing time-aware scheduling, traffic shaping, and synchronization mechanisms. Messenger (2018) provides a foundational overview of TSN, emphasizing its ability to support real-time communication over shared networks. Lo Bello and Steiner (2019) further analyze TSN from an industrial automation perspective, identifying its role in enabling deterministic Ethernet for mission-critical systems.

However, TSN implementation complexity increases when integrated into heterogeneous automotive environments, where mixed-criticality traffic must coexist without violating timing constraints.

2.3 Synchronization Mechanisms and Challenges

Synchronization is a core requirement in TSN-based systems. IEEE 802.1AS and IEEE 1588 provide clock synchronization protocols, but their performance degrades under large-scale or adversarial network conditions. Gutiérrez et al. (2017) demonstrate that synchronization quality varies significantly in industrial automation networks depending on topology and traffic load.

Furthermore, Lisova et al. (2016) highlight that clock synchronization mechanisms are vulnerable to adversarial interference, requiring network-level monitoring for anomaly detection. Hirschler and Treytl

(2011) validate IEEE 1588 Annex K, emphasizing the need for robust verification methods to ensure synchronization correctness.

2.4 Cybersecurity in Time-Sensitive Networks

Security in TSN environments remains a critical concern. Alghamdi and Schukat (2021) analyze attack strategies targeting Precision Time Protocol (PTP), demonstrating that synchronization attacks can severely disrupt deterministic communication. Similarly, Lindberg (2011) examines vulnerabilities in vehicle diagnostic systems using DoIP, revealing potential entry points for attackers in automotive networks.

Schonberger et al. (2021) further investigate time-delay attacks on PTP systems, showing that increased detection sensitivity is necessary for mitigating subtle timing manipulations. Boatright and Tardo (2012) also emphasize security risks in Ethernet-based automotive backbones, particularly when integrating AVB technologies.

2.5 Predictability and Real-Time Systems Theory

Predictability is a fundamental requirement for real-time systems. Stankovic and Ramamritham (1990) define predictability as the ability of a system to guarantee bounded response times under all operating conditions. Grund et al. (2011) extend this concept by proposing formal templates for predictability definitions with supporting evidence.

These theoretical foundations are critical for TSN design, where deterministic communication must be maintained even under dynamic workloads and potential failures.

3. METHODOLOGY

3.1 Architectural Synthesis Approach

This research adopts a structured synthesis methodology combining conceptual modeling, comparative analysis, and theoretical integration. The architecture is derived by mapping TSN standards onto automotive and industrial CPS requirements, focusing on synchronization, fault tolerance, and cybersecurity integration.

The automotive architecture framework by Volvo Cars serves as a foundational reference model for system structuring and modular decomposition (Pelliccione et al., 2017). This framework is extended to incorporate TSN-specific communication layers and security modules.

3.2 Synchronization Modeling

Synchronization is modeled using IEEE 802.1AS and IEEE 1588 protocols as baseline mechanisms. Performance constraints are analyzed under varying network loads and adversarial conditions. The model evaluates clock offset, jitter, and propagation delay as primary metrics of synchronization quality.

3.3 Fault Tolerance Design

Fault tolerance is incorporated through redundancy-based architectures and lockstep processing mechanisms. Automotive-grade dual-core lockstep designs demonstrate how fault detection and correction can be embedded at the hardware level, improving system reliability (Abdul Salam Abdul Karim, 2023). These mechanisms are mapped onto TSN communication layers to ensure end-to-end resilience.

3.4 Cybersecurity Integration Framework

Cybersecurity is modeled as a layered defense mechanism targeting synchronization protocols, network traffic, and diagnostic communication channels. Attack surfaces include PTP manipulation, traffic injection, and anomaly-based disruptions. Detection mechanisms rely on network monitoring and event correlation strategies as discussed in industrial anomaly detection frameworks (Herold et al., 2016).

4. RESULTS

The analytical synthesis of Time-Sensitive Networking (TSN) architectures for automotive and industrial cyber-physical systems reveals several critical findings across synchronization, fault tolerance, and cybersecurity dimensions.

First, synchronization emerges as the most sensitive determinant of system-wide determinism. IEEE 802.1AS and IEEE 1588-based clock synchronization mechanisms provide acceptable performance under

controlled network conditions; however, their stability significantly degrades in large-scale or high-load environments. Empirical observations from industrial deployments indicate that synchronization quality is highly dependent on network topology and traffic shaping strategies (Gutiérrez et al., 2017). In scenarios with mixed-criticality traffic, jitter accumulation leads to bounded but non-negligible timing deviations, which directly impact deterministic scheduling guarantees.

