The American Journal of Applied Sciences

ISSN 2689-0992 | Open Access

TYPE Original Research
PAGE NO. 45-51

The Convergence of IEEE 802.11be, 5G, And Wired Time-Sensitive Networking: A Comprehensive Framework for Deterministic Industrial Cyber-Physical Systems

Priya Bharadwaj

Department of Electrical Engineering and Information Technology, University of Munich, Germany

OPEN ACCESS

SUBMITED 13 January 2025
ACCEPTED 02 March 2025
PUBLISHED 31 March 2025
VOLUME Vol.07 Issue 03 2025

CITATION

Priya Bharadwaj. (2025). The Convergence of IEEE 802.11be, 5G, And Wired Time-Sensitive Networking: A Comprehensive Framework for Deterministic Industrial Cyber-Physical Systems. The American Journal of Applied Sciences, 7(03), 45–51. Retrieved from https://theamericanjournals.com/index.php/tajas/article/view/7648

Abstract: The rapid evolution of Industry 4.0 has necessitated a paradigm shift from traditional "best-effort" networking to deterministic communication frameworks capable of supporting ultra-reliable low-latency communication (URLLC). Time-Sensitive Networking (TSN) has emerged as the foundational set of standards to provide these guarantees over Ethernet; however, the modern industrial landscape increasingly demands mobility and flexibility, shifting the focus toward wireless integrations. This research article provides an extensive investigation into the convergence of wired TSN standards with emerging wireless technologies, specifically 5G and IEEE 802.11be (WiFi 7). By analyzing the mechanisms of precise clock synchronization, scheduled traffic enhancements, and the impact of cyber-physical threats on synchronization stability, this paper establishes a holistic framework for next-generation industrial networks. We explore the architectural shifts from domain-specific E/E architectures in automotive sectors to zonal controllers and the integration of fault-tolerant dual-core lockstep systems. Furthermore, the paper delves into the security vulnerabilities inherent in the Precision Time Protocol (PTP), evaluating the impact of delay-box attacks and internal malicious actors on network integrity. Through a deep theoretical synthesis of current standards and empirical observations from recent literature, this study identifies the critical gaps in cross-layer synchronization and provides a roadmap for achieving microsecond-level jitter in heterogeneous wireless-wired industrial environments.

Keywords: Time-Sensitive Networking, WiFi 7, 5G URLLC, Precision Time Protocol, Industry 4.0, Cyber-Physical Security.

Introduction: The contemporary industrial landscape is undergoing a profound transformation characterized by the deep integration of physical processes with digital computation and networking, a phenomenon widely recognized as the Fourth Industrial Revolution or Industry 4.0. At the heart of this transformation is the requirement for seamless, deterministic communication between sensors, controllers, and actuators. Historically, industrial automation relied on proprietary Fieldbus systems or specialized Industrial Ethernet protocols to ensure that control loops remained stable. However, these siloed solutions created fragmented ecosystems that hindered the scalability and interoperability required for modern smart manufacturing. The emergence of Time-Sensitive Networking (TSN), a suite of standards developed by the IEEE 802.1 Working Group, marked a significant milestone by bringing determinism to standard Ethernet (Farkas, Bello, and Gunther, 2018).

TSN is not a single protocol but a complex toolbox of sub-standards designed to address various aspects of time-critical communication. These include time synchronization (IEEE 802.1AS), traffic scheduling (IEEE 802.1Qbv), frame replication and elimination for reliability (IEEE 802.1CB), and resource management. While wired TSN has seen significant adoption in automotive in-vehicle networks and factory floor backbones, the rigid nature of physical cabling presents a barrier to the "Agile Factory" concept, where mobile robots, Automated Guided Vehicles (AGVs), and modular production cells require high-bandwidth, low-latency wireless connectivity. This has led to an intense academic and industrial focus on extending TSN capabilities to wireless domains, specifically through 5G New Radio (NR) and the upcoming IEEE 802.11be, commercially known as WiFi 7 (John, Noor-A-Rahim, Vijayan, Poor, and Pesch, 2024).

