Safer Crossways using I2V

Public report

Project within Traffic-safe automation – FFI, DNR 2024-00815

Authors Abhilash Balan, Nithin Puravankara, Sudha Padmanabhan,
Sumesh Pushpangadan, Danilo Chinchilla, Sara Dalvig, Maria Ulan

Date 2025-03-05

FFI Fordonsstrategisk Forskning och Innovation

Content

FFI in short

FFI, Strategic Vehicle Research and Innovation, is a joint program between the state and the automotive industry running since 2009. FFI promotes and finances research and innovation to sustainable road transport.

For more information: www.ffisweden.se

1. Summary

Although overall road fatalities in Sweden have decreased, this reduction has not translated to Vulnerable Road Users (VRUs) in the past five years, highlighting the urgent need for better safety solutions, particularly for VRUs. In this context, we have focused on the need for open and interoperable infrastructure and its potential to drive scalable and cost effective solutions. This pre-study investigated the feasibility of an open architecture for Road Side Units (RSUs), a main component of Infrastructure-to-Vehicle (I2V) communication, aiming to enhance road safety in a secure and cost-effective way.

The pre-study explored the following research questions:

- Are there technical barriers to developing an open architecture for RSUs?
- What are the technical minimum requirements to achieve an open architecture for an RSU?
- Is an RSU with an open architecture relevant to stakeholders?

The findings, while detailed and multifaceted, generally support the feasibility and potential benefits of creating this open architecture.

The study employed a structured approach to assess the feasibility of an open RSU platform. Three work packages (WPs) were executed to evaluate different aspects of the I2V communication infrastructure. WP2 focused on analyzing sensing systems by testing radar and camera-based Detection Units (DUs) and assessing the transmission of metadata to alert mechanisms. WP3 investigated I2V/Vehicle-to-Everything (V2X) messaging standards, specifically examining the suitability of Collective Perception Messages (CPMs) and VRU Awareness Messages (VAMs) for VRU protection and their role in improving situational awareness. WP4 investigated the legal and ethical landscape of RSU deployment, aiming to identify potential challenges and pathways to compliance with applicable laws and regulations. By integrating technical evaluations, stakeholder discussions, and regulatory analysis, the study provided a comprehensive perspective on the feasibility and challenges of an open RSU platform.

Key findings of the project highlight that existing technologies, such as ONVIF Profile M and Robot Operating System 2 (ROS2), can facilitate RSU-DU communication, yet a universally accepted Intelligent Transportation Systems (ITS)-specific standard remains elusive. Effective V2X messaging for VRU safety requires a minimum dataset, including position, speed, direction, timestamp, and object ID of VRUs. The study indicates that, among messaging protocols, CPMs are better suited for RSU-based VRU detection than VAMs due to technological constraints and adoption challenges.

Introducing standardized messaging between DUs and RSUs has the potential to improve the state of the art in I2V-related infrastructure for ITS. Privacy and regulatory compliance, particularly adherence to the General Data Protection Regulation (GDPR) and Sweden’s Camera Surveillance Act, are critical considerations for implementing I2V

in public spaces. Public Key Infrastructure (PKI) interoperability, infrastructure costs, and spectrum allocation for V2X communication remain key challenges.

This study has identified technological and regulatory gaps in RSU-based VRU protection and offers insights that can support the development of an open RSU platform. Standardizing RSU-DU communication is a key future consideration the study puts forward.

2. Sammanfattning på svenska

Projektets Bakgrund och Syfte

Detta projekt syftade till att utvärdera genomförbarheten av en öppen arkitektur som kan integrera ett brett urval av intelligenta sensorer och ansluta dem till en I2V-infrastruktur på ett säkert, interoperabelt och kostnadseffektivt sätt. Den övergripande ambitionen var att möjliggöra en standardiserad lösning som kan implementeras av kommuner, väg myndigheter och privata aktörer för att förbättra trafiksäkerheten.

Trots en minskning av det totala antalet trafik dödsfall i Sverige förblir dödsolyckor bland oskyddade trafikanter (VRU) relativt höga. Detta understryker behovet av förbättrade säkerhetsmekanismer, särskilt vid övergångsställen, korsningar och andra riskområden där VRU interagerar med fordonstrafik.

Projektet syftade till att besvara tre huvudfrågor:

1. **Tekniska hinder** – Finns det idag tekniska begränsningar som hindrar utvecklingen av en öppen arkitektur?
2. **Minimikrav** – Vilka är de lägsta tekniska kraven för att implementera en sådan arkitektur?
3. **Relevans och behov** – Är det relevant för slutanvändare, VRU, förare, kommuner och företag att utveckla en standard?

Svaren på dessa frågor är omfattande och nyanserade men indikerar i huvudsak positiva förutsättningar för att realisera en sådan öppen arkitektur.

Metod och Arbetsprocess

Studien följde en strukturerad metod för att analysera genomförbarheten av en öppen RSU-plattform (Roadside Unit) och var uppdelad i tre arbetspaket:

- **WP2: Sensor- och detektionsanalys**
  - Utvärdering av radarenheter och kamerabaserade system för att upptäcka VRU vid vägkanter och övergångsställen.

    - Testning av olika detektionsalgoritmer och deras förmåga att generera och överföra metadata i realtid.
    - Analys av datakvalitet och latens i detektering och överföring till varningssystem.

- **WP3: Kommunikationsstandarder och I2V/V2X-meddelandehantering**
    - Undersökning av CPM (Collective Perception Messages) och VAM (VRU Awareness Messages) som kommunikationsstandarder för att förbättra situationsmedvetenhet och skydd av VRU.
    - Identifiering av minimikrav för V2X-meddelanden, inklusive position, hastighet, riktning, tidsstämpel och objekt-ID.
    - Analys av nätverkslatens och dataöverföringshastighet för realtidskommunikation mellan RSU och fordon.

- **WP4: Juridiska och etiska aspekter**
    - Utvärdering av dataskydd och integritetslagstiftning, inklusive GDPR och Sveriges kameraövervakningslag.
    - Rättsliga begränsningar vid användning av kamerabaserade system i offentlig miljö.
    - Regulatoriska krav för V2X-kommunikation, inklusive frekvensallokering och krav på PKI (Public Key Infrastructure) för säker kommunikation.

