Standardized Vehicle-to-Vehicle Overtake Assistance Protocol

Emiliano F. Martín, Eng.

(Telecommunications engineer)

Contents

Preface

In 2010, as part of an engineering final project, we developed *GPS CAD*: a conceptual system where vehicles acted as mobile sensors, sharing position and motion data with a central server to infer real-time traffic conditions and assist route planning. The core idea was cooperative intelligence emerging from standardized data exchange between moving vehicles.

Years later, while driving on a two-lane rural highway, a different but related safety problem became evident: **the lack of reliable information when attempting to overtake slower vehicles in opposing-traffic roads**. Despite modern navigation, radar, and driver assistance systems, drivers still rely almost entirely online of sight and intuition to judge whether a passing manoeuvres is safe.

This document proposes a new step in cooperative vehicle intelligence: a **standardized, open Vehicle-to-Vehicle (V2V) communication layer specifically designed to assess overtaking safety**. This specification defines a communication layer and shared semantic meaning of fields. It does not define decision logic, HMI behaviour, or driving policy. It also provides advisory information only and shall not be the sole basis for safety-critical manoeuvres.

The intent is not to define a commercial product, but to publish a **technical seed** — an initial open framework that could evolve into a shared industry standard adopted by vehicle manufacturers, infrastructure providers, and research institutions.

If any organization, research group, or manufacturer is interested in advancing this concept toward real-world implementation or formal standardization, the author would welcome being informed and contributing where possible.

In April 2011, shortly after earning my degree, a former project partner and a friend — also an engineer — met with the intention of bringing GPS CAD (Computer Aided Driving) to life. Not long after, we discovered that Waze already existed and covered much of the original GPS CAD vision, so we decided to step back from the project.

Despite the many years that have passed since then, neither Waze, Google Maps, nor current autonomous driving systems have addressed the specific problem discussed in this document. A relevant safety niche still remains uncovered.

As of February 2026, to the author's knowledge, no publicly documented navigation or autonomous driving system provides a standardized, vehicle-agnostic cooperative protocol specifically focused on overtaking feasibility on two-lane roads. This statement is intended as contextual background rather than a comprehensive market survey.

This document is shared as a seed — an invitation to develop an open, cooperative standard aimed at making overtaking manoeuvres safer for everyone on the road.

Emiliano F. Martín

Vision Statement

Road safety **should not depend on vehicle brand**, model year, or proprietary ecosystems. Every vehicle on the road shares the same physical space, the same risks, and the same need for awareness of its surroundings.

The vision behind this proposal is to enable **universal cooperative driving assistance** through a common, open, and interoperable communication protocol. By allowing vehicles to exchange essential motion and safety-related information in a standardized way, drivers and on-board systems can make more informed decisions, especially in critical manoeuvres such as overtaking on two-way roads.

This work is not intended to define a finished solution, but to spark collaboration toward a **worldwide standard that prioritizes safety**, compatibility, and long-term interoperability over fragmentation.

Innovation, competition, and better user experiences should flourish on top of a shared foundation — one where every compliant vehicle can help protect every other road user.

Disclaimer

As stated before, this document is a seed. This document intentionally focuses on core concepts and architectural principles rather than exhaustive specification detail. It is not my intention to publish a flawless protocol at this stage.

If any company, organization, or independent group has the resources (people, time, and funding) to further develop this idea, refine the technical details, resolve incompatibilities, and improve performance, you are more than welcome to build upon it.

I would truly appreciate being informed if this work becomes the foundation for future development, even if the final protocol differs significantly from the definitions presented here.

I would also be glad to stay involved and contribute where possible, although I cannot guarantee the level of participation that a full standardization effort might require.

It is my hope that the **core purpose of this project** — improving road safety through open and universal vehicle cooperation — remains stronger than purely commercial interests. The vision is to foster a **worldwide interoperable protocol**, allowing every compliant vehicle to assist others regardless of manufacturer.

As adoption grows, manufacturers will naturally compete by building better hardware, improved performance, and more refined user experiences, while still relying on a common communication foundation. Such an ecosystem would benefit both innovation and safety.

With that said, let us now move on to the technical content of the document.

Introduction

Executive Overview — Safety Impact and System Value

Before discussing protocol structures, message formats, or implementation details, it is important to clearly state the practical value of this proposal.

What Problem Does This Solve?

Overtaking on two-lane roads with opposing traffic remains one of the most dangerous everyday manoeuvres in road transport. Drivers must estimate:

- Speeds of multiple vehicles
- Distance to oncoming traffic
- Required acceleration and time
- Available re-entry space

All under time pressure and often with limited visibility.

Human perception alone is frequently insufficient, leading to high-severity head-on collisions.

What This Protocol Enables

This protocol introduces **cooperative situational awareness** specifically targeted at overtaking safety.

Vehicles can share:

- Their real-time motion state
- The presence of non-cooperative vehicles
- Intent signals related to overtaking
- Information beyond line of sight through controlled relaying

The result is not automation, but **augmented human decision-making** based on a broader and more reliable situational picture.

Key Benefits

1. Reduced Head-On Collision Risk
Drivers gain awareness of oncoming vehicles beyond visual range, including those hidden by hills, curves, or traffic queues.

2. Safer Overtake Timing
The system evaluates whether the manoeuvre can be completed within conservative safety margins, accounting for uncertainty and latency.

3. Transparency of Assumptions
Drivers are informed of the assumed speed and number of vehicles considered, reducing blind trust and encouraging informed judgment.

4. Graceful Degradation
If data is incomplete or uncertain, the system withholds recommendations rather than issuing unsafe guidance.

5. Manufacturer Independence
The protocol standardizes **data exchange**, not user interfaces or decision algorithms, allowing innovation while maintaining interoperability.

Network Impact vs. Safety Gain

The communication overhead required to enable this cooperative awareness is **extremely small** relative to available V2V bandwidth, as shown in the feasibility analysis.

This represents a rare case in safety engineering where:

A minimal communication cost can address a manoeuvre responsible for some of the most severe crash types.

Executive Conclusion

This proposal does not aim to replace driver responsibility or create fully automated overtaking.
Its purpose is to provide drivers with **earlier, broader, and more reliable awareness** than human vision alone can offer.

By combining conservative modelling, cooperative data exchange, and transparent driver communication, the protocol has the potential to:

- Reduce fatal head-on collisions
- Improve decision quality in critical manoeuvres
- Do so **without overloading communication networks**

In short, it is a **low-bandwidth, high-impact safety layer** designed to be shared across manufacturers for the benefit of all road users.

1. The Problem

On two-lane roads with opposing traffic, overtaking is one of the most dangerous manoeuvres a driver can perform. The decision depends on multiple dynamic variables:

- Speed of the vehicles ahead
- Speed of oncoming traffic
- Distance and visibility
- Road geometry (curves, hills, crests)
- Driver reaction time

Human drivers estimate these variables visually, often under imperfect visibility and time pressure. Errors in judgment frequently lead to high-severity head-on collisions.

Existing driver assistance systems focus mainly on:

- Lane keeping
- Adaptive cruise control
- Collision avoidance in the same direction

Few systems actively assess **the safety of initiating and completing an overtaking manoeuvre** in real time.

Target audience: researchers, vehicle manufacturers, Tier-1 suppliers, road-safety specialists, and standardization bodies interested in cooperative V2V safety systems.

---

2. Opportunity for Cooperative Safety

Modern vehicles already possess:

- GNSS positioning
- Inertial sensors
- Radar and camera systems
- High-performance on-board processors

In parallel, Vehicle-to-Vehicle (V2V) communication technologies are emerging that allow nearby vehicles to exchange motion data with very low latency.

By combining:

1. **Local sensors** (radar, camera, IMU)

2. **High-definition maps**
3. **Standardized V2V motion messages**

Vehicles could collaboratively evaluate whether an overtaking manoeuvre can be completed **within safe spatial and temporal margins**, even beyond line of sight.

---

3. System Goals

The proposed protocol aims to:

1. Provide **real-time awareness** of nearby vehicles relevant to an overtaking manoeuvre
2. Support **predictive trajectory modelling** under uncertainty
3. Operate safely despite:
    - Packet loss
    - Positioning errors
    - Intermittent connectivity
4. Degrade gracefully when data quality is insufficient
5. Preserve **driver privacy** while ensuring vehicle identity uniqueness: messages contain no personally identifiable information. Device identifiers are designed to ensure protocol-level uniqueness while minimizing traceability to a specific vehicle or individual.
6. Be independent of any specific manufacturer or user interface

The system is advisory only and must be designed to **fail safe**: in case of uncertainty, it must refrain from recommending an overtake.

---

4. Communication Architecture

4.1 Localized Cooperative Awareness

Each equipped vehicle periodically broadcasts a compact Cooperative Motion Message (CMM) describing its dynamic state. When necessary, and under clearly defined relay rules, vehicles may retransmit selected messages to extend situational awareness beyond direct line of sight (for example, over hills or around traffic queues). Relaying is controlled rather than indiscriminate, ensuring that communication efficiency and channel capacity are preserved.

Messages are intended only for **nearby vehicles** in the same road segment and do not rely on centralized infrastructure.

4.2 Multi-Hop, Distance-Limited Dissemination

To extend awareness beyond direct line of sight (e.g., over hills or around traffic queues), vehicles may retransmit messages from others using controlled multi-hop forwarding.

To prevent uncontrolled propagation, each message includes:

- A **maximum relevance distance**
- A **timestamp and expiration time**
- Road segment relevance (derived from map matching)

Vehicles retransmit only messages that remain spatially and temporally relevant to their current road context.

4.3 Operation in Non-Line-of-Sight Conditions

Hills, crests, and curves may block direct radio communication. The system compensates through:

- Multi-hop message propagation
- Conservative safety margins when visibility is geometrically limited
- Map-based detection of no-visibility zones

If the system cannot confirm sufficient visibility or reliable opposing-traffic data, it must **withhold overtaking recommendations**.