The challenge of wireless TSN integration is multifaceted. Unlike copper or fiber optics, the wireless medium is inherently stochastic, prone to multi-path fading, interference, and variable propagation delays. Achieving the sub-microsecond synchronization accuracy required for high-performance motion control over a radio interface requires revolutionary changes to the MAC and Physical layers. For instance, while 5G offers a robust framework for URLLC, its integration with a wired TSN bridge requires complex mapping of internal 5G system (5GS) clocks to the external TSN grandmaster clock (Atiq, Muzaffar, Seijo, Val, and Bernhard, 2022). Similarly, WiFi 7 introduces Multi-Link Operation (MLO) and restricted Target Wake Time (rTWT) to mitigate the latency spikes common in previous WiFi generations, yet the alignment of these features with IEEE 802.1AS remains a subject of active research (Adame, Carrascosa-Zamacois, and Bellalta, 2021).

Moreover, as these networks become more interconnected and software-defined, the attack surface expands. The Precision Time Protocol (PTP), which serves as the heartbeat of TSN, is vulnerable to various cyber-physical attacks. Malicious actors can exploit the protocol's reliance on transparent and boundary clocks to introduce artificial delays or spoofed sync messages, leading to "time-chase" scenarios where the slave clocks are driven out of phase, potentially causing catastrophic failures in synchronized machinery (Lisova, Uhlemann, Åkerberg, and Björkman, 2017). Understanding the intersection of deterministic performance and cybersecurity is therefore paramount. This article seeks to provide an exhaustive analysis of these converging technologies, evaluating their theoretical foundations, implementation challenges in automotive and industrial sectors, and the evolving threat landscape that governs their deployment.

The theoretical underpinning of Time-Sensitive Networking is rooted in the transition from asynchronous to synchronous communication models. In a traditional Ethernet environment, packets are handled via a "best-effort" mechanism where queuing delays are non-deterministic and dependent on the overall network load. For time-critical applications such as closed-loop control in robotics, a delay of even a few milliseconds or a high degree of jitter can lead to instability in the physical system. Fedullo, Morato, Tramarin, Rovati, and Vitturi (2022) provide a comprehensive review of how TSN addresses these issues by partitioning the available bandwidth into distinct time slots, ensuring that time-sensitive traffic is never blocked by lower-priority data.

Central to this architecture is the IEEE 802.1Qbv standard, which introduces the Time-Aware Shaper (TAS). The TAS operates on a revolving schedule known as a Gate Control List (GCL), which dictates when the transmission gates for specific priority queues are open or closed. By aligning the transmission of critical packets with these open gate intervals, the network can guarantee that a packet will traverse the switch with near-zero queuing delay. However, the effectiveness of the TAS is entirely dependent on the precision of the network's common sense of time. If the clocks between the talker, the switches, and the listener are not perfectly synchronized, the "protected" window of the TAS may be missed, leading to collisions with non-critical traffic (Seol, Hyeon, Min, Kim, and Paek, 2021).

The evolution of clock synchronization is most prominently seen in the progression from the Network Time Protocol (NTP) to the Precision Time Protocol (PTP), specifically the IEEE 1588 standard and its TSN-specific profile, IEEE 802.1AS. Shrestha, Pang, and Dzung (2018) emphasize that in high-performance wireless environments, achieving precise synchronization involves compensating for the variable delays introduced by the wireless physical layer. This is particularly difficult in 5G networks, where the internal architecture is divided into the User Plane Function (UPF) and the Radio Access Network (RAN). To the external TSN network, the entire 5GS is treated as a "virtual TSN bridge," which necessitates a sophisticated translation between the 5G internal timing and the TSN domain timing (Satka, Ashjaei, Fotouhi, Daneshtalab, Mjödin, and Mubeen, 2023).

The shift toward wireless TSN is further catalyzed by the limitations of 4G and early WiFi versions in industrial settings. While 5G was designed with industrial use cases in mind through the 3GPP Release 16 and 17 specifications, WiFi has historically been a consumer-oriented technology. However, with the development of IEEE 802.11be, the WiFi alliance is directly challenging 5G in the industrial space. WiFi 7's introduction of Multi-Link Operation (MLO) allows a device to transmit and receive across multiple bands simultaneously, providing a redundancy mechanism that mirrors the wired IEEE 802.1CB standard. This redundancy is vital for mitigating the impacts of localized electromagnetic interference which is common in factory environments (Adame et al., 2021).