Genom att kombinera tekniska tester, intressentdialoger och regulatoriska analyser skapades en helhetsbild av genomförbarheten och utmaningarna med en öppen RSU-plattform.

Huvudresultat och Slutsatser

Projektet identifierade flera viktiga insikter:

- **Teknologi och standardisering**
    - Befintliga teknologier som ONVIF Profile M och ROS2 kan underlätta kommunikation mellan RSU och DU.
    - Det saknas dock en universellt accepterad ITS-specifik standard, vilket försvårar interoperabilitet mellan leverantörer.

- **Meddelandeprotokoll för VRU-skydd**
    - CPM (Collective Perception Messages) är bättre lämpade för RSU-baserad VRU-detektering än VAM, på grund av tekniska begränsningar och utmaningar vid adoption.
    - Effektiv V2XD-meddelandehantering kräver minimidatauppsättningar för att kunna förmedla trafiksituationen på ett korrekt sätt.

- **Utmaningar vid implementering**

- Bristen på en standardiserad RSU-DU-kommunikation utgör ett hinder för leverantörsoberoende lösningar.
- Integritets- och regulatoriska krav är avgörande och måste uppfyllas för att möjliggöra bred adoption.
- PKI-interoperabilitet, infrastrukturkostnader och frekvensallokering för V2X-kommunikation utgör ytterligare utmaningar.

Vägen Framåt

Denna studie har kartlagt både tekniska och regulatoriska luckor i RSU-baserat VRU-skydd och tillhandahåller insikter som kan stödja utvecklingen av öppna RSU-plattformar.

För att möjliggöra skalbar implementering är det avgörande att:

1. Etablera en standard för RSU-DU-kommunikation
2. Säkerställa regulatorisk efterlevnad och integritetsskydd
3. Optimera tekniska lösningar för realtidsdetektering och varning

Vidare forskning och pilotprojekt kan bidra till att övervinna nuvarande hinder och bana väg för framtidens intelligenta transportsystem, där öppna RSU-lösningar kan spela en nyckelroll i att öka säkerheten för oskyddade trafikanter.

3. Background

The driving force behind this project is a desire for safer roads for all users, especially the most vulnerable ones (VRUs - pedestrians, cyclists, powered two-wheelers). In 2024, a total of 210 people lost their lives in reported traffic accidents in Sweden. Vulnerable road users accounted for 44% of the fatalities: 16% were motorcyclists, 12% bicyclists, 15% pedestrians, and 1% moped-drivers.[1] Moreover, the number of road traffic fatalities decreased by almost 20 people compared to the previous year, but the decline is most noticeable for protected road users, which include cars, trucks and buses. For unprotected road users such as cyclists, motorcyclists and pedestrians, there is no decline, but rather a slight increase compared to the average of the last five years. These figures highlight the ongoing need for efforts to achieve the Vision Zero[2] goals, especially VRUs.

Vulnerable Road Users (VRUs) face disproportionate risks on the road due to their limited protection and visibility. As traffic complexity increases, the need to enhance their safety becomes paramount. This research project, focusing on the potential of Infrastructure-to-Vehicle (I2V) communication technology, aims to address this challenge by exploring innovative solutions to improve safety at crossways, a particularly hazardous area for VRUs. By enabling communication between vehicles and roadside infrastructure, I2V technology offers promising opportunities to provide timely warnings and critical information to drivers and VRUs, ultimately contributing to a safer road environment for all.

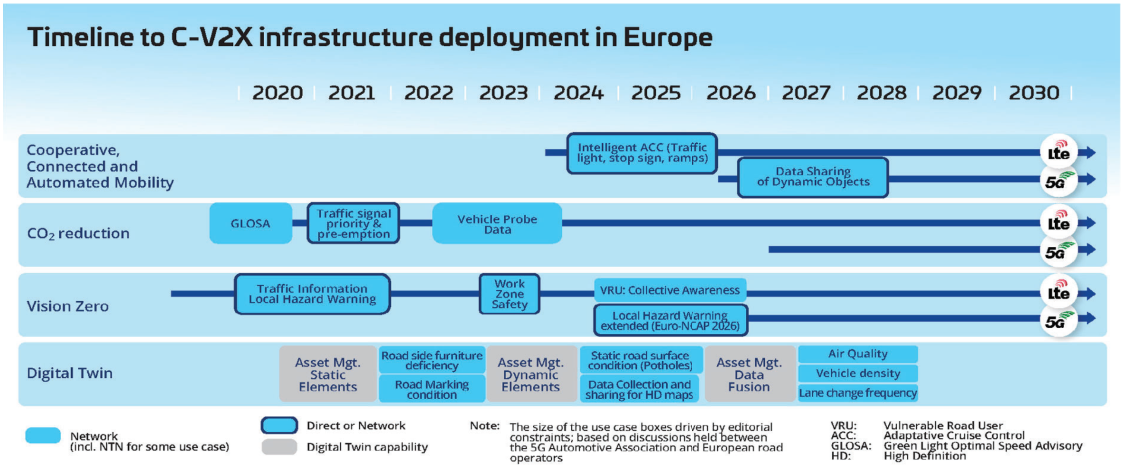
3.1. Vehicle-to-Everything (V2X) Communication

Vehicle-to-Everything (V2X) communication enables vehicles to exchange information wirelessly with each other (V2V), with infrastructure (V2I), and with vulnerable road users (V2P) such as pedestrians and cyclists. This real-time exchange of data, including road conditions, potential hazards, and the movements of other vehicles, empowers drivers to make more informed decisions, ultimately enhancing safety and optimizing traffic flow. V2X technology holds significant promise for preventing collisions, reducing congestion, and improving overall transportation efficiency.[3]

In the Nordic region, the Nordic Way initiative[4] has been instrumental in advancing V2X communication as a key component of its broader mission to foster the development and deployment of intelligent transportation systems (ITS). Through collaborative projects and pilot deployments, the initiative evaluates the real-world benefits of V2X applications, such as cooperative collision avoidance, traffic signal optimization, and pedestrian safety systems. These efforts typically involve partnerships among public authorities, industry stakeholders, research institutions, and technology providers, fostering innovation and accelerating the adoption of V2X-enabled technologies.

