

Technical White Paper

TSN and MACsec in Automotive Radar Applications



Abstract

Modern vehicles are moving from domain-based electrical architectures to zonal and central compute architectures, where data from multiple radar sensors is combined at a central processor and used for sensor fusion, distributed aperture radar, and advanced driver assistance. This shift places new demands on the Ethernet links that carry radar data. The link must distribute a precise, nanosecond-accurate time base so that every sensor captures data at the same moment, and the link must protect that data so that a central perception stack can trust the data received.

This white paper explains how two IEEE standards built into the Ethernet physical layer (PHY) address these needs in automotive radar applications. IEEE 802.1as (gPTP) provides time synchronization, while IEEE 802.1ae (MACsec) provides protection against spoofing, tampering, and eavesdropping attacks.

Table of Contents

1 Introduction.....	2
2 Time Synchronization for Radar With IEEE 802.1as.....	2
3 Securing Radar Data With MACsec.....	3
4 Using MACsec and PTP Together.....	4
5 TI Ethernet PHYs With TSN and MACsec.....	4
6 Conclusion.....	4
7 References.....	4

Trademarks

All trademarks are the property of their respective owners.

1 Introduction

Most vehicles on the road today use a domain architecture, in which electronic control units (ECUs) and the associated cabling are grouped by function, such as powertrain, body, infotainment, or ADAS. The industry is moving toward a zonal architecture, in which functions are grouped by physical location in the vehicle. Zonal modules aggregate the sensors and actuators in an associated area and connect to a central vehicle compute node over a high-speed Ethernet backbone. This architecture reduces the number of ECUs and the length of the wiring harness. The architecture also enables over-the-air (OTA) software updates to vehicle functions, which is the foundation of the software-defined vehicle (SDV) and the path toward higher levels of driving automation.

In this architecture, the central compute combines data from several radar sensors, and from cameras and other sensors, which are connected over Ethernet. Two requirements follow:

1. The data must be time-aligned. The central processor fuses data from several radars, and from cameras and other sensors. The fused result is only correct if every measurement describes the same moment in time. This depends on all sensors sharing a precise common time base, which IEEE 802.1as distributes over the Ethernet network.
2. The data must be trustworthy. Radar data travels over Ethernet cables that run through the vehicle; a central perception stack that makes braking and steering decisions must be able to verify that the data comes from the real sensor and has not been altered, replayed, or read in transit. IEEE 802.1AE MACsec provides this protection at the link layer.

2 Time Synchronization for Radar With IEEE 802.1as

Why Radar Needs a Shared Time Base

Sensor fusion without temporal aliasing: Radar and camera each have limits. A camera is sensitive to darkness, glare, and weather, while radar has lower angular resolution and cannot read signs or lane markings. Fusing the two overcomes the limits of each, but only if both measurements describe the same instant. Consider a vehicle traveling at 30m/s. If a camera captures a frame at $t = 0$ and the radar captures the frame at $t = 10\text{ms}$, the vehicle has moved 0.3m between the two measurements, and the fused result places the same object in two different positions. A shared time base lets the central processor timestamp each measurement and compensate for the difference, or lets the system trigger the sensors at the same moment in the first place.

Aligned frame start across radar sensors: Radar sensors that run from individual clocks drift apart by the parts-per-million (ppm) difference between those clocks, so the frames slide against each other over time. When the PHY in each sensor provides a frame trigger derived from the IEEE 802.1AS time, every radar starts the chirp sequence at the same network time. This action is useful whenever several sensors are meant to work as one system, the central ECU can combine the data without needing to compensate for timing differences. This function is essential for distributed aperture radar.

Distributed aperture radar: In a satellite architecture the central ECU combines data from several sensor heads. A further step is distributed aperture radar (DAR), in which two or more smaller radar heads operate together as one radar with a much larger virtual aperture, giving a finer angular resolution than any single head can. This requires the heads to be synchronized in time with nanosecond-level accuracy, which is well beyond what software-based synchronization can deliver. The quality of the Ethernet time base is therefore a direct performance factor for the radar system. See [ZEN-3P-DARSW](#) for more information on distributed aperture radar.

How IEEE 802.1as Works

IEEE 802.1AS (gPTP) is one of the *Time-Sensitive Networking* (TSN) standards. This standard lets every node in an Ethernet network share a common wall clock. One node acts as the leader and provides the reference time. Each follower node exchanges timestamped messages with the leader to correct the offset between the two clocks, correct the frequency drift of the local clock, and measure the path delay of the link. The achievable accuracy depends on how precisely the timestamps are captured. For more information on the gPTP algorithm and the timestamp handshake, see [Time Sensitive Networking With Ethernet PHY](#).