The automotive sector has been a primary driver for these advancements. Modern vehicles are transitioning from a distributed E/E (Electrical/Electronic) architecture, where dozens of Electronic Control Units (ECUs) are connected via low-speed CAN buses, to a centralized or zonal architecture. In these new models, high-performance zonal controllers manage large sections of the vehicle's functionality, all connected via an Ethernet TSN backbone. Navale, Williams, Lagospiris, Schaffert, and Schweiker (2015) discuss this "(R)evolution" of E/E architectures, noting that the sheer volume of data from LIDAR, cameras, and radar sensors requires the gigabit throughput and deterministic delivery that only TSN can provide. Furthermore, the safety-critical nature of automotive systems requires fault-tolerant hardware, such as dual-core lockstep processors, to ensure that transient hardware faults do not lead to system-wide failures (Abdul Salam Abdul Karim, 2023).

METHODOLOGY

To investigate the performance and security of integrated wired-wireless TSN systems, this research employs a multi-dimensional analytical framework. The methodology focuses on three primary pillars: synchronization accuracy, traffic scheduling efficiency, and security resilience.

First, we analyze the synchronization mechanism across disparate layers. In a wired TSN environment, synchronization is achieved through the exchange of Sync and Follow_Up messages. The methodology evaluates the mathematical models for calculating the Mean Path Delay and the Peer-to-Peer delay mechanism defined in IEEE 802.1AS. For the wireless component, we examine the "Time-of-Arrival" (ToA) estimation techniques used in 5G and WiFi 7. Specifically, we look at how the 5G System (5GS) acts as a transparent clock, utilizing the 5G internal reference clock to bridge the time between the TSN Translator at the network side and the TSN Translator at the device side (Atiq et al., 2022).

Second, the methodology addresses the scheduling complexity in a converged network. We utilize the theoretical constraints of the Time-Aware Shaper (TAS) to model how schedules are generated. In a heterogeneous network, the schedule must account for the different transmission characteristics of Ethernet, 5G, and WiFi. For example, while Ethernet has a fixed bit rate and predictable propagation, 5G scheduling is dependent on the Resource Block (RB) allocation by the gNodeB. We analyze the "Security-aware routing and scheduling" models proposed by Mahfouzi, Aminifar, Samii, and Eles (2019), which suggest that scheduling should not only optimize for latency but also for the isolation of critical traffic flows to prevent side-channel attacks.

Third, the methodology incorporates a threat-modeling component based on the STRIDE framework (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege). We apply this framework to the Precision Time Protocol to identify vulnerabilities in the synchronization path. We specifically focus on "Delay Attacks," where an attacker introduces a constant or fluctuating delay in the synchronization messages. This is modeled using sensitivity analysis to determine how much delay is required to desynchronize a slave clock beyond the operational threshold of an industrial actuator (Lisova et al., 2017). The methodology also reviews the effectiveness of MACsec (IEEE 802.1AE) and other cryptographic measures in protecting the integrity of these messages (IEEE, 2018).

Finally, we explore the integration of fault-tolerant architectures in zonal controllers. By examining the NXP S32G processor's dual-core lockstep (DCLS) mode, we evaluate how hardware-level redundancy complements network-level determinism. This involves analyzing the mechanism of "comparison logic" where two cores execute the same instructions, and any discrepancy triggers a fault recovery protocol, thereby ensuring that the data being sent over the TSN network is computationally correct (Abdul Salam Abdul Karim, 2023).

Detailed Analysis of Wireless TSN: 5G and WiFi 7 Convergence

The integration of 5G into the TSN ecosystem represents a significant leap toward the "Wireless Factory." In 3GPP Release 16, the 5G system was designed to support TSN as a set of features that allow the 5GS to appear as one or more TSN bridges. This "Black Box" approach is critical because it allows industrial operators to use existing TSN configuration tools, such as a Centralized Network Configuration (CNC) entity, to manage the wireless links without needing to understand the underlying 5G complexity.