3.2. Future Focus: Advancing Infrastructure-Based Intersection Safety

5GAA[5] plans to publish a technical report on infrastructure-based intersection safety use cases documenting the concept of operations, descriptions of various deployment options, and detailed system-level profile recommendations on the messages and protocols needed to enable interoperable and trustworthy implementations.[6] Our research is closely aligned with this direction, focusing on infrastructure-based intersection safety use cases, deployment models, and system-level protocols to enable interoperable and trustworthy implementations.



Timeline to C-V2X infrastructure deployment in Europe
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
Cooperative, Connected and Automated Mobility
Intelligent ACC (Traffic light, stop sign, ramps)
Data Sharing of Dynamic Objects
CO₂ reduction
GLOSA
Traffic signal priority & pre-emption
Vehicle Probe Data
Vision Zero
Traffic Information Local Hazard Warning
Work Zone Safety
VRU: Collective Awareness
Local Hazard Warning extended (Euro-NCAP 2026)
Digital Twin
Asset Mgt. Static Elements
Road side furniture deficiency
Road Marking condition
Asset Mgt. Dynamic Elements
Static road surface condition (Potholes)
Data Collection and sharing for HD maps
Asset Mgt. Data Fusion
Air Quality
Vehicle density
Lane change frequency
lte
5G
Network (incl. NTN for some use case)
Direct or Network
Digital Twin capability
Note: The size of the use case boxes driven by editorial constraints; based on discussions held between the 5G Automotive Association and European road operators
VRU: Vulnerable Road User
ACC: Adaptative Cruise Control
GLOSA: Green Light Optimal Speed Advisory
HD: High Definition

Figure 1: Timeline to C-V2X infrastructure deployment in Europe [4]

The Day 2 phase of the C2C-CC Roadmap[7] also aims to extend the V2X system to additionally permit vehicles and RSUs to share information about objects detected via on-board sensors such as cameras, LiDARs (Light Detection and Ranging) or RADARs (Radio Detection and Ranging).

Other than VRU protection, RSUs with sensors provide feasibility of adding extra features like Vehicle Co-operation with traffic light controllers, Extended Cooperative Awareness Messages(CAMS) and Decentralized Environmental Notification Messages (DENMS), Traffic Misbehavior detection, and Improved positioning support by GPS corrections from infrastructure [7].

4. Purpose, research questions and method

4.1. Purpose

The purpose of this pre-study is to explore the feasibility of defining a non-proprietary, communications agnostic platform architecture that can integrate sensors and enable them to be added to an I2V infrastructure in an easy and cost efficient manner, to enhance road safety.

With the acceleration of machine learning and Artificial Intelligence, sensor technology based on camera, RADAR and LiDAR imaging will continue to advance at a very high speed. While advancements in vehicle safety have greatly improved protection for occupants, a similar reduction in fatalities among VRUs has not been achieved[8]. This highlights the urgent need to prioritize VRU safety. A real-world example from Malmö, Sweden, illustrates this need: a parking exit intersects with a pedestrian and bicycle path, creating a blind spot for both drivers and cyclists (*Figure 2*). Many bicycle accidents occur at road crossings, with drivers often citing “failure to look properly” as the cause of collisions[8]. This scenario demonstrates how limited visibility elevates the risk of accidents, endangering VRUs.

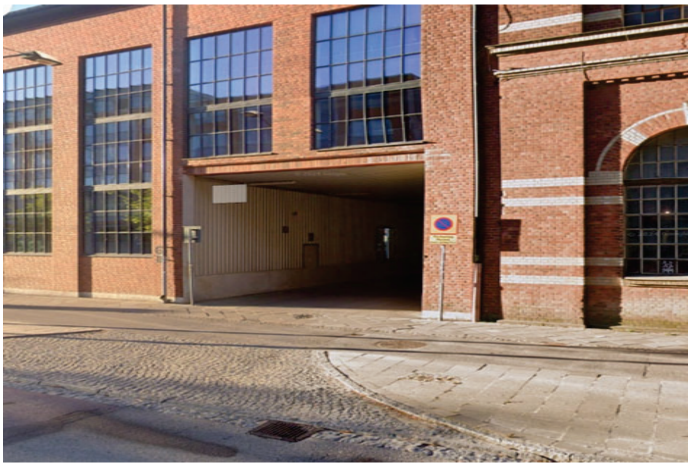


Figure 2. Exit for cars from parking area onto pedestrian and bicycle path

Sensor-based solutions could address these safety challenges effectively. Two potential implementations for the Malmö scenario include(Figure 3):

1. **Cyclist and Pedestrian Detection for Vehicles Exiting the Parking Area:**
   Installing two radars in opposite directions at the parking exit can detect approaching cyclists. When a cyclist is detected, a red warning lamp (optionally with a siren) alerts the driver, enabling them to stop in time and prevent a potential collision.

2. **Vehicle Detection for Cyclists and Pedestrians:**
   A camera positioned inside the parking gate detects vehicles exiting. When a car approaches the exit, a red warning lamp (optionally with a siren) alerts cyclists and pedestrians nearby, giving them sufficient time to avoid the vehicle's path.