---

5. Positioning Uncertainty and Safety Margins

GNSS positioning errors (commonly in the range of 1–10 meters depending on receiver quality and environmental conditions) can accumulate between vehicles. Therefore, the system must never treat positions as exact points. In fact, as it will be defined later, the vehicles should not be treated as points either but segments.

Instead, each vehicle is modelled as occupying a **dynamic uncertainty envelope** that accounts for:

- Positioning error
- Vehicle length
- Possible acceleration changes
- Communication latency

Trajectory predictions must consider **worst-case overlap scenarios**. An overtake may be recommended only if safe completion is possible even under pessimistic assumptions.

---

6. Cooperative Motion Message (CMM)

6.1 Purpose

The CMM provides a standardized description of a vehicle's motion state for cooperative safety calculations. These definitions **represent the version=**0 of the protocol. Eventually, a version 1 could exist with different sizes or definitions for the messages.

6.2 Example Data Fields

- Anonymous Vehicle ID
- Timestamp
- Position (latitude, longitude, altitude)
- Velocity vector
- Acceleration estimate
- Heading
- Vehicle length class
- Position confidence indicator
- Motion status flags (braking, accelerating, turn signal active, overtake intention)

Messages should be compact and transmitted at a frequency appropriate for low-latency safety applications.

---

7. Overtake Feasibility Logic

When the driver requests assistance, the vehicle:

1. Identifies relevant vehicles ahead and in the opposing lane
2. Predicts future positions with uncertainty margins
3. Calculates required distance and time to complete the manoeuvre
4. Verifies road geometry constraints from maps
5. Issues one of the following outcomes:
    - **Safe with high margin**
    - **Not safe**

- **Insufficient data**

During the manoeuvre, continuous re-evaluation may trigger an **abort recommendation** if conditions change.

The system **shall not recommend overtaking** in areas where road rules, map data, or infrastructure constraints prohibit the manoeuvre (e.g., tunnels, solid centre lines, restricted visibility zones).

When reliable positioning or map context cannot be confirmed (for example due to GNSS degradation in tunnels or dense environments), the system shall default to a conservative outcome and refrain from recommending an overtake manoeuvre. This specification defines communication semantics only and does not mandate or enforce driving behaviour.

In other words, absence of reliable environmental information shall never be interpreted as clearance to proceed.

---

8. Human Interface Independence

This document does not define how information is presented to the driver. Manufacturers may choose:

- Visual indicators
- Head-up displays
- Haptic feedback
- Auditory alerts

The protocol standardizes **data exchange**, not user experience.

---

9. Limitations and Ethical Considerations

The system:

- Does not replace driver responsibility
- Cannot guarantee absolute safety
- Must be designed to minimize false “safe” indications
- Must comply with regional legal and spectrum regulations

10. Legal and Attribution Considerations

This protocol is not intended to provide legal-grade evidence of driver behaviour, nor to enable enforcement actions such as speed violations or liability attribution.

Devices participating in the network may be transferred between vehicles, resold, or installed in configurations not known to manufacturers or authorities. As a result, the association between a transmitted message and a specific vehicle — and even more so a specific driver — cannot be guaranteed.

Furthermore, V2V messages are based on onboard sensor estimates and GNSS-derived positioning, which are inherently subject to measurement uncertainty. These messages are designed for cooperative situational awareness, not for forensic reconstruction or legal enforcement.

For these reasons, information exchanged under this protocol should be treated as advisory and cooperative in nature, and not as legally binding or attributable evidence of a traffic infraction.

---

11. Conclusion

This proposal outlines an open, cooperative approach to one of the most dangerous everyday driving manoeuvres. By combining local sensing, shared motion data, and conservative predictive modelling, vehicles could assist drivers in making safer overtaking decisions.

The aim of this document is to seed the creation of a **single worldwide standard protocol**. This is essential to ensure that every compliant device can correctly interpret messages regardless of the brand that transmitted them. While each vehicle or display manufacturer remains free to define the user interface and user experience — including how surrounding vehicles are shown or how the driver interacts with the system — the underlying data format must be shared. Manufacturers may also implement their own algorithms to estimate distances and determine whether an overtaking manoeuvre is safe, but all devices must speak a common, interoperable language.

The author invites collaboration from researchers, standards bodies, and manufacturers interested in developing this concept into a real-world interoperable standard.

Author's Note

This document represents a conceptual and exploratory proposal rather than a finalized technical standard. Its purpose is to seed discussion, inspire development, and encourage expert review.

While the author has an engineering background, the fields involved in cooperative vehicular communications, radio systems, and high-integrity positioning are broad and specialized. Therefore, many implementation details and technical decisions are intentionally left open for refinement by professionals with domain-specific expertise.

This document represents an architectural and conceptual proposal intended to stimulate expert discussion and collaborative refinement. Certain engineering domains involved (e.g., radio resource management, high-integrity positioning, and cooperative perception) require deep specialization, and therefore some parameters and mechanisms are deliberately left open for expert-driven optimization.

Readers are encouraged to question assumptions, validate mechanisms, and improve upon the ideas presented here. The goal is not to deliver a finished specification, but to contribute a starting point for a collaborative effort toward safer roads.

Development

Some extra considerations before the technical stuff should be explained first to set up the main definitions of the protocol itself.

As already stated, the aim is to define the protocol, each manufacturer will define how to interact with the user, which information will be shown (and how) and how will process and/or calculate the speeds/distances.

Message Consistency and Self-Data Override

When a vehicle retransmits Cooperative Motion Messages originally generated by other vehicles, it **must first inspect whether any message in its buffer refers to itself**.

If so:

- Any relayed data describing the host vehicle must be **discarded**
- The vehicle must insert its **most recent locally generated state data** instead

This ensures that:

1. The freshest and most accurate data about each vehicle is propagated
2. Stale or indirect descriptions of a vehicle do not persist in the network
3. Each vehicle remains the authoritative source of its own motion state

Detection of Non-Cooperative Vehicles

Vehicles equipped with perception sensors (radar, LIDAR, cameras) may detect road users that do not broadcast Cooperative Motion Messages.

In such cases, the detecting vehicle may generate and transmit a **Non-Cooperative Object Report (NCOR)** with the following constraints:

- The object must be labelled with a temporary identifier marked as **ANONID.**
- No personally identifiable information (license plate, make, model, or visual identity) must be included.
- Only kinematic and geometric estimates may be transmitted (position, speed, direction, size class, confidence level)

The idea of these NCOR-type CCM is to provide the system with information of vehicles that are not compliant with this protocol. If this equipped vehicle

detects (with the aid of their sensors or cameras) the presence of a vehicle which has already published its information it **must refrain from transmitting a NCOR message**.

Replacement by Authoritative Self-Reports

If a vehicle previously reported as **ANONID** later begins transmitting its own Cooperative Motion Messages:

- Receiving vehicles must prefer the **self-reported data.**
- Corresponding **ANONID** reports referring to the same physical object should be discarded once correlation confidence is high.

Persistence of ANONID Objects

If a detected vehicle never transmits cooperative messages:

- Other vehicles may continue to propagate its presence using **ANONID** object reports.
- These reports must include a **confidence level** that decays over time if the object is not re-observed.

🔁 Message Propagation Scope and Relay Rules

To prevent uncontrolled message flooding while still enabling non-line-of-sight awareness, all Cooperative Motion Messages (CMM) must follow a geographically bounded relay policy.

Each vehicle shall only retransmit messages from other vehicles if the original sender is considered spatially relevant according to the following rule:

A message is eligible for retransmission only if the sender's reported position is within:

- **1.5 km ahead** of the receiving vehicle (in the direction of travel), or
- **1.0 km behind** the receiving vehicle (in the direction of travel).

If a received message does not satisfy this condition, the receiving device shall:

- Forward the message with **TTL = 0**, and
- Refrain from evaluating it for further retransmission.

This allows the message to still reach vehicles slightly beyond the relevance boundary, but ensures it will not propagate further or consume processing resources unnecessarily.

This spatial filter applies to T1, T2, T3, and NCOR-derived messages.

Every 10Hz should analyse all actual T2 messages and re-transmit them. Every 1Hz should analyse all actual T1 messages and re-transmit them.

Relay decisions must NOT be based solely on (TempID + SequenceNumber) history.

Multi-hop forwarding exists to extend spatial coverage, not to suppress repeated awareness. Its purpose is to extend the propagation even if a slope a curve interferes with direct line of sight.

A relay node must evaluate spatial relevance, TTL, and freshness — not just duplication history.

Third-Party T2 Relay Rules

A vehicle may retransmit T2 messages originally generated by other vehicles to extend awareness beyond line-of-sight limitations.

However, retransmission shall be subject to the following constraints:

1. The original sender must be within the defined spatial relevance window (1.5 km ahead / 1.0 km behind).
2. The message is neither expired based on timestamp nor its timestamp is older than 1 second relative to GNSS time.
3. The relay node must replace any relayed description of itself with its own latest self-generated T2.
4. Under channel congestion, relaying of third-party T2 messages shall be reduced before reducing transmission of self-generated T2 messages.

A message shall be relayed ONLY if ALL the following conditions are met (in order):

1. TTL > 0
2. Timestamp not expired
3. Spatial relevance condition satisfied
4. Channel load control allows transmission

This ensures spatial continuity of awareness while prioritizing local accuracy and channel stability.

Fields definitions

🆔 Temporary Anonymous Vehicle Identifier (TEMPID)

Each transmitting device shall use a **Temporary Anonymous Vehicle Identifier (TempID)** to identify its messages at the protocol level without revealing the physical identity of the vehicle, its owner, or the on-board unit.

The TEMPID is designed to support cooperative awareness while preserving user privacy.