The 5G TSN architecture relies on two key components: the Device-Side TSN Translator (DS-TT) and the Network-Side TSN Translator (NW-TT). These translators are responsible for ingress and egress time-stamping, as well as holding the port-level features of a TSN switch, such as the Time-Aware Shaper. As explored by Satka et al. (2023), the NW-TT handles the connection to the wired TSN grandmaster. When a Sync message arrives, the NW-TT timestamps it using the 5GS internal clock. As the message traverses the 5G core and the radio interface to the User Equipment (UE), the DS-TT uses the difference between its local 5GS clock and the NW-TT's timestamp to calculate the residence time within the 5G system. This residence time is then added to the original Sync message, effectively "transparentizing" the 5G network's internal delay.

However, challenges remain in the RAN (Radio Access Network). The 5G air interface uses Orthogonal Frequency Division Multiple Access (OFDMA), where resources are allocated in the time and frequency domains. For TSN traffic, the gNodeB must prioritize these packets using Semi-Persistent Scheduling (SPS) or Configured Grants (CG). These mechanisms allow the UE to transmit data without waiting for a specific scheduling request, which significantly reduces the "handshake" latency. Despite these features, the inherent jitter in 5G-caused by retransmissions (HARQ) and channel quality variations-remains higher than that of wired Ethernet. This necessitates larger "Guard Bands" in the TSN schedule, which can reduce overall bandwidth efficiency.

In parallel, IEEE 802.11be (WiFi 7) is introducing features that mimic TSN capabilities. The most prominent is the Restricted Target Wake Time (rTWT). In previous WiFi standards, TWT allowed devices to negotiate when they would wake up to transmit data, primarily for power saving. In WiFi 7, rTWT allows the Access Point (AP) to reserve specific time windows for latency-sensitive traffic, prohibiting other devices from contending for the medium during these slots. Adame et al. (2021) point out that this brings WiFi closer to the "Gated" model of IEEE 802.1Qbv. Furthermore, Multi-Link Operation (MLO) allows a WiFi 7 device to use 2.4 GHz, 5 GHz, and 6 GHz bands simultaneously. If one band suffers from a sudden burst of interference, the packet can be transmitted on another band, fulfilling the reliability requirements of TSN's IEEE 802.1CB (Frame Replication and Elimination for Reliability).

The comparison between 5G and WiFi 7 for industrial TSN reveals a trade-off between coverage and control. 5G offers superior mobility and wide-area coverage, making it ideal for large-scale outdoor logistics or massive factory complexes. However, 5G often requires a licensed spectrum or complex private network management. WiFi 7, operating in the unlicensed 6 GHz band, offers a more cost-effective solution for localized, high-density deployments. The work of John et al. (2024) suggests that a hybrid approach-where WiFi 7 handles the "last meter" connectivity to sensors and 5G provides the "backhaul" between production cells-may be the most viable path forward for Industry 4.0.

RESULTS

As networks move from isolated, air-gapped systems to integrated, cloud-connected frameworks, security becomes a primary concern. In a TSN environment, the most critical vulnerability is the time synchronization protocol itself. If an attacker can manipulate the perceived time, they can disrupt the entire schedule of the network, leading to packet collisions, buffer overflows, and the failure of real-time control loops.

One of the most insidious attacks is the "Delay Attack" or "Delay-Box Attack." In this scenario, a malicious node or a compromised switch intercepts PTP Sync messages and deliberately delays them before forwarding them to the next node. Because PTP relies on calculating the residence time or path delay to adjust the slave clock, an uncompensated delay causes the slave to believe its clock is faster or slower than it actually is. Lisova et al. (2020) describe this as a "time chase," where the slave clock's synchronization algorithm constantly tries to correct for an error that is being artificially injected. If the delay is carefully modulated, it can cause the slave clock to drift slowly enough to avoid detection by simple threshold-based monitors, yet significantly enough to move the transmission window of the TAS out of alignment with the network gates.