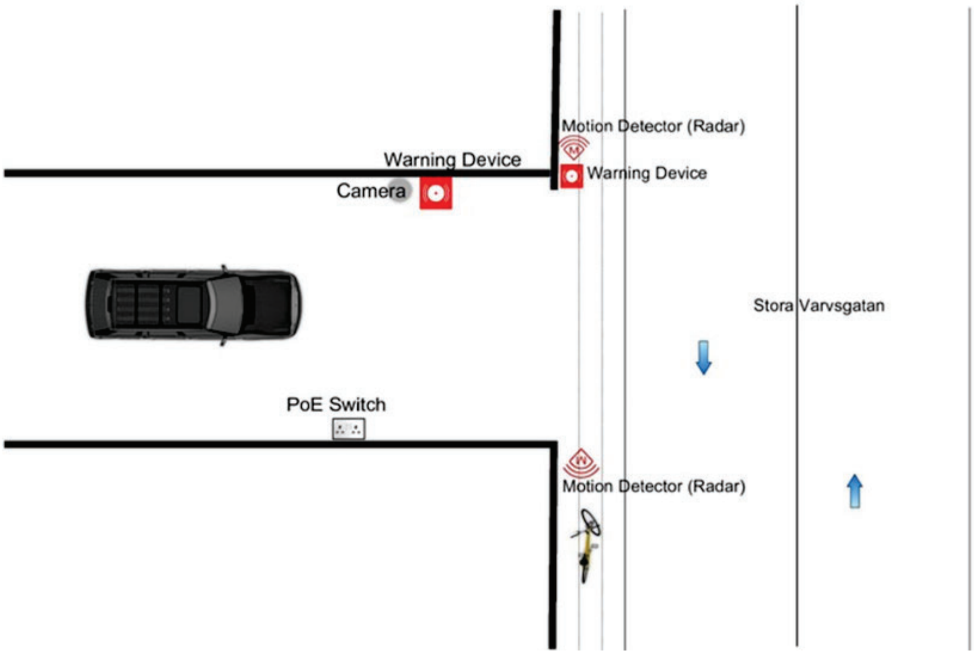


Figure 3. Potential use of radars and cameras to reduce safety risks

Sensor-based solutions like these demonstrate the potential to enhance road safety significantly, but their broader adoption is often hindered by challenges related to cost and scalability. While numerous sensors and digital connectivity solutions exist to improve road safety, many are neither cost-effective nor easy to scale. Developing open, communication-agnostic standards simplifies system complexity, enhances cost-effectiveness, promotes vendor neutrality, and ensures interoperability. Streamlining implementation and maintenance through standardization can lead to faster deployments, ultimately contributing to reduced road fatalities.

For I2V communication systems to effectively improve safety for VRUs, it is essential that transmitted messages contain precise and actionable information. At a minimum, this includes accurate Global Navigation Satellite System (GNSS) coordinates that establish the exact position of detected objects. However, to provide meaningful context, additional data such as speed, acceleration, and direction of movement are critical. This dynamic information allows other road users and infrastructure to anticipate the behavior of VRUs and respond appropriately.

Equally important is the need for a shared coordinate framework. Isolated coordinates have limited value without a consistent reference plane that ensures all connected vehicles and infrastructure interpret positional data in the same spatial context. This ensures that detection and warning systems can accurately assess proximity, trajectory, and potential collision risks in real-world environments.

By embedding this contextual and dynamic data into communication protocols, I2V systems can deliver timely and relevant alerts to drivers and connected vehicles. This is particularly vital in complex urban scenarios-such as the Malmö parking exit example-where limited visibility increases the risk of accidents. Messages that effectively combine precise location data with movement context can empower both human drivers and automated systems to make better, safer decisions.

Establishing communication standards that support the seamless integration of such data is fundamental to achieving scalable and interoperable safety solutions. However, the state of the art indicates a gap in efforts to create an open, communication-agnostic RSU architecture[9]. Although we recognize that we cannot drive the standardization process ourselves, we aim to provide valuable insights into existing V2X systems, identifying areas where standards are already implemented and where there is room for improvement.

4.1.1 Scope

The scope of this feasibility study is limited to analyzing the compatibility and interoperability of various sensor systems and warning systems using I2V communication. The study aims to provide foundational insights and recommendations for an open and standardized RSU platform, facilitating safer and more efficient integration between vehicles, infrastructure, and vulnerable road users.

4.2. Research Questions

The study focused on evaluating the practical and technical viability of designing an open, flexible architecture for RSUs, a critical component in connected vehicle and smart infrastructure ecosystems.

The following sub questions were formulated to approach the study in a comprehensive manner covering different aspects of the problem.

- Are there any technical barriers to creating an open RSU architecture?

This question aims to identify potential challenges or constraints (e.g., interoperability, security risks, or standardization issues) that may hinder the development of an open architecture for RSUs. It also involves investigating technological gaps and existing roadblocks in integrating diverse systems under an open framework.

- What are the technical minimum requirements to achieve an open architecture for an RSU?

This question explores the foundational technical specifications and capabilities required for an open and standardized Roadside Unit (RSU) architecture, focusing primarily on the communication aspects. Recognizing that most RSUs already possess or can readily incorporate essential hardware components like a capable processor, Hardware Security Module, Ethernet, USB, GNSS, and wireless communication modules (e.g., WiFi, LTE/5G), this study does not delve into hardware specifics. Instead, it prioritizes critical aspects such as communication protocols, adherence to established standards, privacy considerations, data protection mechanisms, and scalability.

- Is an RSU with an open architecture relevant for stakeholders?

This question evaluates the importance and practicality of adopting an open architecture for RSUs in real-world scenarios. It includes examining stakeholder needs and potential benefits like cost reduction.

4.3. Methodology

Three work packages - WP2, WP3, and WP4 - were developed to address the key research questions outlined in the study.

In each work package, the TIPPSS framework[10] - Trust, Identity, Privacy, Protection, Safety, and Security - served as a valuable guide for addressing the multifaceted concerns inherent to I2V communication. By aligning the RSU architecture with the principles of TIPPSS, this research aims to foster a robust and trustworthy I2V ecosystem that prioritizes the safety and security of all road users while upholding ethical data management practices.

We also held discussions with researchers and practitioners at the forefront of road safety solutions to gain insights into cutting-edge developments relevant to each work package.

4.3.1. WP2: Evaluate sensing systems for Road Side Units (RSU)

In this work package, we aimed to conduct a high-level exploration of the communication structures between Sensing Systems (*also referred to as Detection Units (DUs) in this document*) and Roadside Units (RSUs), evaluating the feasibility of a minimal message structure to enable end-to-end I2V communication, specifically for use cases involving the protection of VRUs on crossways.