Second, cybersecurity analysis demonstrates that TSN systems are inherently vulnerable to timing manipulation attacks. Precision Time Protocol (PTP)-based synchronization is particularly exposed to delay attacks and spoofing techniques. Studies show that even minor perturbations in synchronization packets can cascade into systemic timing failures, disrupting deterministic communication flows (Alghamdi & Schukat, 2021). Additionally, time-delay attacks targeting PTP significantly reduce system predictability, requiring advanced detection sensitivity mechanisms to maintain operational stability (Schönberger et al., 2021).

Third, fault tolerance mechanisms integrated at architectural and hardware levels significantly enhance system resilience. Lockstep-based dual-core architectures, as demonstrated in automotive zonal controllers, provide strong fault detection capabilities by executing redundant computational paths (Abdul Salam Abdul Karim, 2023). When combined with TSN scheduling mechanisms, these architectures ensure continuity of service even under partial hardware or communication failures. However, redundancy introduces additional latency overhead, requiring careful balancing between reliability and timing constraints.

Fourth, comparative architectural analysis shows that centralized automotive computing platforms improve scalability and resource efficiency but introduce systemic risks due to shared communication backbones. The Race architecture demonstrates that centralized control simplifies software integration but increases dependency on deterministic network infrastructure (Sommer et al., 2013). Similarly, automotive frameworks deployed in industrial environments highlight that modular design improves maintainability but requires strict synchronization enforcement across subsystems (Pelliccione et al., 2017).

Fifth, traffic shaping and Ethernet-based switching mechanisms play a crucial role in maintaining determinism. Analysis of Ethernet switch traffic shapers indicates that improper configuration can lead to queue congestion and deadline violations in in-vehicle networks (Thangamuthu et al., 2015). Therefore, scheduling policies must be tightly integrated with TSN timing models to ensure bounded latency.

Overall, the findings confirm that achieving deterministic, secure, and resilient TSN systems requires a tightly integrated co-design approach. Independent optimization of synchronization, security, or fault tolerance is insufficient for guaranteeing system-wide predictability in automotive and industrial CPS environments.

5. DISCUSSION

The results highlight a fundamental trade-off between determinism, security, and system complexity in TSN-based architectures. While synchronization protocols such as IEEE 802.1AS provide the structural foundation for time-aware communication, their vulnerability to adversarial interference introduces a critical challenge for real-world deployment. The dependence on precise timing makes TSN systems particularly sensitive to security breaches that target temporal consistency rather than data integrity.

From a theoretical perspective, predictability frameworks defined in real-time systems theory emphasize bounded response behavior under all conditions (Stankovic & Ramamritham, 1990). However, the findings of this study suggest that predictability in TSN environments cannot be guaranteed solely through scheduling and synchronization mechanisms. Instead, it must incorporate security-aware timing models that account for adversarial perturbations.

The automotive architecture framework proposed in industrial practice demonstrates that modular system design improves scalability and integration efficiency (Pelliccione et al., 2017). Nevertheless, this modularity introduces interdependency risks when multiple subsystems rely on shared timing infrastructure. Consequently, a failure in synchronization can propagate across the entire system, leading to cascading timing violations.

Cybersecurity considerations further complicate the TSN design landscape. Attacks on synchronization protocols, particularly PTP-based mechanisms, reveal that attackers do not need to compromise payload

data to disrupt system behavior; manipulating timing information alone is sufficient to degrade system performance (Alghamdi & Schukat, 2021). This shifts the security paradigm from data-centric protection to time-centric resilience.

Fault tolerance mechanisms, particularly lockstep architectures, provide strong mitigation against hardware-level failures. However, their integration into TSN systems introduces computational redundancy that may conflict with strict latency constraints. This trade-off necessitates adaptive scheduling strategies capable of dynamically balancing redundancy and performance requirements.

Industrial studies on Ethernet traffic shaping further reinforce the importance of correct network configuration. Improper shaping can lead to deadline misses, undermining the deterministic guarantees promised by TSN (Thangamuthu et al., 2015). Therefore, traffic engineering must be considered a core component of TSN architecture rather than a peripheral optimization layer.

In synthesis, the study demonstrates that TSN systems must evolve beyond traditional networking paradigms. A holistic design approach is required, integrating synchronization, fault tolerance, and cybersecurity into a unified architectural framework. Without such integration, deterministic guarantees remain theoretical rather than practical.

6. CONCLUSION

This research presented a comprehensive analytical study of secure and deterministic Time-Sensitive Networking (TSN) architectures for automotive and industrial cyber-physical systems. The study demonstrated that synchronization accuracy, fault tolerance, and cybersecurity resilience are deeply interdependent factors that collectively determine system determinism.