DeCusatis, Lynch, Kluge, Houston, Wojciak, and Guendert (2020) conducted experiments on the impact of cyberattacks on PTP, demonstrating that even low-intensity attacks can lead to microsecond-level offsets that are fatal for high-speed motion control. They suggest that traditional IT security measures, such as firewalls and encryption, are insufficient because they do not account for the temporal characteristics of the traffic. For example, a packet may be cryptographically secure and correctly routed, but if it arrives five microseconds late, it is "wrong" from a TSN perspective.

To counter these threats, several advanced methodologies have been proposed. Moussa, Kassouf, Hadjidj, Debbabi, and Assi (2020) suggest an extension to PTP that enables the detection of such attacks by using redundant timing paths and cross-checking the time from multiple grandmasters. If the time reported by one path significantly deviates from the others, that path is flagged as compromised. Similarly, Alghamdi and Schukat (2017) propose methodologies to deter internal attacks by using machine learning to establish a baseline of "normal" delay variations and flagging any deviation as a potential intrusion.

Another layer of security is provided by IEEE 802.1AE (MACsec), which provides point-to-point encryption and integrity checks at the Ethernet layer. While MACsec protects against spoofing and tampering of the packet content, it introduces its own set of challenges for TSN. The encryption and decryption process adds a constant latency to every hop. In a TSN network, this latency must be accounted for in the static schedule. Furthermore, the hardware must be capable of performing MACsec at wire speed to avoid introducing jitter. Li, Li, Zhang, Shou, Hu, and Liu (2021) propose a security management architecture that integrates PTP security with high-precision network management, ensuring that security protocols do not compromise the deterministic performance of the system.

Automotive E/E Architectures and Zonal Controllers

The automotive industry serves as a primary incubator for TSN technology. The transition from legacy protocols like LIN (Local Interconnect Network) and CAN (Controller Area Network) to Ethernet-based TSN is driven by the demand for autonomous driving and advanced infotainment. In a centralized vehicle architecture, the "Brain" of the car requires high-speed, low-latency data from various "Zonal Controllers" that aggregate sensor data from specific physical regions of the vehicle (e.g., front-left, rear-right).

Brunner, Rodger, Kurcera, and Waas (2017) discuss how Ethernet TSN enhances automotive E/E architectures by providing a scalable backbone. In this setup, critical traffic, such as braking and steering commands, is given the highest priority using the Time-Aware Shaper (IEEE 802.1Qbv), while infotainment data is sent via the Credit-Based Shaper (IEEE 802.1Qav) to ensure it doesn't starve the critical commands but also doesn't cause congestion. The use of IEEE 802.1CB for frame replication ensures that if a single cable or switch fails, a duplicate packet reaches its destination via a different path, providing the functional safety required by ISO 26262.

A critical component of these zonal controllers is the underlying hardware. Abdul Salam Abdul Karim (2023) highlights the use of the NXP S32G processor, which is designed specifically for automotive gateways and zonal controllers. The S32G features dual-core lockstep (DCLS) configurations for its ARM Cortex-M7 and Cortex-A53 cores. In DCLS mode, two cores execute the exact same stream of instructions in a staggered fashion (usually two clock cycles apart). A comparison unit checks the outputs of both cores. If a cosmic ray or electromagnetic interference causes a bit-flip in one core, the outputs will not match, and the system can immediately trigger a safe state. This hardware-level reliability is a necessary counterpart to the network-level reliability provided by TSN.

Farzaneh, Shafaei, and Knoll (2016) explore the formal verification of these in-vehicle networks. Because the configuration of TSN is so complex-involving hundreds of gate control lists and thousands of traffic flows-manual configuration is prone to error. They propose a logic programming-based approach to formally verify that a given TSN configuration will meet all deadline constraints under all possible traffic conditions. This move toward "Verified by Design" is essential as vehicles move toward Level 4 and Level 5 autonomy, where the network is literally a life-critical system.

DISCUSSION

The Future of Deterministic Communication

The convergence of wired TSN, 5G, and WiFi 7 represents a significant milestone, yet several challenges remain unresolved. The most prominent is the issue of "Cross-Domain Configuration." Currently, the configuration of a wired TSN switch, a 5G core, and a WiFi 7 access point involves three different management planes. For a truly seamless industrial network, a unified Centralized Network Configuration (CNC) is needed that can view the entire heterogeneous path as a single deterministic pipe. This requires standardization of the Northbound Interfaces (NBIs) of 5G and WiFi management systems to accept TSN-style configuration parameters (Nasrallah et al., 2019).