Our approach was to evaluate the current state of communication between RSUs and Sensing Systems/DUs, identifying any existing standards that define these interactions. The goal is to explore how RSU-DU communication can be made vendor-agnostic. This work package focused on the structure of the data, transmission protocols, and the channels through which it is communicated.

To accomplish this, we planned to evaluate several DUs to gain insights into the current state of the art. Some of the questions we have aimed to answer in this work package are

- What existing standards or protocols govern the communication between RSUs and DUs?
- How do current RSU-DU communication practices vary across different vendors and implementations?
- How can a minimal message structure facilitate vendor-agnostic communication?
- What are the common data structures used in RSU-DU communication, and how do they impact performance and reliability?
- Which communication protocols are most widely used, and how do they compare in terms of efficiency, reliability, and scalability?
- What would an ideal communication framework between RSUs and DUs look like in the context of smart infrastructure?
- How to apply TIPPSS considerations to the communication between DUs and RSUs

To address the questions outlined in this work package, the following steps were planned:

Testing of Leading Detection Units: Conducting tests on major Detection Units available in the market to analyze and understand their data structures.

Reviewing Existing Standards: Investigating any current standards utilized in Intelligent Transportation Systems (ITS) to identify frameworks relevant to RSU-DU communication.

4.3.2. WP3: Evaluate alerting systems for Road Side Units (RSU) using I2V

This work package focused on evaluating the communication between Roadside Units (RSUs) and Alerting Mechanism Units (AMUs) using Infrastructure-to-Vehicle (I2V) communication. The primary objective was to assess the compatibility and interoperability of RSUs and AMUs in the context of Vulnerable Road Users (VRUs). To achieve this, the study examined I2V and Vehicle-to-Infrastructure (V2I) messaging standards, as defined by the European Telecommunications Standards Institute (ETSI) for the European Union.

The research was carried out through the following steps:

- Exploration of I2V/V2X Messaging Standards

Performing an in-depth review of I2V and broader V2X message types to identify those most relevant to VRU-related use cases.

- Evaluation of Minimum Data Requirements

Identifying a potential minimum set of data elements required from the Detection Unit to support effective I2V communication for VRU scenarios, ensuring accurate and timely alerts.

- Analysis of Real-World V2X Messages

Collecting and analyzing real-world V2X message samples that contain data pertaining to VRUs, evaluating their structure, content, and relevance to the use case.

- Assessment of Current Adoption and Limitations

Evaluating the current status of adoption of relevant standards, along with identifying technological and operational limitations that may hinder widespread deployment or interoperability.

4.3.3. WP4: Evaluate policy and regulation for RSUs

This work package focused on evaluating the legal and ethical considerations related to the use of sensors in public spaces, particularly concerning privacy. The study aimed to analyze data collection, storage, and usage practices to identify the requirements for compliance with relevant laws and regulations, such as GDPR, while prioritizing individuals' rights. We also sought to evaluate the potential of I2V communication systems for stakeholders, pinpointing key adoption challenges, including cost and other barriers.

The approach used to accomplish this involved the following steps.

- Studying the respective laws and regulations
- Interviews with stakeholders like municipalities and experts.

5. Objective

This study explored the feasibility of developing an open, communication-agnostic RSU platform architecture by assessing technical and practical challenges, defining minimum requirements, and evaluating its relevance in real-world scenarios.

As we progressed in our study, we realised that, while existing standards, such as ONVIF[11], define communication protocols for devices like DUs, they have not been widely adopted or popularized. Similarly, established standards already govern communication between RSUs and OBUs. As a result, we have placed greater emphasis on RSU-to-DU communication (Figure 4), specifically addressing gaps in standardization related to traffic safety and adoption in this area.

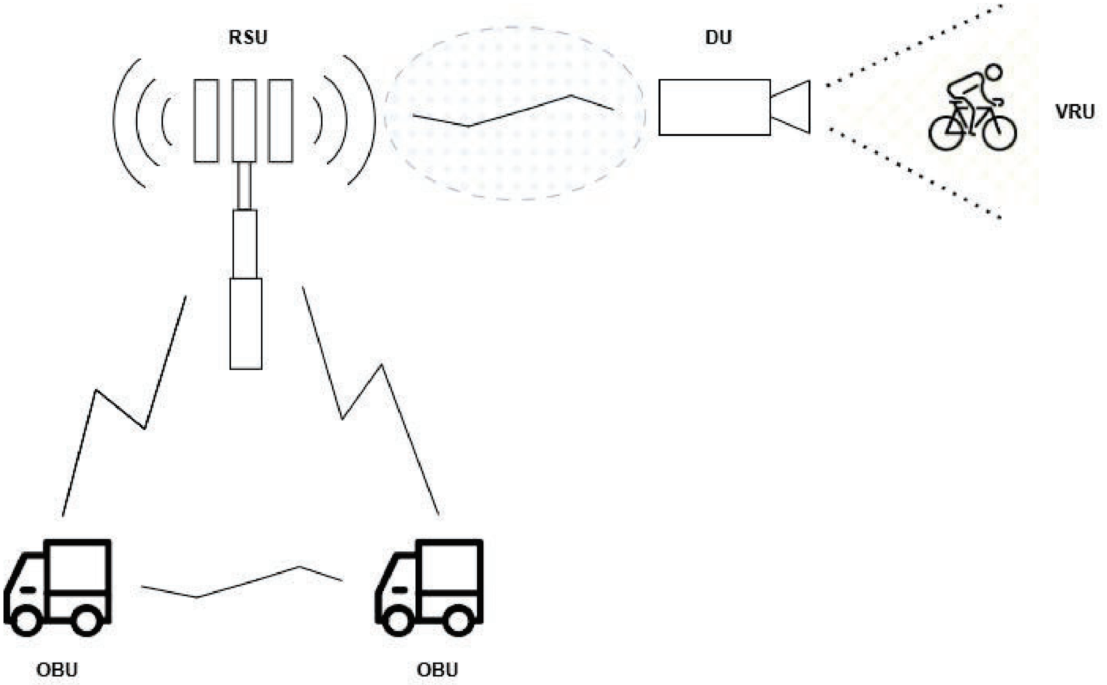


Figure 4. The blue oval represents the refined focus of communication between RSU-to-DU

Rather than proposing or implementing a solution, this study provides a foundational analysis, offering insights into where existing standards are effective and where improvements or new standards could be most impactful. This approach aims to inform and guide future efforts in developing scalable, interoperable solutions for improved road safety and connectivity.