Timestamping Location

A packet can be timestamped in the PTP software stack, in the MAC of the processor, or in the PHY. Any variable delay between the wire and the point where the timestamp is taken becomes a timing error, so the closer to the cable the timestamp is taken, the more accurate the synchronization. The software, start-of-frame detect, and hardware methods are described in [How to Implement IEEE 1588 Time Stamping in an Ethernet Transceiver](#). For ADAS sensors such as radar, the PHY is the best place to take the timestamp, since the highest level of accuracy is achieved. A single-digit nanosecond level of accuracy can be achieved with this method, which is essential for applications such as distributed aperture radar.

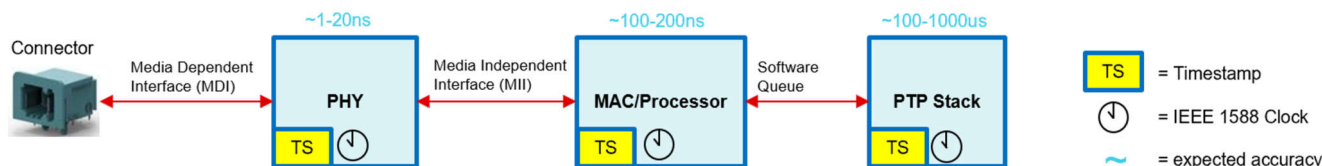


Figure 2-1. PTP Timestamping Location

3 Securing Radar Data With MACsec

Why Radar Links Need Security

Radar sensors in advanced driver assistance systems (ADAS) are safety-critical. These sensors provide the real-time data that a vehicle uses to detect obstacles, maintain safe following distances, and trigger emergency braking. As vehicles move toward zonal and central compute architectures, this data travels over Ethernet from the sensors to a central processor, which means the data passes through cables that run through the vehicle, and these cables are potentially physically accessible on the underside or front of the vehicle.

At the same time, modern vehicles have connections to the outside world through telematics, OTA update systems, and diagnostic interfaces. These connections increase the attack surface available to a malicious actor. An attacker who gains access to the in-vehicle network, whether physically or remotely, can target the radar data stream.

Threats to Radar Data

A radar link carrying safety-critical data is a potential target. The following table describes the main attack types, consequences of these attacks, and how MACsec addresses each potential attack.

Table 3-1. Threats and Mitigations for Radar Data

Threat	Description	Consequence	MACsec Protection Mechanism
Spoofing	Injecting a false <i>object detected</i> frame from a device that is not the radar	Unwanted emergency braking	Authenticated key agreement. Every frame carries an ICV that only a key holder can generate.
Replay	Recording a <i>clear road</i> stream and replaying the stream at a later time	A real obstacle is masked	Packet number in the SecTAG. Frames with old or repeated numbers are dropped.
Man in the Middle	Intercepting frames and modifying bits to change <i>obstacle</i> to <i>clear</i> or vice-versa	A real obstacle is masked	ICV integrity check on each frame. Modified frames fail the check and are dropped.
Eavesdropping	Capturing the stream to reverse-engineer sensor capability, resolution, or waveform	Loss of intellectual property	Payload encryption

MACsec in the PHY

MACsec, defined in IEEE 802.1AE, operates at layer 2, the data link layer. The sender adds a security tag (SecTAG) to every frame and appends an integrity check value (ICV), and encrypts the payload. The receiver verifies the SecTAG and the ICV, drops the frame if the check fails, and decrypts the frame if the frame passes.

The two ends establish keys with the MACsec Key Agreement (MKA) protocol defined with IEEE 802.1X. For a full description of how MACsec works, the frame format, and the key terms, see [Enhancing the Confidentiality and Integrity of Automotive Ethernet Data Using MACsec](#).