Definition

The **TempID** is a temporary, non-persistent, randomly generated identifier with the following properties:

- Length: **48 bits (6 bytes)**
- Generated using a **cryptographically secure random number generator (CSPRNG)**
- Shall not contain embedded information about the vehicle, device, manufacturer, location, or time
- Shall have **no deterministic relationship with previous or future identifiers used by the same device**

The identifier is used solely for:

- Message association
- Duplicate suppression
- Motion tracking within a limited spatial and temporal scope

The **TempID** shall not be used as a permanent vehicle identifier. Devices should avoid reusing recently observed **TEMPID**s within a short time window (e.g., 60 seconds) when generating a new **TEMPID**, to minimize transient collision risk.

Reserved Value — ANONID

The following value is reserved and shall not be used as a valid **TempID**:

ASCII "ANONID"

Hexadecimal: 0x41 0x4E 0x4F 0x4E 0x49 0x44

This value is reserved for use in **NCOR (Non-Cooperative Object Report) messages** to represent objects that do not have an assigned **TempID**.

If the random **TempID** generation process produces this value, the device shall discard it and generate a new **TempID**.

Under no circumstances shall a cooperative transmitting vehicle use the ANONID value as its **TempID**.

Collision Probability and Suitability

A 48-bit identifier provides:

281,474,976,710,656 possible values (over 281 trillion)

This extremely large identifier space makes accidental collision highly unlikely even in dense traffic environments involving very large numbers of vehicles.

This size provides an appropriate balance between:

- Privacy protection
- Operational reliability
- Efficient message size
- Minimal wireless channel usage

Increasing the identifier length would provide negligible practical benefit while increasing communication overhead.

Even under extremely dense traffic conditions, the probability of two vehicles selecting the same **TEMPID** simultaneously is negligible.

The following table illustrates the probability using the birthday paradox approximation:

Number of simultaneous vehicles	Collision probability
100 vehicles	0.0000000018 %
1,000 vehicles	0.00000018 %
10,000 vehicles	0.000018 %
100,000 vehicles	0.0018 %

Number of simultaneous vehicles	Collision probability
1,000,000 vehicles	0.18 %

Real-World Context

Even the most congested highway segments rarely exceed:

200–300 vehicles within communication range

At that density, collision probability is effectively zero.

Additionally, this protocol includes collision detection mechanisms based on:

- Position consistency
- Motion continuity
- Timestamp progression
- TTL evolution

If a collision is detected, both vehicles are required to generate new **TEMPID**s.

Conclusion

TEMPID collisions are:

- Statistically negligible
- Detectable
- Recoverable
- Non-disruptive to protocol operation

Therefore, 48-bit **TEMPID**s provide sufficient uniqueness while preserving minimal packet size and optimal bandwidth efficiency. For comparison, the probability of **TEMPID** collision at typical traffic densities is significantly lower than the probability of GNSS position overlap within its normal error margin.

Identifier Change Policy

To preserve anonymity and prevent long-term tracking, **TempID**s shall be temporary and periodically replaced.

Identifier change should occur:

- At randomized time intervals
- After vehicle restart
- After extended stationary periods
- When leaving and re-joining traffic
- When privacy conditions are favourable (for example, when surrounded by multiple vehicles)

Identifier change should preferably occur when:

- Vehicle speed is zero, or
- The vehicle remains stationary for several seconds

This reduces the ability of external observers to correlate identifiers based on motion continuity.

TempID changes shall not be explicitly announced. When a device changes its **TEMPID**, it shall immediately discard any locally stored relay messages that use its previous **TEMPID**.

TEMPID Transition Handling by Receiving Vehicles

If a receiving device determines that two different **TEMPID**s correspond to the same physical vehicle based on position continuity and timestamp consistency, it shall:

• Treat the newer **TEMPID** as the valid identity.

• Discard relay entries associated with the older **TEMPID**.

Receiving devices shall not permanently suppress retransmission solely based on **TEMPID** reuse, as **TEMPID**s are anonymous and may be reassigned to different vehicles over time.

Each message shall be evaluated independently based on its timestamp, position, and relay validity.

Collision Detection and Resolution

A TEMPID collision shall be assumed if messages with identical TEMPID are received that cannot originate from the same message propagation chain.

This condition is met if any of the following apply:

• Messages have identical TEMPID but inconsistent timestamps relative to propagation delay

• Messages have identical TEMPID but incompatible TTL values that cannot result from normal relay behaviour

• Messages with identical TEMPID originate from spatially incompatible positions given their timestamps and relay constraints

When a collision is detected:

Both vehicles shall generate a new TempID as soon as reasonably possible.

The new **TempID** shall be generated using the same random generation requirements.

Normal operation shall resume using the new **TempID**.

TEMPID collision detection should consider spatial proximity within a realistic GNSS uncertainty margin.

Under normal automotive GNSS operation, horizontal uncertainty rarely exceeds 10 meters.

Therefore, if two messages share the same TEMPID but differ by more than 30 meters within a short time window (e.g., < 500 ms), they shall be considered distinct vehicles.

Additional discrimination shall use:

• Sequence Number continuity

• Timestamp consistency

• TTL evolution

A retransmitted packet will always preserve timestamp and sequence number while presenting a lower TTL value.

TEMPID Generation — Blacklist and Reuse Prevention

To reduce the risk of identifier confusion and ensure continuity of vehicle tracking, devices shall avoid assigning a **TEMPID** that could be associated with another vehicle in recent memory.

When generating a new **TEMPID**, the following values shall be excluded from selection:

- The reserved value **ANONID**.
- The vehicle's current **TEMPID**.
- Any **TEMPID** currently in use by nearby vehicles.

- Any **TEMPID** present in the local **TEMPID** blacklist.

The **TEMPID** blacklist shall include:

Recently changed own TEMPIDs

TEMPIDs previously used by the same vehicle shall remain in the blacklist for at least **1 minute** after replacement.

This prevents other vehicles still receiving delayed or relayed messages from misinterpreting the identifier change.

Recently disappeared TEMPIDs

TEMPIDs associated with vehicles that have disappeared from reception range shall remain in the blacklist for at least **5 minutes**.

This prevents reassignment of identifiers that may still belong to legitimate vehicles that temporarily moved out of range and may reappear.

Rationale

Without this safeguard, the following ambiguity could occur:

A vehicle ahead using **TEMPID** *ABCDEF* leaves communication range. Shortly afterward, another vehicle generates a new **TEMPID** and randomly selects *ABCDEF*.

When the original vehicle re-enters range, nearby devices would observe two distinct vehicles using the same **TEMPID**, leading to incorrect tracking and potentially unsafe overtake calculations.

The blacklist mechanism ensures sufficient temporal separation to avoid such conflicts.

Privacy Considerations

The use of temporary random **TempID**s ensures that:

- Messages cannot be linked to a specific vehicle identity
- Long-term tracking becomes
- Vehicle identity and ownership remain protected

Tracking a vehicle would require continuous physical observation, which provides no advantage over direct visual identification.

This design provides strong privacy protection while maintaining full protocol functionality.

🕒 Timestamp

All CMM messages shall include a **32-bit timestamp**.

Timestamp format:

- Unit: **milliseconds**
- Reference: **GNSS time (GPS time or equivalent global satellite time)**
- Wraparound is allowed and receivers must handle modular arithmetic

Timestamps are used for:

- Motion prediction alignment
- Expiration of stale data
- Correlation of NCOR and cooperative reports

Definition

The **Timestamp** represents the absolute time at which the vehicle state data contained in the message was generated.

It shall be derived from the vehicle's **GNSS-synchronized clock** or an equivalent time source disciplined by GNSS.

The timestamp reflects **measurement time**, not transmission or retransmission time.

Retransmitting devices **must not modify** the original timestamp.

Encoding

- Size: **32 bits unsigned integer**
- Unit: **milliseconds**
- Epoch: **GNSS time-of-week (TOW)** modulo one week

This provides:

- Resolution: **1 ms**

- Range before wrap:

2^{32} ms ≈ 49.7 days (well beyond the GNSS week rollover period when modulo is used)

Using GNSS time-of-week avoids dependency on civil time (UTC, leap seconds, time zones).

Wrap Handling

Since the timestamp is modulo the GNSS week, receivers shall handle wrap-around by assuming the smallest positive time difference when comparing two timestamps from the same sender.

Receiver Usage

Receivers shall use the timestamp to:

• Determine **data age**

• Discard **expired messages**

• Select the **most recent state** when multiple messages about the same vehicle are available

• Evaluate **temporal consistency** for motion prediction

Timestamp **must take precedence over Sequence Number** when determining message freshness.

Message Expiration

A message shall be considered **expired** if:

Current_GNSS_Time – Message_Timestamp > Expiration_Threshold

Recommended default values:

Message Type	Expiration Threshold
T2 (state)	1 second

Message Type	Expiration Threshold
NCOR	1 second
T3 (event)	5 seconds
T1 (static)	10 seconds

Expired messages must not be processed nor retransmitted.

Clock Synchronization

Devices shall maintain time synchronization using GNSS signals. If GNSS time is temporarily unavailable, devices may continue transmitting using their internal clock but shall:

- Increase Position Confidence uncertainty accordingly
- Mark degraded operation if drift exceeds acceptable bounds

Rationale

Using an absolute GNSS-based timestamp instead of relative timers:

• Allows consistent multi-vehicle temporal alignment

• Prevents relay devices from "refreshing" old data

• Enables correct motion modelling across different manufacturers

• Keeps protocol independent from local time settings

Sequence Number

Each message type (T1, T2, T3, NCOR) shall include an **16-bit sequence number** maintained independently per sender and per message category. The sequence number wraps around when reaches the maximum value. With a 10Hz frequency that would happen every 25 seconds with an 8-bit sequence number. This could lead to misinterpretation as an old message (26 seconds old) reaches the device with the same sequence number as a newer. In those cases, the device should also check the timestamp to detect if there are different messages or the same. To avoid extra complexity, this number was defined as a 16-bit value.