Furthermore, the environmental impact on wireless TSN performance cannot be ignored. In a factory with heavy metallic machinery, multi-path fading and shadowing can cause sudden, unpredictable drops in signal quality. While WiFi 7's MLO and 5G's URLLC features mitigate this, they do not eliminate the fundamental uncertainty of the wireless medium. Future research must focus on "Adaptive TSN," where the network schedule can dynamically adjust in real-time to changing channel conditions without violating the hard-real-time constraints of the applications.

From a security perspective, the industry must move beyond "Bolt-on" security. The integration of STRIDE-based threat modeling during the network design phase, as suggested by Microsoft (2021) and applied to TSN by various researchers, is a step in the right direction. However, we need more robust, hardware-accelerated security primitives that can provide nanosecond-level precision in timestamping while maintaining high-throughput encryption. The development of "Time-Aware Security" protocols that can detect anomalies not just in packet content but in the timing of packet arrival will be crucial for protecting the industrial infrastructure of the future.

Finally, the role of AI and machine learning in TSN management is an emerging frontier. As networks become too complex for human engineers to optimize, AI could be used to predict traffic bursts and pre-emptively adjust gate control lists. However, the non-deterministic nature of many AI algorithms contradicts the deterministic requirements of TSN. Reconciling these two paradigms-using "Black Box" AI to manage "White Box" deterministic networks-is perhaps the greatest theoretical challenge facing the field today.

CONCLUSION

This research has provided a comprehensive investigation into the state of Time-Sensitive Networking and its integration with 5G and WiFi 7. We have established that while wired TSN provides the necessary deterministic foundation, the future of Industry 4.0 and automotive E/E architectures depends on the successful extension of these guarantees to the wireless domain. The shift from distributed to zonal architectures in vehicles, supported by fault-tolerant hardware like dual-core lockstep processors, demonstrates the practical application of these technologies in safety-critical environments.

We have also highlighted the significant security risks associated with the Precision Time Protocol and the potential for cyber-physical attacks to disrupt synchronized systems. The analysis of delay-box attacks and the proposed detection mechanisms underscore the need for a holistic approach to network design that treats time as a first-class citizen in the security hierarchy. As we move toward 2030, the maturation of WiFi 7 and the continued evolution of 5G will likely see these technologies converge into a unified, deterministic, and secure communication fabric that will power the next generation of autonomous systems and smart factories.

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. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/7749
2. Adame, T., Carrascosa-Zamacois, M., and Bellalta, B. Time-sensitive networking in IEEE 802.11be: On the way to low-latency WiFi 7. Sensors, vol. 21, no. 15, p. 4954, 2021.
3. Alghamdi, W., and Schukat, M. Advanced methodologies to deter internal attacks in PTP time synchronization networks. Proceedings of the ISSC, Killarney, Ireland, June 20-21, 2017.
4. Atiq, M. K., Muzaffar, R., Seijo, S., Val, I., and Bernhard, H.-P. When IEEE 802.11 and 5G meet time-sensitive networking. IEEE Open Journal of the Industrial Electronics Society, vol. 3, pp. 14–36, 2022.
5. Brunner, S., Rodger, J., Kurcera, M., and Waas, T. Automotive E/E-architecture enhancements by usage of ethernet TSN. Proceedings of the 13th Workshop on Intelligent Solutions in Embedded Systems (WISES), Hamburg, Germany, 2017.
6. DeCusatis, C., Lynch, R. M., Kluge, W., Houston, J., Wojciak, P. A., and Guendert, S. Impact of cyberattacks on precision time protocol. IEEE Trans. Instrum. Meas., 69 (5), pp. 2172-2181, 2020.
7. Farkas, J., Bello, L. L., and Gunther, C. Time-sensitive networking standards. IEEE

Communications Standards Magazine, vol. 2, no. 2, pp. 20–21, 2018.