The key contribution of this work lies in synthesizing existing automotive and industrial network frameworks into a unified conceptual model that highlights the necessity of co-designed TSN architectures. The analysis confirmed that synchronization vulnerabilities, particularly in IEEE 802.1AS and IEEE 1588-based systems, represent a critical risk vector for system-wide stability. Additionally, cybersecurity threats targeting timing protocols were shown to have disproportionate effects on system determinism compared to traditional data attacks.

Fault tolerance mechanisms such as lockstep architectures improve system resilience but introduce additional latency constraints, requiring careful architectural balancing. Furthermore, centralized automotive computing frameworks enhance scalability but increase dependency on deterministic communication infrastructure, amplifying the impact of synchronization failures.

Future research should focus on developing adaptive TSN frameworks capable of real-time security awareness and self-correcting synchronization mechanisms. Integration of AI-driven anomaly detection and predictive fault mitigation may further enhance resilience in next-generation automotive and industrial CPS environments.

REFERENCES

1. Abdul Salam Abdul Karim. (2023). Fault-Tolerant Dual-Core Lockstep Architecture for Automotive Zonal Controllers Using NXP S32G Processors. International Journal of Intelligent Systems and Applications in Engineering, 11(11s), 877–885.
2. Alghamdi, W., Schukat, M. Precision time protocol attack strategies and their resistance to existing security extensions. Cybersecurity, 4(1), 1–17, 2021.
3. Baas, I. A glimpse into the future of travel and its impact on marketing. The Drum, 2018.
4. Boatright, R., Tardo, J. Security aspects of utilizing ethernet AVB as the converged vehicle backbone. SAE International Journal of Passenger Cars -Electronic and Electrical Systems, 5(2), 470–478, 2012.
5. Grund, D., Reineke, J., Wilhelm, R. A template for predictability definitions with supporting evidence. OpenAccess Series in Informatics, 18, 22–31, 2011.
6. Gutiérrez, M., Steiner, W., Dobrin, R., Punnekkat, S. Synchronization quality of IEEE 802.1AS in large-scale industrial automation networks. Proceedings of the IEEE RTAS, 273–282, 2017.
7. Hartwich, F. Introducing CAN XL into CAN networks. 17th CAN in Automation Conference, 2020.

8. Herold, N., Posselt, S.-A., Hanka, O., Carle, G. Anomaly detection for SOME/IP using complex event processing. IEEE/IFIP NOMS, 2016.

9. Hirschler, B., Treytl, A. Validation and verification of IEEE 1588 Annex K. IEEE ISPCS, 2011.

10. Lindberg, J. Security Analysis of Vehicle Diagnostics Using DoIP. Chalmers University, 2011.

11. Lisova, E., et al. Protecting clock synchronization: adversary detection through network monitoring. Journal of Electrical and Computer Engineering, 2016.

12. Lo Bello, L., Mariani, R., Mubeen, S., Saponara, S. Recent advances and trends in on-board embedded and networked automotive systems. IEEE Transactions on Industrial Informatics, 15(2), 2019.

13. Lo Bello, L., Steiner, W. A perspective on IEEE time-sensitive networking for industrial communication and automation systems. Proceedings of the IEEE, 107(6), 1094–1120, 2019.

14. Messenger, J. L. Time-sensitive networking: an introduction. IEEE Communications Standards Magazine, 2(2), 29–33, 2018.

15. Pelliccione, P., Knauss, E., Heldal, R., Ågren, S. M., Mallozzi, P., Alminger, A., Borgentun, D. Automotive architecture framework: The experience of Volvo Cars. Journal of Systems Architecture, 77, 83–100, 2017.

16. Schonberger, L., Hamad, M., Gomez, J. V., Steinhorst, S., Saidi, S. Towards an increased detection sensitivity of time-delay attacks on precision time protocol. IEEE Access, 9, 157398–157410, 2021.

17. Sommer, S., Camek, A., Becker, K., Buckl, C., Zirkler, A., Fiege, L., Armbruster, M., Spiegelberg, G., Knoll, A. Race: a centralized platform computer based architecture for automotive applications. IEEE IEVC, 2013.

18. Stankovic, J. A., Ramamritham, K. What is predictability for real-time systems? Real-Time Systems, 2(4), 247–254, 1990.

19. Thangamuthu, S., Concer, N., Cuijpers, P. J., Lukkien, J. J. Analysis of ethernet-switch traffic shapers for in-vehicle networking applications. DATE Conference, 55–60, 2015.

20. Tuohy, S., Glavin, M., Hughes, C., Jones, E., Trivedi, M., Kilmartin, L. Intra-vehicle networks: a review. IEEE Transactions on Intelligent Transportation Systems, 16(2), 534–545, 2014.