6. Results and deliverables

6.1. WP2: Evaluate sensing systems(DUs) for Road Side Units (RSU)

The following section provides a detailed description of the key steps undertaken in this work package.

6.1.1. Analyzing Metadata Transmission for Specific Use Cases Through Tests

The evaluation focused on analyzing the metadata transmitted by Detection Units (DUs) during motion detection events. To facilitate this, two DUs were procured, and various use cases were implemented to collect and assess this metadata.. An Alert Mechanism Unit (AMU) was also procured to simulate the end-to-end communication from the DU to an alerting mechanism that does not involve V2X, but helps to establish the efficacy of the data from the Detection Units. In a real world scenario, an RSU connected to the network will be receiving the metadata from the DUs and sending the required V2X message to nearby vehicles.

The devices procured included:

1. **AXIS Q1656-DLE (DU)**

   This device utilizes the fusion of radar and visible light sensors. Information in different electromagnetic frequencies complement and correct each other delivering enhanced detection and visualization. As an example, it can identify, classify and count an object as a human, animal, car, motorcycle, bus etc, and also track its speed and direction.[12]

2. **AXIS D2210-E Radar (DU)**

   This network-based radar device utilizes advanced technology to accurately detect, classify, and track humans and vehicles under diverse weather and lighting conditions.[13]

3. **AXIS D4100-E (AMU)**

   Network-connected strobe siren for indoor and outdoor use, providing visual alerts with configurable flash patterns and colours. Integrates with Axis network cameras and video management systems for event-driven activation and centralized management.[14]

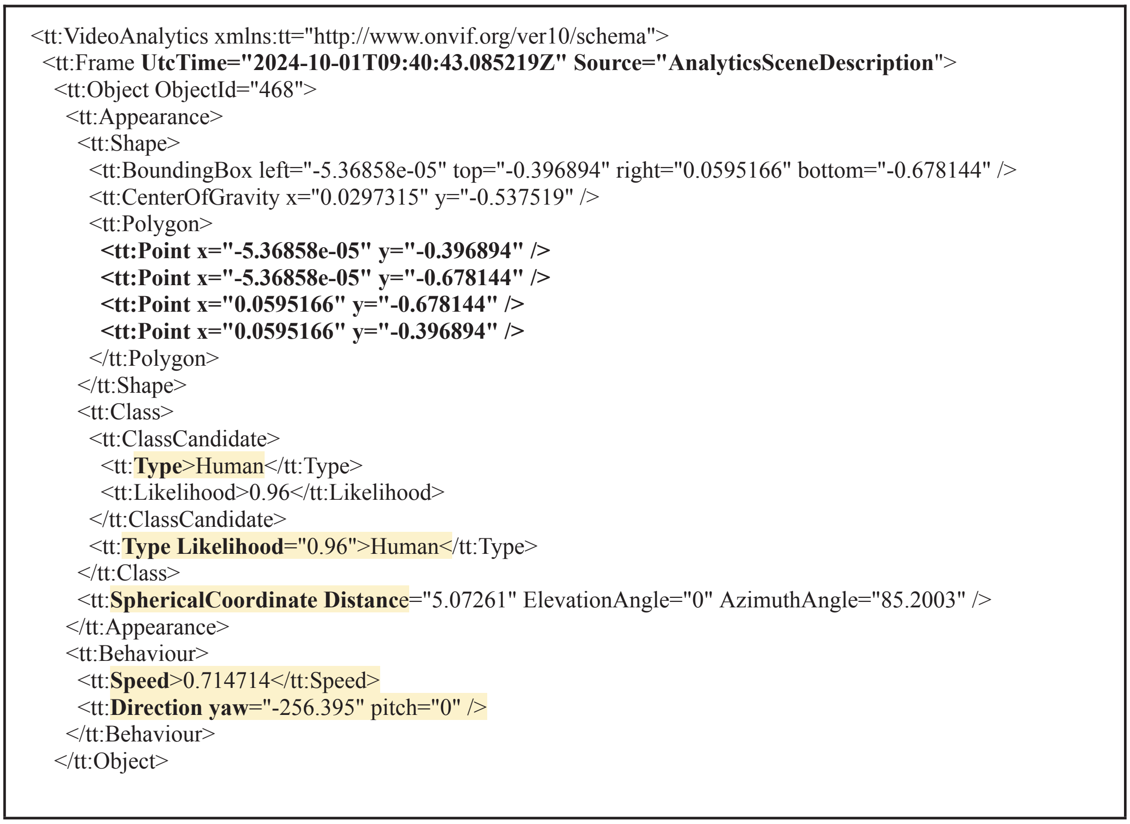
The following section provides a comprehensive overview of the use cases designed to test the functionality of the procured Detection Units (DUs). It focuses on the structure of the metadata and the details transmitted upon object detection. In the following test cases, the visual data is processed locally in the detection units, and only the metadata is sent to the network. This eliminates all personally identifiable information from the data and thus strengthens the TIPPSS aspect of the entire system.