8. Farzaneh, M. H., and Knoll, A. Time-sensitive networking (TSN): an experimental setup. Proceedings of the IEEE Vehicular Networking Conference (VNC), Turin, Italy, 2017.

9. Farzaneh, M. H., Shafaei, S., and Knoll, A. Formally verifiable modeling of in-vehicle time-sensitive networks (TSN) based on logic programming. Proceedings of the IEEE Vehicular Networking Conference (VNC), Columbus, OH, USA, 2016.

10. Fedullo, T., Morato, A., Tramarin, F., Rovati, L., and Vitturi, S. A comprehensive review on time sensitive networks with a special focus on its applicability to industrial smart and distributed measurement systems. Sensors, vol. 22, no. 4, p. 1638, 2022.

11. IEEE. IEEE Standard for Local and Metropolitan Area Networks-Media Access Control (MAC) Security. Piscataway, NJ. USA, 2018.

12. IEEE standard for local and metropolitan area networks-bridges and bridged networks-Amendment 25: enhancements for scheduled traffic. IEEE Stand., 802, 2015.

13. IEEE. TSN Ethernet as Core Network in the Centralized Vehicle E/E Architecture: Challenges and Possible Solution. Piscataway, NJ. USA, 2019.

14. John, J., Noor-A-Rahim, M., Vijayan, A., Poor, H. V., and Pesch, D. Industry 4.0 and Beyond: The Role of 5G, WiFi 7, and Time-Sensitive Networking (TSN) in Enabling Smart Manufacturing. MDPI Future Internet, vol. 16, no. 9, p. 345, 2024.

15. Li, H., Li, D., Zhang, X., Shou, G., Hu, Y., and Liu, Y. A security management architecture for time synchronization towards high precision networks. IEEE Access, 9, pp. 117542-117553, 2021.

16. Lisova, E., Uhlemann, E., Åkerberg, J., and Björkman, M. Monitoring of clock synchronization in cyber-physical systems: a sensitivity analysis. Proceedings of the IINTEC, Gafsa, Tunisia, 2017.

17. Lisova, E., Uhlemann, E., Åkerberg, J., and Björkman, M. Delay attack versus clock synchronization-a time chase. Proceedings of the IEEE ICIT, Toronto, ON, Canada, 2017.

18. Mahfouzi, R., Aminifar, A., Samii, S., and Eles, P. Security-aware routing and scheduling for control applications on Ethernet TSN networks. ACM Transactions on Design Automation of Electronic Systems, 25, no. 1, 1–26, 2019.

19. Microsoft. Microsoft STRIDE threat model. Redmond, WA, USA, 2021.

20. Moussa, B., Kassouf, M., Hadjidj, R., Debbabi, M., and Assi, C. An extension to the precision time protocol (PTP) to enable the detection of cyber attacks. IEEE Trans. Ind. Inf., 16 (1), pp. 18-27, 2020.

21. Nasrallah, A., Thyagaturu, A. S., Alharbi, Z., Wang, C., Shao, X., Reisslein, M., and ElBakoury, H. Ultra-low latency (ULL) networks: The IEEE TSN and IETF DetNet standards and related 5G ULL research. IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 88–145, 2019.

22. Navale, V. M., Williams, K., Lagospiris, A., Schaffert, M., and Schweiker, M.-A. (R) evolution of E/E a. SAE International Journal of Passenger Cars - Electronic and Electrical Systems, 8, no. 2, 282–288, 2015.

23. Satka, Z., Ashjaei, M., Fotouhi, H., Daneshtalab, M., Sjödin, M., and Mubeen, S. A comprehensive systematic review of integration of time sensitive networking and 5g communication. Journal of Systems Architecture, vol. 138, p. 102852, 2023.

24. Seol, Y., Hyeon, D., Min, J., Kim, M., and Paek, J. Timely survey of time-sensitive networking: Past and future directions. IEEE Access, vol. 9, pp. 142 506–142 527, 2021.

25. Shrestha, D., Pang, Z., and Dzung, D. Precise clock synchronization in high performance wireless communication for time sensitive networking. IEEE Access, vol. 6, pp. 8944–8953, 2018.