The sequence number shall:

- Increment by 1 for each new message of the same type generated by the device
- Wrap around after 65.535
- Be used by receivers to:
    - Detect duplicates caused by multi-hop relays
    - Discard out-of-order stale packets
    - Avoid retransmission loops

Receivers should maintain a short history buffer per sender to suppress duplicates.

Definition

The **Sequence Number** is a monotonically increasing counter assigned by the transmitting device to each newly generated message of a given type (e.g., T2 or T3).

It is used to:

- Detect **duplicate packets**
- Detect **out-of-order reception**
- Detect **packet loss**
- Distinguish **new measurements** from delayed retransmissions of older ones

The Sequence Number **does not represent time** and **must not be used as a substitute for the timestamp**.

Scope

The counter is **maintained independently per transmitting TempID** and per message type where applicable.

A retransmitting device **must NOT modify** the original Sequence Number.

Encoding

- Size: **16 bits unsigned integer**
- Range: **0 – 65,535**
- Wrap-around: After reaching 65,535 the value restarts at 0

At a 10 Hz transmission rate, wrap-around occurs approximately every **1.8 hours**, which is sufficient when combined with timestamp validation.

Receiver Behaviour

When a message is received:

1. **Duplicate Detection**

   If (**TempID**, SequenceNumber) has already been processed recently, the packet shall be discarded.

2. **Out-of-Order Handling**

   If the Sequence Number is lower than the last valid one received from the same **TempID** but the timestamp is newer, the timestamp shall prevail and the message may still be processed.

3. **Loss Detection**

   If the Sequence Number increases by more than 1, receivers may assume one or more packets were lost. This information may be used to adjust confidence in derived values.

4. **Wrap-around Handling**

   If the Sequence Number suddenly drops to a very low value while the timestamp continues to increase, receivers shall assume a counter wrap-around rather than a replay attack or malfunction.

Rationale

Timestamp alone cannot:

- Reliably detect duplicate packets caused by multi-hop retransmission
- Guarantee ordering under wireless jitter
- Indicate packet continuity

Sequence Number provides **communication-layer consistency**, while the timestamp represents **physical-world time**.

📡 Channel Load and Congestion Control Strategy

To maintain communication reliability under dense traffic conditions, devices must adapt transmission behaviour according to estimated channel load.

Baseline transmission rates:

- T1: 1 Hz
- T2: 10 Hz

Under detected channel congestion:

- T2 rate may be reduced gradually down to **2 Hz minimum** for vehicles traveling faster than 40 km/h
- T3 and safety-critical intent messages must always have **priority over T1**
- Relaying of third-party messages should be reduced before reducing transmission of self-generated motion data

Devices shall prioritize:

1. Self T2 messages
2. Safety-related T3 messages
3. NCOR messages
4. T1 presentation messages

👁 NCOR (Non-Cooperative Object Report) Update and Suppression Rules

Any vehicle capable of perceiving non-cooperative road users may generate NCOR messages.

However, to prevent duplication and stale propagation:

A device shall remove from its relay buffer any NCOR referring to an object that:

- Matches a currently observed object in position and velocity within a short time window, or
- Matches a cooperative T1/T2 messages from a real transmitting vehicle

Correlation shall be based on:

- Spatial proximity
- Velocity similarity
- Temporal consistency

Once a real cooperative report or a fresher local perception exists, older third-party NCORs for the same object shall not be retransmitted.

Temporal consistency means that the motion reported by the NCOR message must be physically compatible with the motion reported by another observation over time.

For example, if an NCOR indicates that an object was traveling at 28 m/s at position A at a given timestamp, and a later T2 message reports a vehicle traveling at approximately the same speed and located near the expected propagated position (e.g., ~28 meters ahead after 1 second), both reports shall be considered to refer to the same physical object.

In such cases, the NCOR message shall be discarded and only the cooperative T2 message shall be processed and, if applicable, retransmitted.

Correlation shall allow for reasonable tolerances in speed, position, and time to account for measurement uncertainty and communication latency.

Overtake Intention Flag

A vehicle may include an **Overtake Intention Flag (OIF)** in its Motion Status data when its on-board system is actively evaluating or preparing to initiate an overtaking manoeuvre.

This flag does **not** indicate that the manoeuvre has already started, but that the vehicle is in a decision or pre-manoeuvre phase that could soon alter its trajectory and lane occupancy.

Because this introduces higher uncertainty into traffic predictions, receiving vehicles must apply additional logic when processing messages from vehicles carrying this flag.

Required Handling of Vehicles with Overtake Intention Flag

Case 1 — Same Direction, Behind the Host Vehicle

If the vehicle carrying the Overtake Intention Flag is:

- Traveling in the same direction
- Located behind the host vehicle

Then:

Its intention does not affect the host vehicle's overtaking feasibility calculation and may be ignored for this specific manoeuvre analysis.

Case 2 — Same Direction, Ahead of the Host Vehicle

If the flagged vehicle is:

- Traveling in the same direction
- Located ahead of the host vehicle

Then additional uncertainty is introduced because that vehicle may:

- Initiate an overtake before or during the host vehicle's manoeuvre
- Change lanes unexpectedly
- Reduce available re-entry space after passing

In this situation, the host vehicle should:

- Increase required safety margins, **or**
- Temporarily defer issuing a "safe to overtake" indication until the flagged vehicle's behaviour becomes clearer

The system must avoid assuming that the vehicle ahead will maintain its current lane and spacing.

Case 3 — Opposite Direction Vehicle with Overtake Intention Flag

If a vehicle traveling in the opposite direction carries the Overtake Intention Flag:

It may soon occupy the host vehicle's lane while overtaking another vehicle. However, its future trajectory, timing, and required distance are uncertain.

Therefore:

- The host vehicle must **not** treat this as a simple opposing vehicle in its lane
- The system must assume **increased uncertainty in lane occupancy ahead**

Even if a theoretical time gap appears sufficient, the host vehicle should:

Defer or deny overtaking recommendations unless a large safety margin exists that remains valid even if the opposing vehicle begins and completes its own overtake.

🔒 Design Principle Introduced by This Flag

The Overtake Intention Flag signals:

"My future lane position is less predictable than usual."

Therefore, it should **never make overtaking appear safer**, only:

- Maintain current risk level, or
- Increase required safety margins, or
- Force temporary deferral of a recommendation

Transmission rates

Two vehicles driving at opposite directions at a speed of 100 km/h targets an apparent speed of 200 km/h (between each other) or 55 m/s. This means in only 1 second, there would be 55 meters less to manoeuvre. With an update at a rate of 10 Hz (10 transmission in 1 second), the difference would be reduced to 5.5 meters.

The update rate must be high enough to ensure that the spatial error introduced by motion between successive transmissions remains small relative to required safety margins. At highway closing speeds, this requires sub-second updates, typically on the order of 10 Hz for dynamic motion parameters.

Baseline transmission rate: 10 Hz for dynamic state.

Vehicles may reduce the rate under channel congestion, but not below 2 Hz while moving above 40 km/h.

T1 messages will be sent with a rate of 1Hz while T2 should be transmitted with a 10Hz frequency.

Cooperative Motion Message Structure

There are 4 main type of CMM types. The type of message will be defined with 5 bits.

Common definitions of motion variables

Length class

Class	Length Range	Typical Vehicles
0	< 2.5 m	Motorcycle
1	2.5 – 4.5 m	Small/medium cars
2	4.5 – 5.5 m	Large cars / SUVs / pickups
3	5.5 – 8 m	Vans / small trucks
4	8 – 12 m	Rigid trucks / small buses
5	12 – 18 m	Large trucks / coaches
6	18 – 25 m	Semi-trailers / articulated trucks
7	> 25 m	Extra-long or special combinations
8	6-8 m	Ambulance: Emergency medical vehicle
9	4.5-5.5 m	Police: Law enforcement vehicle
10	7-12 m	Fire: Firefighting vehicle.

Emergency vehicles such as ambulances, police units, and fire brigades present unique operational characteristics that differ from regular traffic.

These vehicles may:

- Accelerate unpredictably
- Exceed normal speed limits
- Travel against traffic flow
- Require immediate right-of-way

To support safe interaction with emergency services, this protocol defines dedicated vehicle classes and an emergency state flag.

Emergency Vehicle Handling

Emergency vehicles such as ambulances, police units, and fire brigades present inherently unpredictable motion characteristics compared to regular traffic.

Even when not actively responding to an emergency, these vehicles may:

- Accelerate suddenly
- Change speed unpredictably
- Initiate urgent manoeuvres without prior indication

For this reason, **additional safety margins shall always be applied when calculating overtake feasibility involving emergency-class vehicles**, regardless of their emergency state flag.

This requirement applies to:

- Emergency vehicles ahead in the same direction
- Emergency vehicles approaching in the opposite direction

Suggested minimum margins when emergency vehicle detected:

- Increase assumed acceleration uncertainty by +2 m/s^2
- Increase speed variation tolerance: +15 m/s
- Increase minimum safety gap distance: +50%

These increased margins ensure that a manoeuvre assessed as safe remains safe even if the emergency vehicle changes behaviour unexpectedly during the overtake.

Emergency warnings shall take priority over overtake recommendations in the driver interface.

Emergency vehicles shall use TEMPID identifiers under the same privacy rules as other vehicles.

The **EmergencyFlag** shall be used to signal operational status.

Unit's specification

For simpler use, all the distances should be sent in meters. In addition, all the speeds should be sent in meters per second.

Direction (or heading)

It will be encoded with 9 bits. These will represent the angle between the geographic North (0º) and the direction of the vehicle being positive in the clockwise direction.

Speed

The speed is encoded with 7 bits. This allows a maximum speed that can be transmitted to 128 (m/s) equivalent to 460 km/h with a resolution of 1 m/s. This is the magnitude itself. The vector of the speed is already defined with the direction/heading.

Acceleration estimate

Definition

The acceleration estimate represents the longitudinal acceleration of the transmitting vehicle along its direction of travel.