Test Case 1

In this scenario, the AXIS Q1656-DLE was deployed to collect metadata generated upon detecting an object. The metadata captured from the DU is detailed below:

Time	2024-10-01T09:40:43.085219Z
Source	AnalyticsSceneDescription
Object Type	Human (Likelihood: 96%)
Distance	5.07261 units
Speed	0.714714 units
Direction	Yaw -256.395 degrees

This metadata provides valuable insights into the object's characteristics and movement, demonstrating the capabilities of the AXIS Q1656-DLE in real-world detection scenarios.



```
<tt:VideoAnalytics xmlns:tt="http://www.onvif.org/ver10/schema">
 <tt:Frame UtcTime="2024-10-01T09:40:43.085219Z" Source="AnalyticsSceneDescription">
  <tt:Object ObjectId="468">
   <tt:Appearance>
    <tt:Shape>
     <tt:BoundingBox left="-5.36858e-05" top="-0.396894" right="0.0595166" bottom="-0.678144" />
     <tt:CenterOfGravity x="0.0297315" y="-0.537519" />
     <tt:Polygon>
      <tt:Point x="-5.36858e-05" y="-0.396894" />
      <tt:Point x="-5.36858e-05" y="-0.678144" />
      <tt:Point x="0.0595166" y="-0.678144" />
      <tt:Point x="0.0595166" y="-0.396894" />
     </tt:Polygon>
    </tt:Shape>
    <tt:Class>
     <tt:ClassCandidate>
      <tt:Type>Human</tt:Type>
      <tt:Likelihood>0.96</tt:Likelihood>
     </tt:ClassCandidate>
     <tt:Type Likelihood="0.96">Human</tt:Type>
    </tt:Class>
    <tt:SphericalCoordinate Distance="5.07261" ElevationAngle="0" AzimuthAngle="85.2003" />
   </tt:Appearance>
   <tt:Behaviour>
    <tt:Speed>0.714714</tt:Speed>
    <tt:Direction yaw="-256.395" pitch="0" />
   </tt:Behaviour>
  </tt:Object>
```

Figure 5, Metadata from Q1656 DLE (Radar and camera fusion) DU

Test Case 2

In this scenario, the AXIS D2210-E Radar DU was used to collect metadata upon detecting an object. The metadata captured is as follows:

Time	2024-10-01T09:18:16.709860Z
Source	RadarMotionTracker
Object Type	Unknown (Likelihood: -1.00)
Distance	9.75 units
Speed	0.67 units
Direction	Yaw -215.771 degrees

This metadata underscores the radar's capability to detect objects at significant distances and track their movement with precision, even in scenarios where object classification may not be determined.

```
<tt:VideoAnalytics xmlns:tt="http://www.onvif.org/ver10/schema">
<tt:Frame UtcTime="2024-10-01T09:18:16.709860Z" Source="RadarMotionTracker">
 <tt:Object ObjectId="2300">
        <tt:Appearance>
         <tt:Shape>
               <tt:BoundingBox bottom="-0.775391" top="-0.755371" right="-0.050781" left="-0.070801" />
               <tt:CenterOfGravity x="-0.070801" y="-0.775391" />
               <tt:Polygon>
                <tt:Point x="-0.080811" y="-0.785400" />
                <tt:Point x="-0.060791" y="-0.785400" />
                <tt:Point x="-0.060791" y="-0.765381" />
                <tt:Point x="-0.080811" y="-0.765381" />
               </tt:Polygon>
         </tt:Shape>
         <tt:Class>
               <tt:ClassCandidate>
                <tt:Type>Other</tt:Type>
                <tt:Likelihood>-1.00</tt:Likelihood>
               </tt:ClassCandidate>
               <tt:Extension>
                <tt:OtherTypes>
                       <tt:Type>Unknown</tt:Type>
                       <tt:Likelihood>-1.00</tt:Likelihood>
                </tt:OtherTypes>
               </tt:Extension>
               <tt:Type Likelihood="-1.00">Unknown</tt:Type>
         </tt:Class>
         <tt:Extension>
               <axrt:RadarObjectInfo xmlns:axrt="http://www.axis.com/2017/radar/axrt">
                <axrt:PolarCoordinate angle="-45.33" range="9.75" elevation-angle="0.00" />
                <axrt:Velocity m-s="0.67" angle="305.77" elevation-angle="0.00" />
                <axrt:Size m="1.40" />
               </axrt:RadarObjectInfo>
               <tt:GeoLocation lon="-0.0000623" lat="0.0000619" elevation="0" />
         </tt:Extension>
         <tt:SphericalCoordinate Distance="9.74805" ElevationAngle="0" AzimuthAngle="135.329" />
         <tt:GeoLocation lon="-0.0000623" lat="0.0000619" elevation="0.00" />
        </tt:Appearance>
        <tt:Behaviour>
         <tt:Speed>0.67</tt:Speed>
         <tt:Direction yaw="-215.771" pitch="0" />
        </tt:Behaviour>
 </tt:Object>
</tt:Frame>
</tt:VideoAnalytics>
```

Figure 6, Metadata from AXIS D2210-E Radar DU

Test Case 3

This use case evaluates the end-to-end integration of a Detection Unit (DU) with an Alert Mechanism Unit (AMU), designed to enhance the detection system by providing immediate and noticeable alerts.

The specific AMU used is the AXIS D4100-E, featuring a networked siren and strobe light for robust alert capabilities.

For this test, we utilized the MQTT protocol[16], which operates on a broker-client architecture. This is particularly relevant as it separates the functions of the AMU and DU, eliminating point-to-point limitations. One or more DUs can publish a payload to a specific topic within the broker. Subsequently, any current or future AMUs can subscribe to this topic, receiving the payload and responding accordingly, supporting scalability.

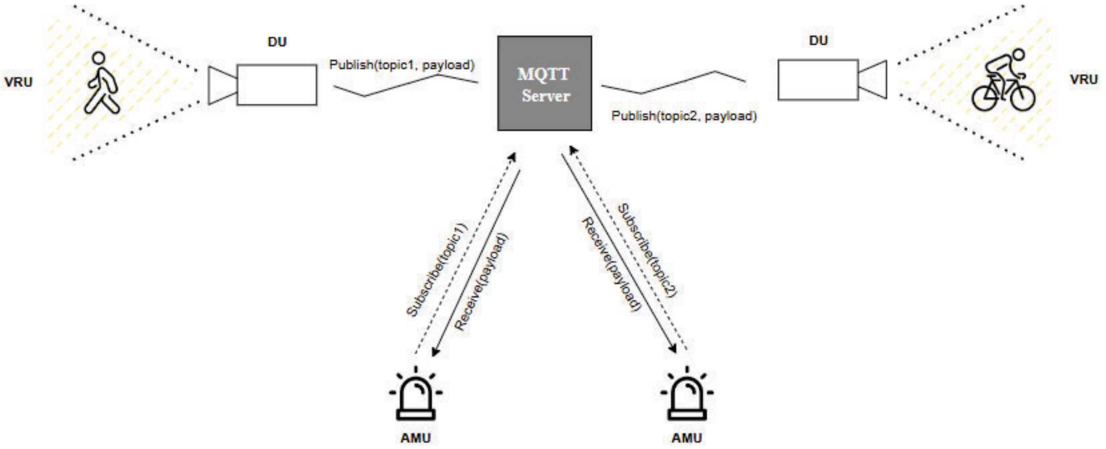


Figure 7. Diagram of implementation

Implementation Steps:

1. **Detection**:
   The DU identifies motion within its field of view.
2. **Notification**:
   Upon detection, the DU sends a predefined message to the AMU.
3. **Alert**:
   The AMU responds to the received message by activating its alert mechanisms, such as the siren and strobe light. This ensures immediate and noticeable notifications of motion detection events.