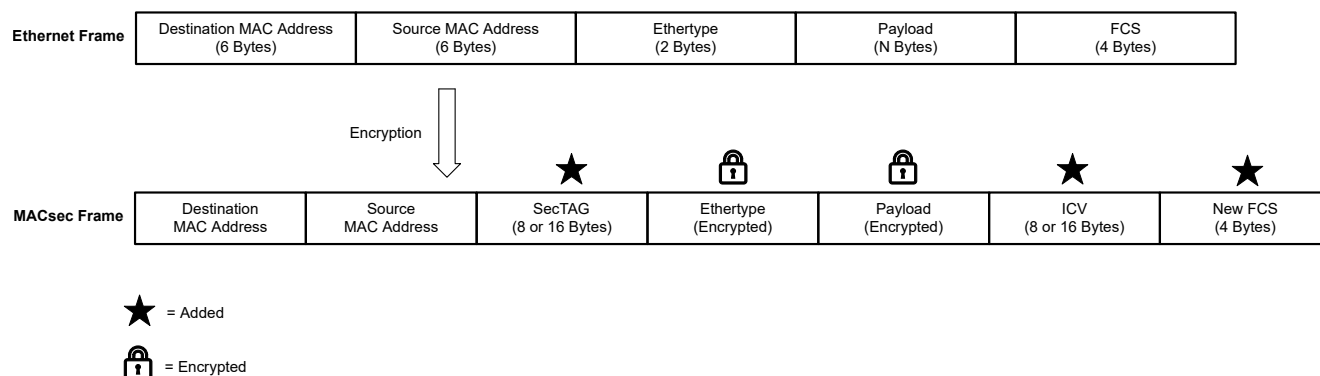


Figure 3-1. MACsec Ethernet Frame

4 Using MACsec and PTP Together

MACsec and IEEE 802.1AS can be used on the same link, so that a radar link has both secure data and an accurate time base. The DP83TC817-Q1 and DP83TC818-Q1 integrate IEEE 802.1as hardware timestamping and IEEE 802.1ae MACsec in one PHY. For links that need timing but not MACsec, the DP83TC815-Q1, DP83TC816-Q1, and DP83TG721-Q1 provide IEEE 802.1as hardware timestamping.

5 TI Ethernet PHYs With TSN and MACsec

TI offers single pair Ethernet PHYs with IEEE 802.1as hardware timestamping and IEEE 802.1ae MACsec for both 100Mbps and 1000Mbps as listed below in the table below.

Table 5-1. TI Offerings

Device	Speed	IEEE 802.1as	MACsec	AVB Clocks
DP83TC815-Q1	100Mbps	Yes	No	No
DP83TC816-Q1	100Mbps	Yes	No	Yes
DP83TC817-Q1	100Mbps	Yes	Yes	No
DP83TC818-Q1	100Mbps	Yes	Yes	Yes
DP83TG721-Q1	1Gbps	Yes	No	Yes

6 Conclusion

The move to zonal and central compute makes the Ethernet link a part of the radar measurement chain. A shared time base, accurate to nanoseconds, lets the vehicle fuse radar with other sensors without temporal aliasing, start the frames of several radars at the same network time, and enable distributed aperture radar. Timestamping in the PHY gives the best accuracy because this location excludes the latency variations of the MAC, the processor, and the operating system.

The same link must be protected. MACsec provides authentication, replay protection, integrity, and encryption at the line rate, which addresses spoofing, replay, tampering, and eavesdropping for radar streams. The DP83TC817-Q1 and DP83TC818-Q1 combine IEEE 802.1as and MACsec in one PHY, so that a 100BASE-T1 radar link can be both time-synchronized and secure.

7 References

1. Texas Instruments, [Are You Ready for the Emerging Automotive Radar Satellite Architecture?](#), technical article.
2. Texas Instruments, [DP83TC815-Q1 100Base-T1 Automotive Ethernet PHY Transceiver With IEEE802.1AS and TC10 Sleep-Wake](#), datasheet.

3. Texas Instruments, [DP83TC816-Q1 100Base-T1 Automotive Ethernet PHY Transceiver With IEEE802.1AS, AVB Clocks and TC10 Sleep-Wake](#), datasheet.
4. Texas Instruments, [DP83TC817S-Q1 Precise and Secure 100BASE-T1 Automotive Ethernet with IEEE802.1AE MACsec, IEEE802.1AS and TC10 Sleep-Wake](#), datasheet.
5. Texas Instruments, [DP83TC818S-Q1 Precise and Secure 100BASE-T1 Automotive Ethernet with AVB Clock Generation, IEEE802.1AE MACsec, IEEE802.1AS and TC10 Sleep-Wake](#), datasheet.
6. Texas Instruments, [DP83TG721x-Q1 1000BASE-T1 Automotive Ethernet PHY With Advanced TSN and AVB](#), datasheet.
7. Texas Instruments, [Enhancing the Confidentiality and Integrity of Automotive Ethernet Data Using MACsec](#), technical white paper.
8. Texas Instruments, [Ethernet PHY With Hardware Synchronization Extends the Range of Automotive Radar](#), technical article.
9. Texas Instruments, [How to Implement IEEE 1588 Time Stamping in an Ethernet Transceiver](#), technical article.
10. Texas Instruments, [How a Zone Architecture Paves the Way to a Fully Software-Defined Vehicle](#), white paper.
11. Texas Instruments, [Time Sensitive Networking With Ethernet PHY](#), technical white paper.
12. Zendar, [ZEN-3P-DARSW - Zendar Distributed Aperture Radar | High Resolution Radar with a Coherent Sensor Network](#), tool.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES "AS IS" AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you fully indemnify TI and its representatives against any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI's products are provided subject to [TI's Terms of Sale](#), [TI's General Quality Guidelines](#), or other applicable terms available either on [ti.com](#) or provided in conjunction with such TI products. TI's provision of these resources does not expand or otherwise alter TI's applicable warranties or warranty disclaimers for TI products. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

TI objects to and rejects any additional or different terms you may propose.

Copyright © 2026, Texas Instruments Incorporated

Last updated 10/2025