Computation

The value may be directly measured by the vehicle or estimated using the difference between the last two transmitted T2 messages (based on speed variation over time).

Priority

Its importance is lower than speed and position and should be treated as an auxiliary kinematic hint rather than a primary safety variable.

Encoding

Property	**Value**
Type	Signed integer
Size	8 bits
Range	−32 to +31.75 m/s²
Resolution	0.25 m/s² per bit
Encoding	Two's complement

Interpretation

- **0** → Constant speed
- **Positive values** → Acceleration
- **Negative values** → Braking
- Values outside physically realistic vehicle limits may be ignored by receivers

Rationale

An 8-bit signed field with 0.25 m/s² resolution provides more than enough dynamic range for real road vehicles while keeping the message compact. Typical passenger vehicle acceleration rarely exceeds ±6 m/s², so this scale allows detection of both gentle and aggressive manoeuvres.

Latitude and Longitude

Latitude and longitude shall be encoded in **fixed-point decimal degrees**.

Format:

- 32-bit signed integer
- Resolution: **1e-7 degrees**
- Range: ±90° latitude, ±180° longitude

This format:

- Allows direct conversion to meters
- Is computationally efficient
- Is widely used in existing V2V standards

Degrees–minutes–seconds encoding shall not be used in the binary protocol.

Position Confidence Indicator

Definition

This field represents the estimated **1-sigma horizontal position uncertainty** of the transmitting vehicle at the time of message generation.

It reflects the quality of the **fused positioning solution** used by the on-board system (GNSS, inertial sensors, wheel odometry, map matching, or other sensors), rather than raw GNSS accuracy alone.

The value is encoded as a **3-bit index** representing discrete uncertainty ranges.

Encoding

Value	Horizontal Uncertainty (± meters)	Interpretation
0	≤ 0.5 m	Very high confidence (sensor fusion + map matching)
1	≤ 1 m	High confidence
2	≤ 2 m	Good confidence
3	≤ 5 m	Moderate confidence
4	≤ 10 m	Low confidence
5	≤ 20 m	Very low confidence
6	> 20 m	Unreliable position
7	Position degraded or fallback mode (e.g., dead reckoning only, GNSS lost)	

Usage Rules

- This indicator **does not prevent transmission** of the position, but informs receivers about how much trust should be placed in it.
- Receivers **may expand safety margins** proportionally to the reported uncertainty.
- Value **7** should be used when the positioning system is operating in a degraded mode where uncertainty cannot be reliably bounded.
- If the field is unavailable, devices shall default to **value 6 (Unreliable)**.

Rationale

Using discrete confidence levels instead of a floating-point accuracy value:

- Keeps the message compact
- Avoids false precision
- Allows heterogeneous sensor stacks to report quality consistently
- Enables receivers to adapt overtake and collision models conservatively

CMM-T1 — Vehicle Presentation Message (Low Rate)

Transmission rate: ~1 Hz.

Purpose: Provide static or rarely changing vehicle information to nearby participants that have not yet received it.

This message acts as a **vehicle descriptor**, not a motion update.

Typical fields:

- Temporary Anonymous Vehicle ID
- Vehicle Length Class
- Vehicle Width Class
- Vehicle Type (car, truck, bus, motorcycle, etc.)

- System capability flags (supports relay, supports perception sharing, in emergency state, etc.)

This message is **not required for real-time motion prediction** and therefore can tolerate low frequency.

Vehicles that already know this information may ignore repeated copies unless the ID changes (rotation event).

Emergency State Flag

EmergencyFlag (1 bit)

Purpose:

The EmergencyFlag indicates that the vehicle is actively responding to an emergency.

When EmergencyFlag is set:

Receiving vehicles should:

- Provide a clear visual indication to the driver in its display.
- Display direction and relative position.
- Assist drivers in yielding appropriately.

The EmergencyFlag is intended for driver awareness and cooperation, and shall not be used as the sole basis for safety margin calculations.

Safety margins are determined by vehicle class, not by the emergency flag state.

CMM-T2 — Dynamic Motion Message (High Rate)

Transmission rate: ~10 Hz (adaptive under congestion).

Purpose: Provide real-time kinematic data required for safety-critical calculations.

This message contains the "live" state used in overtaking feasibility analysis.

Typical fields:

- Temporary Anonymous Vehicle ID
- Timestamp
- Position

- Velocity vector
- Acceleration estimate
- Heading
- Position confidence
- Motion Status Flags (braking, accelerating, turn signal, **Overtake Intention**)

This message must be optimized for low latency and minimal size.

CMM-T3 — Cooperative Intent & Coordination Message

In addition to periodic awareness messages (T1 and T2), the protocol defines a **Type 3 message (CMM-T3)** intended for **event-driven cooperative coordination** between vehicles involved in a specific traffic situation.

Unlike T1 and T2 (pure broadcast), T3 messages are **targeted but may propagate through nearby vehicles** to reach recipients that are not in direct line of sight.

T3 Message Structure

Field	Size	Description
Sender ID	same as CMM ID size	Temporary anonymous ID of sender
Recipient ID	same size	Target vehicle ID
Message Type	1 byte	Defines semantic meaning
Payload Length	1 byte	0–255 bytes
Payload	variable	Message-specific data
TTL (Hop Limit)	1 byte	Maximum number of relay hops

🔁 TTL and Controlled Retransmission

CMM-T3 messages are **not global broadcasts**. They use a **small Time-To-Live (TTL)** value to allow short-range multi-hop propagation.

Recommended default: TTL = 2 hops

This allows the message to:

- Reach vehicles hidden by hills, curves, or traffic queues
- Propagate one intermediate relay beyond direct radio range

But prevents:

- Long-distance flooding
- Network congestion
- Irrelevant vehicles receiving manoeuvre-specific data

Retransmission Rules

A vehicle that receives a CMM-T3 and is **not the final recipient** must:

1. Decrease TTL by 1
2. Retransmit only if TTL > 0
3. Avoid retransmitting duplicate messages (based on Sender ID + message sequence identifier)

This ensures reliability in non-line-of-sight situations while keeping the message geographically local.

◆ Type 0 — Identification Request

Purpose: Resolve missing vehicle classification data needed for safety calculations.

Payload length: 0

Use case:

A vehicle evaluating an overtaking manoeuvre lacks static data (e.g., length class) for another vehicle and cannot complete its safety model.

It sends a **Type 0 request** to that vehicle.

Because TTL > 1, the message can reach the recipient even if direct communication is blocked by terrain or other vehicles.

Upon receiving it, the target vehicle responds with a **CMM-T1** message to provide its classification data.

◆ Type 1 — Overtake in Progress Notification

Purpose: Inform nearby vehicles that the sender has already initiated an overtaking manoeuvre.

Recipients may include:

- Vehicles ahead in the same direction
- Vehicles in the opposite direction within the predicted conflict zone

Because of the limited TTL-based relay, this warning can reach vehicles beyond line of sight (e.g., just beyond a hill crest).

Intent of the message

This message is **advisory, not authoritative**. It is meant to:

- Increase attention in oncoming vehicles
- Discourage nearby vehicles from accelerating unexpectedly
- Discourage other vehicles from initiating simultaneous overtakes

User interface behaviour is manufacturer-defined.

⚠ Critical Safety Constraint for Type 1

To avoid unsafe coupling between automated decisions:

A Type 1 message must never cause another vehicle to assume the manoeuvre is safe or to reduce its own safety margins.

It may only:

- Increase caution
- Trigger driver alerts
- Increase internal uncertainty in trajectory prediction models

---

🌐 Future Extensibility

With 1 byte for message type and 1 byte for payload length:

- Up to **256 message categories**
- Each with up to **255 bytes of payload**

The TTL field ensures future coordination messages can remain **locally relevant** without overloading the network.

Role of T3 in the Protocol Stack

Layer	Role
T1	Static vehicle description
T2	Real-time motion state
T3	Short-range cooperative intent and coordination

T3 adds a **human-like signaling layer** to the system, allowing vehicles to communicate intent while preserving autonomy and safety independence.

🔁 Relationship Between CMM-T1 and CMM-T2

CMM-T1 introduces the vehicle.
CMM-T2 keeps everyone updated about how it is moving.

If a CMM-T2 is received from an **ANONID**:

- The receiving vehicle may temporarily operate using default assumptions
- It should expect a CMM-T1 to arrive later with full classification data

⛰ T3 Message Expiration

In addition to TTL-based hop limitation, T3 messages must include time-based validity.

A T3 message shall be considered expired and must not be retransmitted if:

- More than **5 seconds** have elapsed since its timestamp, or
- The event described is no longer relevant according to local perception and motion evolution

This prevents outdated manoeuvre coordination data from persisting in the network.

CMM-T4 — NCOR objects

Purpose

CMM-T4 messages are used to report the presence and motion of **non-cooperative road users** detected through onboard perception systems such as radar, cameras, or LIDAR.

These objects represent vehicles or obstacles that **do not transmit V2V messages**, either because they lack compatible equipment or are temporarily unable to communicate.

Nature of the Message

An NCOR message is a **state report**, similar in nature to a T2 dynamic state message, but with key differences:

- It represents a **perceived external object**, not the transmitting vehicle itself
- It does **not contain a TempID**, since the object is unknown to the system
- Its data originates from **sensor perception**, not self-reported vehicle telemetry

Because there is no associated T1 message for NCOR objects, all relevant motion and positioning data must be included directly within the T4 message.

Role in the System

NCOR messages allow cooperative vehicles to:

- Be aware of traffic participants that lack V2V capability.
- Maintain safer models of surrounding traffic in mixed-technology environments.
- Bridge perception gaps in curves, hills, or visual obstructions through multi-hop propagation.

However, NCOR data is considered **lower confidence** than cooperative T1/T2 data and is subject to replacement and suppression rules defined in the **NCOR Update and Suppression Rules** section.

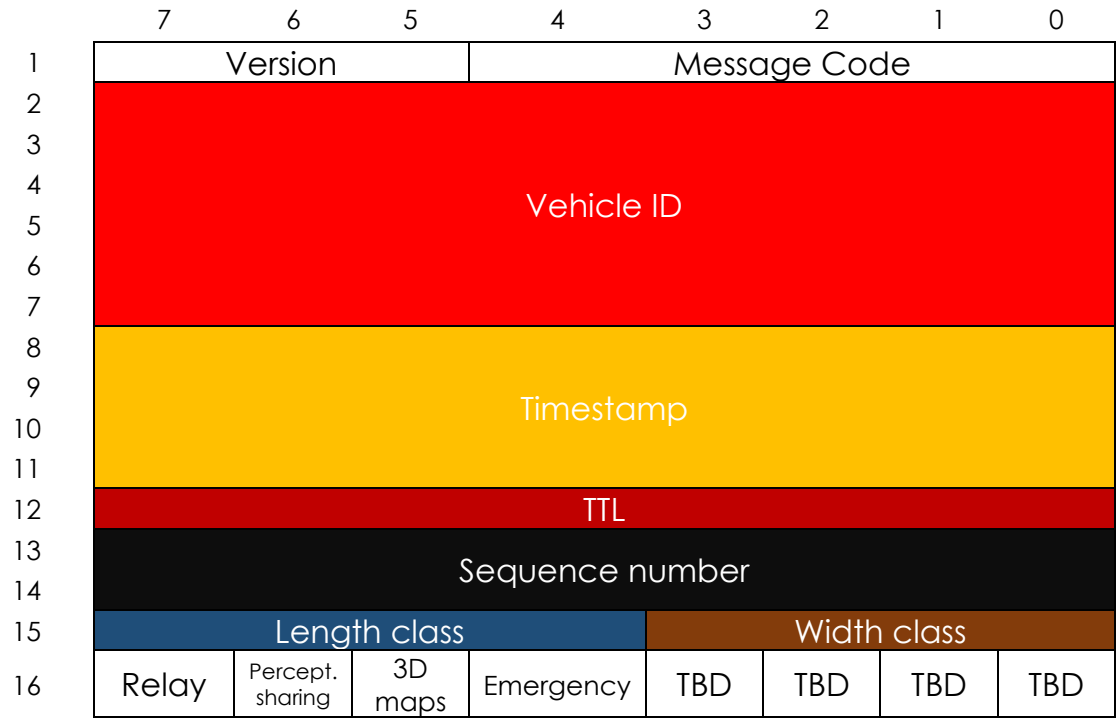
Priority Principle

Whenever a real vehicle begins transmitting cooperative messages (T1/T2), any NCOR messages referring to the same physical object shall be considered **secondary** and handled according to the NCOR suppression logic.

CCM - Structures

CCM – T1

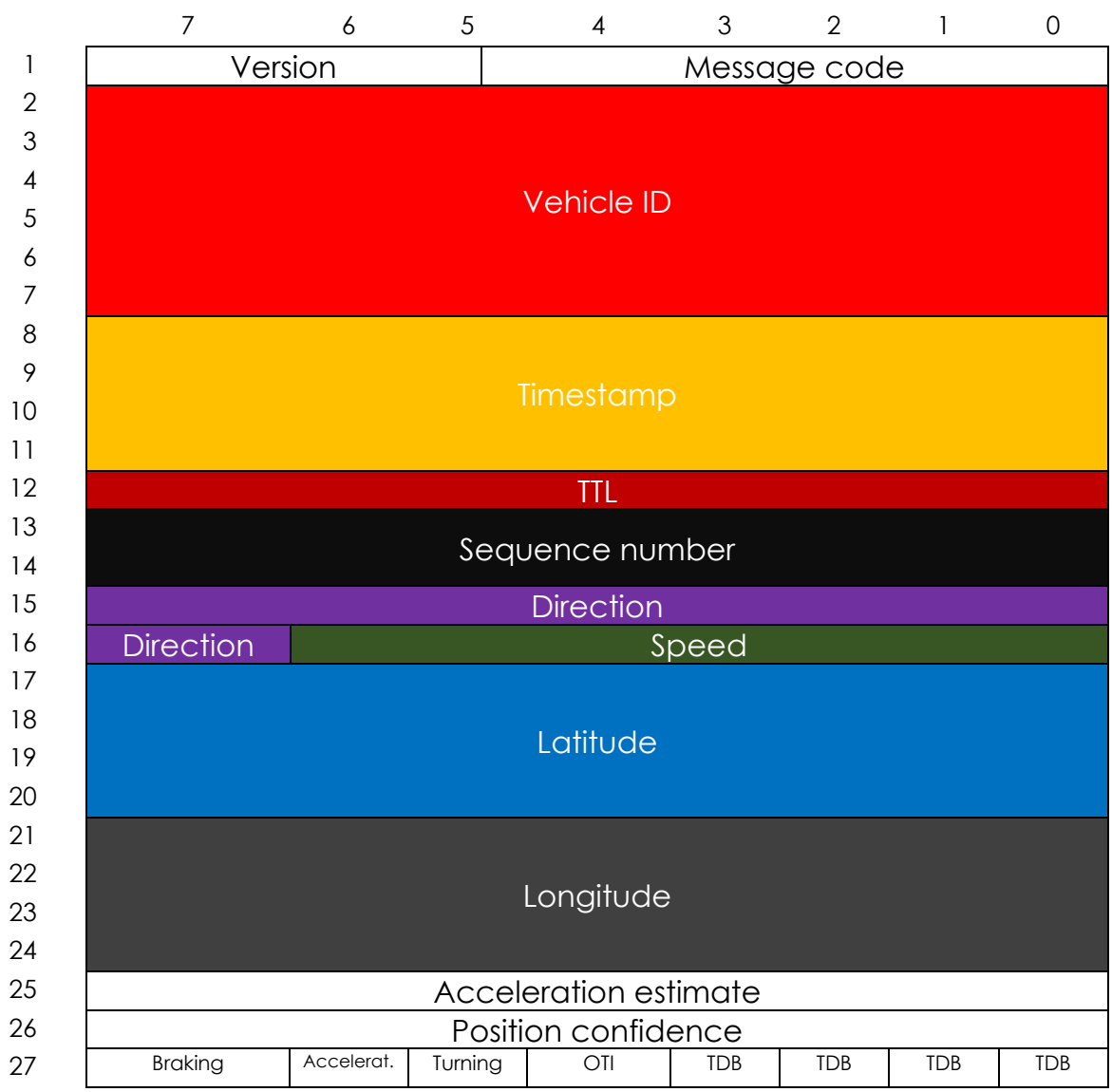
The message code would be 1. The rest of the structure is defined in the next table.



1. 3 bits for the version, 5 bits for the message code. In this case value = 1.
2-7. 6 bytes for Vehicle ID
8-11. Timestamp
12. TTL
13-14. Sequence number.
15. 4 bits for length class, 4 bits for width class (TBD).
16. Flags byte: Supports relay, Supports perception sharing, has 3D maps, Emergency state (0 = normal operation, 1 = emergency response mode), etc.

CCM – T2

The message code would be 2. The rest of the structure is defined in the next table.

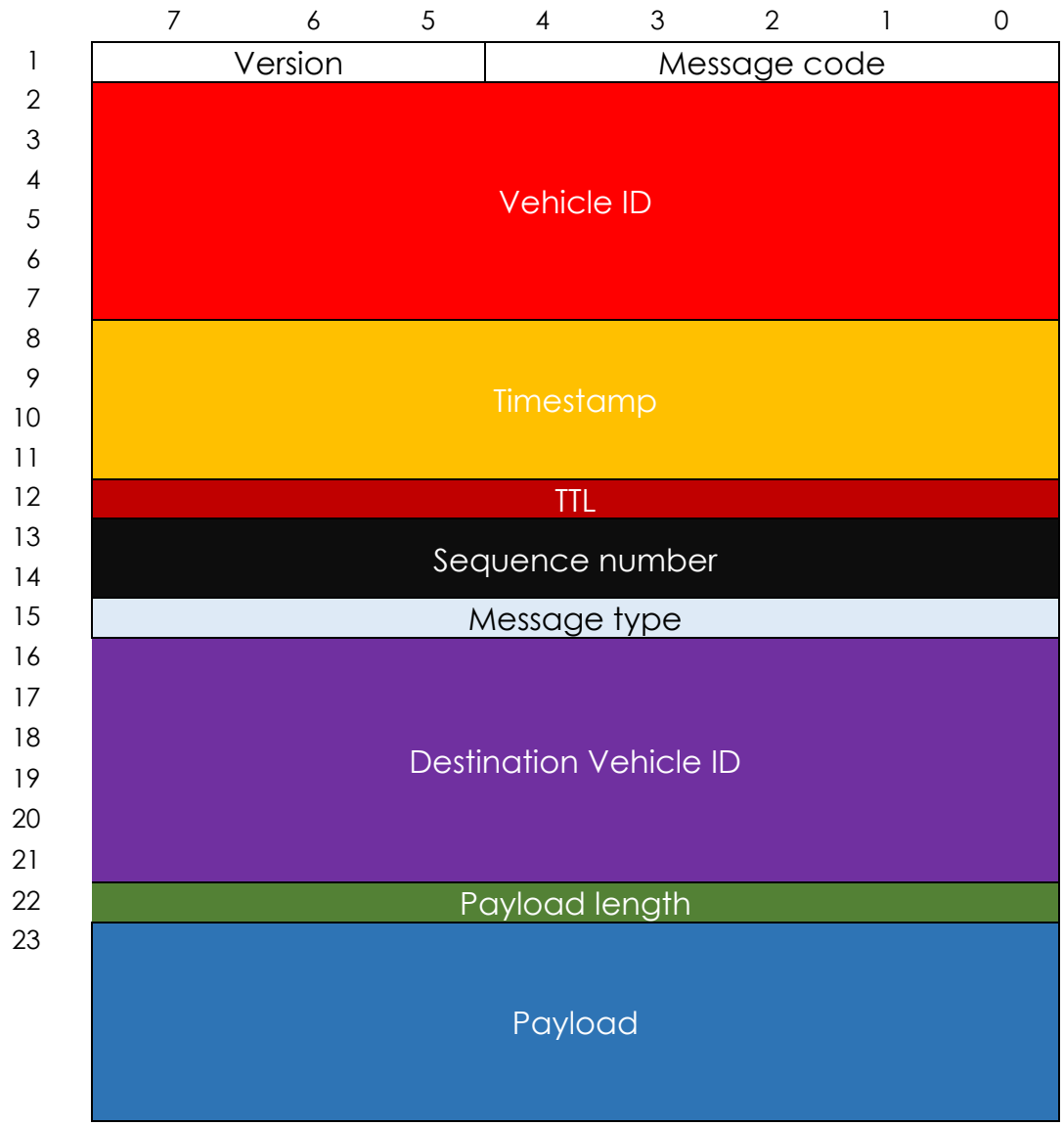


1. 3 bits for the version, 5 bits for the message code. In In this case value = 2.
2-7. 6 bytes for Vehicle ID
8-11. Timestamp
12. TTL
13-14. Sequence number.
15. 8 most significant bits for direction.
16. 1 less significant bit for direction, 7 bit for speed.
17-20. Latitude
21-24. Latitude.
25. Acceleration estimate

26. Position confidence.
27. Motion flags: Braking, Accelerating, turn signal, overtake intention, etc.

CCM – T3

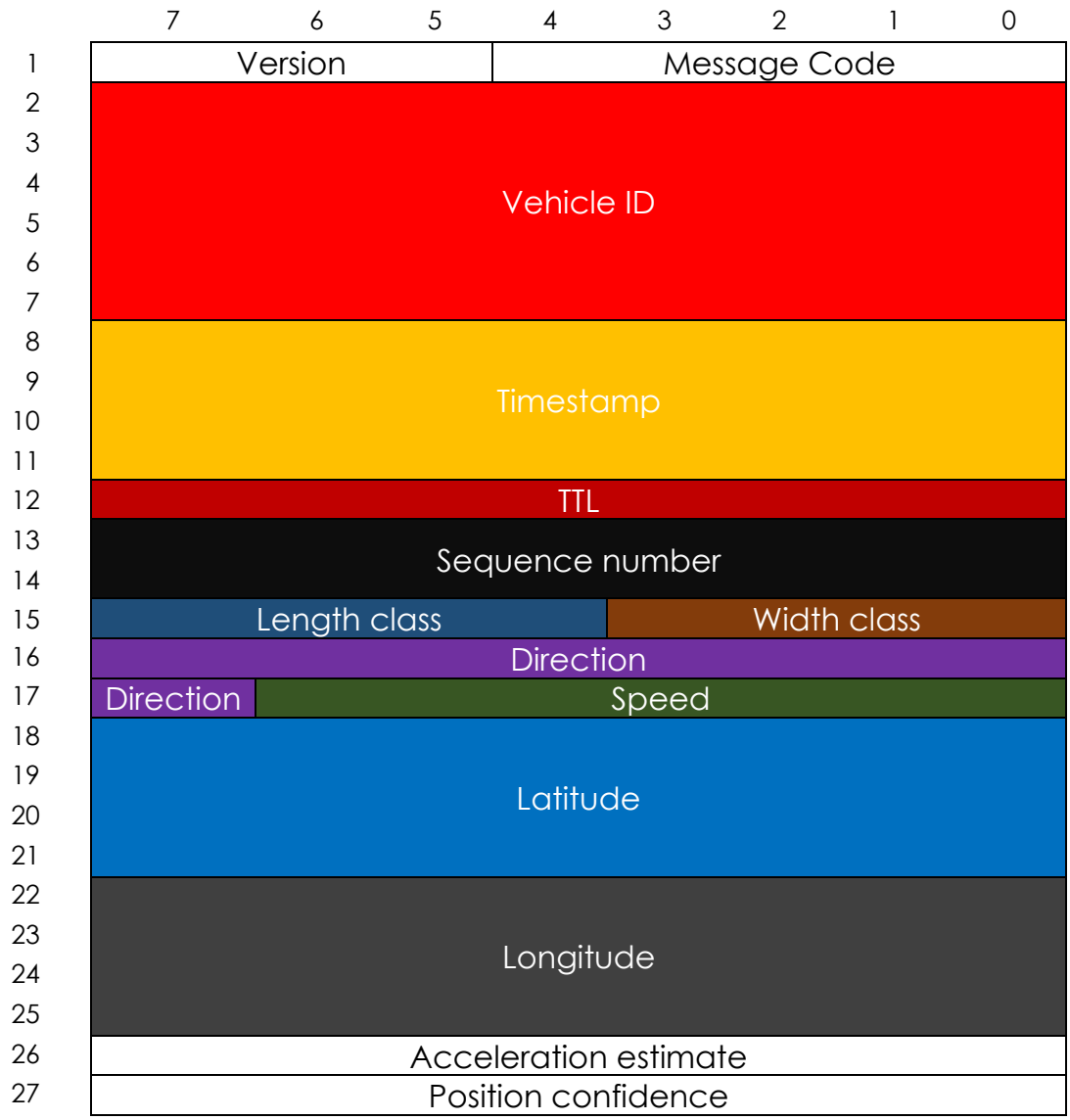
The message code would be 3. The rest of the structure is defined in the next table.



1. 3 bits for the version, 5 bits for the message code. In In this case value = 3.
2-7. 6 bytes for Vehicle ID
8-11. Timestamp
12. TTL
13-14. Sequence number.
15. Message type
16-21. Destination Vehicle ID
22. Payload length
23-N: Payload (if present)

CCM – T4 --- NCOR

The message code would be 4. The rest of the structure is defined in the next table.



1. 3 bits for the version, 5 bits for the message code. In this case value = 1.
2-7. 6 bytes for Vehicle ID
8-11. Timestamp
12. TTL
13-14. Sequence number.
15. 4 bits for length class, 4 bits for width class (TBD).
16. 8 most significant bits for direction.
17. 1 less significant bit for direction, 7 bit for speed.
18-21. Latitude
22-25. Latitude.

26. Acceleration estimate
27 Position confidence.

Use of Timestamp and Position Confidence in Safety-Critical Calculations

Purpose

Vehicle motion data is inherently uncertain due to:

- GNSS positioning errors
- Sensor fusion limitations
- Communication latency
- Packet loss and retransmission delays

To ensure conservative and interoperable behavior, receivers shall consider both **data age** and **position uncertainty** when performing safety-related evaluations such as overtake feasibility or collision risk.

This protocol does **not** impose a specific physical model, but defines how uncertainty information must be interpreted.

Effective Position Uncertainty

When processing the state of another vehicle, the receiver shall treat the reported position as uncertain within a confidence radius composed of two parts:

```
Effective_Uncertainty = Position_Confidence_Radius + Motion_Uncertainty
```

Where:

1. Position Confidence Radius
Derived directly from the **Position Confidence Indicator** field.

2. Motion Uncertainty
Accounts for possible displacement due to message age:

```
Motion_Uncertainty = Relative_Speed × Data_Age
```

Where:

- **Relative_Speed** is the absolute speed difference between vehicles (or a conservative upper bound if unknown)
- **Data_Age = Current_GNSS_Time – Timestamp**

Interpretation

Receivers shall treat the remote vehicle as occupying **any position within the Effective Uncertainty region**, not just the nominal coordinates.

This effectively expands the vehicle's physical envelope, producing conservative safety margins.

Safety Margin Adaptation

Manufacturers may incorporate Effective Uncertainty into their own models by:

- Increasing minimum safe passing distances
- Expanding predicted collision envelopes
- Reducing allowed maneuver aggressiveness
- Delaying "safe overtake" indications

The protocol does not mandate how this is done, only that uncertainty must not be ignored.

Degraded Data Handling

If:

- Position Confidence indicates **Unreliable (6)**, or
- Timestamp age exceeds the validity threshold but the packet is still within relay limits,

receivers should treat the vehicle as **high-risk** and may:

- Prohibit overtake assistance
- Increase warning sensitivity
- Require additional confirmation before approving maneuvers

Rationale

Two vehicles with identical nominal positions can have very different risk profiles depending on:

- Sensor quality

- Message latency
- Communication conditions

By explicitly modeling uncertainty growth over time, this protocol ensures that safety decisions remain conservative without requiring a centralized or standardized motion prediction algorithm.

Feasibility Analysis — Communication Load and Network Impact

One potential concern when introducing a cooperative Vehicle-to-Vehicle safety protocol is the assumption that continuous motion data exchange between vehicles could saturate the wireless channel, especially in dense traffic environments. For this reason, a quantitative feasibility analysis is essential before drawing conclusions about scalability.

Baseline Transmission Model

Under normal operating conditions, each equipped vehicle transmits:

Message Type	Purpose	Nominal Rate	Typical Size (bytes)
T1	Static vehicle info	1 Hz	~20 B
T2	Dynamic motion state	10 Hz	~28 B
T3	Event-driven coordination	Rare	~20–40 B
T4 (NCOR)	Non-cooperative objects	Situational	~28 B

The dominant contributor is **T2**, used for real-time motion awareness.

Per-Vehicle Data Rate

Assuming:

- T1 = 20 B × 1 Hz = **20 B/s**
- T2 = 28 B × 10 Hz = **280 B/s**

Baseline broadcast load per vehicle:

≈ 300 bytes per second
≈ **2.4 kbit/s**

Even when adding protocol overhead (headers, MAC layer, security encapsulation), a conservative estimate of **5 kbit/s per vehicle** remains realistic.

Dense Traffic Scenario

Consider a worst-case scenario of **100 equipped vehicles** within mutual communication range — a very dense highway cluster.

Total raw cooperative data:

100 vehicles × 5 kbit/s ≈ **500 kbit/s**

Modern V2V technologies such as IEEE 802.11p / ITS-G5 or C-V2X sidelink are designed to handle **multi-megabit per second** channel capacities under congestion control schemes.

Even before adaptive rate reduction mechanisms defined in this protocol are applied, the estimated load remains **well below 10% of typical channel capacity**.

Congestion Control Mechanisms

The protocol already incorporates safeguards to prevent overload:

- T2 rate reduction down to 2 Hz under congestion
- Relay suppression before self-message suppression
- Spatial relevance filtering (1.5 km ahead / 1 km behind)
- TTL-limited multi-hop propagation
- Expiration of stale data

Under congestion, per-vehicle load may drop below **1.5 kbit/s**, further reducing channel utilization.

Comparison with Everyday Data Usage

For perspective:

System	Typical Data Rate
Music streaming (low quality)	96 kbit/s
Voice call (VoIP)	24–40 kbit/s
This protocol (dense scenario)	~5 kbit/s per vehicle

A single streaming user consumes more bandwidth than **15–20 cooperative vehicles**.

Extreme Stress Scenario (Upper-Bound Analysis)

To address concerns about theoretical worst-case congestion, an intentionally pessimistic scenario is evaluated below. This scenario does not represent typical road behavior but serves as an upper-bound stress test.

Assumptions

Parameter	Value	Notes
Vehicles in communication range	200	Extremely dense, multi-lane cluster
Protocol adoption rate	90%	Near-universal penetration
Active T2 transmitters	180 vehicles	Almost all moving vehicles
T2 transmission rate	10 Hz	No rate reduction yet
Average effective packet size	60 bytes	Includes PHY/MAC/security overhead
Relay factor	2x	Some packets relayed once

Channel Load

180 vehicles × 10 msg/s × 60 bytes × 2
= **216,000 bytes/s ≈ 1.7 Mbps**

Super-Extreme Stress Scenario (Upper-Bound Analysis)

Considering 300 vehicles on each direction:

Assumptions

Parameter	Value	Notes
Vehicles in communication range	600	Extremely dense, multi-lane cluster
Protocol adoption rate	90%	Near-universal penetration
Active T2 transmitters	540 vehicles	Almost all moving vehicles
T2 transmission rate	10 Hz	No rate reduction yet
Average effective packet size	60 bytes	Includes PHY/MAC/security overhead
Relay factor	2x	Some packets relayed once

Channel Load

540 vehicles × 10 msg/s × 60 bytes × 2
= **648,000 bytes/s ≈ 5.1 Mbps**

Even under this exaggerated scenario, channel load remains within the operational envelope of ITS-G5 / C-V2X systems, which typically sustain several megabits per second even under congestion control regimes.

Once congestion control mechanisms activate (rate reduction, suppression rules, spatial filtering), effective load would drop significantly below this value.

Interpretation

This stress test shows that even when assuming:

- Very high vehicle density
- Near-total adoption
- Maximum transmission rate
- Additional relay traffic

the protocol still operates within the capacity range of modern V2V communication systems.

Conclusion of Feasibility

Even in pessimistic high-density scenarios, the proposed protocol represents a **small fraction of the capacity of modern V2V communication channels**. When congestion control and spatial filtering are active, network impact becomes even smaller.

Therefore, concerns about **systematic channel saturation are not supported by quantitative analysis**, and should not be used as a basis to dismiss feasibility without measurement.

Appendix

Human-Machine Interface Considerations

Despite this protocol is not intended to define either the user-interface or the user-experience, there are a few considerations that I think would be nice-to-have or, in some cases, quite indispensable.

Implementation Recommendation — Latencies

When performing overtake feasibility calculations, implementations should account for realistic system, vehicle, and human response times.

There may be a short delay between the completion of the calculation and the moment the result is presented to the driver. In addition, drivers typically require time to read, understand, and decide whether to act on the recommendation. Finally, the vehicle itself may need additional time to reach the target speed assumed in the calculation, particularly under adverse conditions such as headwinds, road gradients, or suboptimal gear selection.

For these reasons, it is strongly recommended that implementations apply conservative margins when estimating timing, distances, and required speed profiles. Incorporating these real-world delays helps ensure that a manoeuvre assessed as safe under ideal assumptions remains safe under practical driving conditions.

Manufacturers remain free to define the latency assumptions used in their systems, but adopting conservative estimates will generally lead to safer outcomes for all road users.

Implementation Recommendation — Driver Feedback

When the system determines that an overtake manoeuvre is safe under current conditions, the driver should be informed using a clear and contextual message such as:

"Safe to overtake # preceding vehicle(s) at XXX km/h"

A secondary line or subtitle should also be displayed:

"Before # oncoming vehicle(s) approach"

Where:

- **# preceding vehicle(s)** indicates how many vehicles ahead were included in the overtake feasibility calculation
- **XXX** represents the speed assumed by the onboard system
- **# oncoming vehicle(s)** indicates how many approaching vehicles were considered in the available gap

Notifying the assumed speed is essential. The feasibility of the overtake is calculated based on a specific speed profile, and if the driver is unwilling or unable to reach that speed, the manoeuvre may no longer be safe. Omitting this information could increase the likelihood of an unnecessary and potentially hazardous aborted overtake.

This information provides transparency about the assumptions behind the calculation. If the driver observes more vehicles ahead than those included in the calculation, and no visible gap exists between them, the driver can infer that the system may be operating with incomplete situational awareness.

If a visible gap does exist, the system may still be operating with complete information but may have calculated that an earlier re-entry point is required (see ***"Re-entry Context Communication"*** recommendation).

Similarly, if zero oncoming vehicles are shown while visibility of the opposite lane is limited, the driver should understand that the system's knowledge of approaching traffic may be partial.

Providing this context reduces the risk of overreliance on the system and helps drivers make better-informed decisions, especially in environments where not all vehicles are cooperative or detectable.

Manufacturers remain free to adapt wording and interface design, but the system should clearly communicate both the required speed and the traffic scenario used in the safety assessment.

Implementation Recommendation — Information Completeness Awareness

Overtake assistance systems should acknowledge that traffic perception may be incomplete due to:

- Non-cooperative vehicles
- Occlusions caused by terrain or curves
- Limited sensor range
- Temporary communication gaps

Therefore, when presenting overtake advisories, the system should provide an indication of the **information coverage level** used in the calculation.

This may be communicated through a short secondary message such as:

- "Based on cooperative data only"
- "Limited visibility ahead"
- "Oncoming traffic partially unknown"

The goal is not to guarantee that all relevant vehicles were detected, but to avoid conveying a false sense of total awareness. Drivers should understand that the recommendation is based on the **best available data**, not complete certainty.

Manufacturers may choose how to represent this concept visually or textually, but the system should never imply full knowledge of traffic conditions beyond its sensing and communication capabilities.

Implementation Recommendation — Automatic Overtake Detection

The on-board system should continuously monitor vehicle dynamics and surrounding traffic conditions to detect the likely initiation of an overtake manoeuvre.

This monitoring should apply both:

- After the system has explicitly indicated that an overtake is safe, and
- When the driver begins an overtake without prior system assistance

If the on-board system detects that the vehicle is accelerating and moving to pass a preceding vehicle (for example, by observing increasing relative speed and lateral displacement consistent with a lane change), it may infer that an overtake manoeuvre is underway.

In such cases, the device should proactively transmit a **T3-1 (Overtake in Progress)** message to relevant nearby vehicles, even if the manoeuvre was not initiated following a prior "safe to overtake" advisory.

This ensures that other cooperative vehicles are informed of the developing manoeuvre and can avoid actions that would reduce the available safety margin, such as accelerating, initiating another overtake, or reducing headway.

Manufacturers remain free to define the internal detection logic and thresholds, but the objective should be to notify surrounding vehicles as early as reasonably possible once an overtake manoeuvre becomes likely.

This proactive evaluation does not imply encouragement of the manoeuvre; it only ensures that safety assessment is available at the earliest possible moment.

Implementation Recommendation — Use of Map and Road Geometry

Overtake feasibility calculations should not rely solely on real-time vehicle data. The onboard system should also incorporate **digital map information and road geometry** into the decision process.

An overtake that would end within a **curve, hill crest, or limited-visibility segment** is inherently high risk. In many countries, such manoeuvres are also legally prohibited. Even if cooperative vehicle data suggests sufficient space, a non-cooperative vehicle may be approaching from the opposite direction but remain undetected due to:

- Lack of V2V capability
- Absence of nearby vehicles capable of relaying information
- Occlusion caused by terrain, curves, or elevation changes

Therefore, the system should avoid recommending a safe overtake if the predicted manoeuvre would:

- Begin within a no-overtaking zone indicated by road markings or map data
- End within or beyond a visibility-restricted area such as a curve or hill crest
- Depend on line-of-sight conditions that cannot be guaranteed through cooperative data alone

Digital map attributes such as road curvature, slope, elevation profile, and overtaking restrictions should be used to apply conservative constraints to the overtake evaluation.

Manufacturers may choose how to integrate map data and perception systems, but the overtake assistance logic should never assume full traffic visibility beyond geometric or legal road limitations.

Implementation Recommendation — Re-entry Context Communication

When the calculated overtake manoeuvre does not involve passing all visible preceding vehicles, the driver interface should communicate the intended **safe re-entry position** rather than only the number of vehicles included in the overtake calculation.

The goal is to align the system's message with the manoeuvre outcome the driver will observe, avoiding confusion when additional vehicles are present beyond the re-entry gap.

Possible examples include:

- "Safe re-entry position available ahead"
- "Rejoin lane before next vehicle"

This approach reduces cognitive load and prevents misinterpretation that the system has failed to detect all visible vehicles.