This integrated scenario demonstrates the seamless collaboration between detection and alert units, providing an efficient and scalable solution for enhanced security and monitoring.

Following a detailed comparison and analysis of the collected metadata, the table below illustrates the data transmitted from the DUs upon detecting an object.

Features		**Q1656 (Radar and camera fusion)**	**Q1656 (Only camera)**	**D2210-E Radar**
UtcTime		✓	✓	✓
Source		✓	✓	✓
Appearance / Shape		✓	✓	✓
Type		✓	✓	Not tested
GeoLocation		✓		✓
SphericalCoordinate		✓		✓
Speed		✓		✓
Direction		✓		✓

Table1, Useful Metadata fields of different DUs upon detecting an object

6.1.2. Discussion with AstaZero

We investigated the application of Roadside Units (RSUs) through engagement with key organizations. Notably, AstaZero[17], a user of Commsignia[18] RSUs, provided valuable insights into their practical implementation. AstaZero, in collaboration with Halmstad University, developed a system to track vulnerable road users (VRUs) and send warnings to equipped vehicles.[19] A number of roadside units and onboard units were used in experiments at the AstaZero test track, as well as in open traffic in Gothenburg, rural areas, and along the E4 highway.

The key takeaways from our discussions were:

- AstaZero developed a mobile application to simulate Vulnerable Road User (VRU) detection.
- The mobile app sends MQTT messages to the RSU, which then frames Vehicle-to-Everything (V2X) messages to alert the Alert Mechanism Unit (AMU).
- In this specific case, the AMU was a Volkswagen ID.2 vehicle.
- AstaZero implemented a custom application layer on top of Commsignia's protocol stack to interpret the MQTT messages received from the mobile application.

This approach showcases how AstaZero integrated multiple components to achieve a seamless VRU detection and alerting system using a user device. One significant insight was the need to develop a custom application layer, as the proprietary software used in RSUs complicates integration. Additionally, the use of development tools is subject to licensing agreements, further limiting transparency and flexibility.

6.1.3. Research into existing standards from other industries

We conducted an analysis of existing standards utilized in Intelligent Transportation Systems (ITS) for metadata sharing.

One of the key advantages of using standardized sensors like cameras, RADARs, and LiDARs is the ability to leverage rapidly evolving technology and seamlessly integrate it into ITS. Utilizing a standardized approach opens the door to a wide range of sensors and vendors by employing a unified Application Programming Interface (API) and Software Development Kit (SDK).

It is also important to acknowledge the evolution of surveillance systems - from early closed-circuit television (CCTV) to modern networked devices equipped with advanced sensor capabilities. This evolution has paved the way for the integration of sophisticated sensor technologies into ITS, enabling enhanced data collection and analysis for improved road safety and traffic management.

Our research highlighted several standards relevant to these advancements. For the purposes of this discussion, both metadata and telemetry are collectively referred to as metadata. Here, metadata provides contextual information about the data, such as sensor type, sample time, reading certainty, and sensor health, while telemetry represents the actual sensor data collected.

6.1.3.1. The ONVIF Standard

ONVIF(Open Network Video Interface Forum) standardizes communication between IP-based physical security products and services, ensuring interoperability across different brands and deployments. Primarily used in the surveillance industry, it facilitates the integration of data from sensors manufactured by various vendors into a centralized surveillance station. Today, over 30,000 products conform to the ONVIF profile.[16]

ONVIF Profile M

ONVIF supports multiple profiles for various use cases. Profile M[20] is a standard developed by ONVIF to improve interoperability for metadata and events in intelligent security and IoT applications. It essentially standardizes how devices send and receive information about what's happening in a scene, beyond just the basic video stream.

Key Features:

Metadata Streaming: Profile M defines how devices can stream metadata in real-time. This allows for continuous monitoring and analysis of events.

Event Handling: It standardizes how devices report events, making it easier for other systems to respond to triggers like alarms or intrusions.

Object Classification: Profile M supports various object classifications, allowing for more specific analysis of what's happening in a scene.

MQTT Support: This allows for seamless integration with IoT applications and platforms.

Purposes/Use Cases:

Standardizing Metadata: Profile M defines a standard way for devices (like cameras) to send metadata, which is data about the video content. This metadata can include information like object classifications (person, vehicle), object tracking data, and event triggers (motion detection, line crossing, etc).

Enabling Advanced Analytics: By standardizing metadata, Profile M makes it easier for different systems to process and use this information for advanced analytics, such as people counting, heat mapping, and intrusion detection.

IoT Integration: Profile M also supports communication with IoT platforms and applications using MQTT (Message Queuing Telemetry Transport), enabling integration with other smart systems.

Limitations

Complexity and cost: Because it is an IP based communication protocol, the sensors need to have a network hardware and software stack and related software packages to support it.

Limited scope: ONVIF mainly addresses the communication interface for surveillance equipment. It might be difficult to propose changes needed for ITS use cases.

Testing and certification: ONVIF devices are self-certified. This means that some devices may not be fully compliant with ONVIF standards.

6.1.3.2. The Robot Operating System (ROS) Standard

The Robot Operating System (ROS) is an open-source framework designed to streamline the development of robotic and automation systems. It offers a comprehensive suite of libraries and tools for building robotic applications, including hardware abstraction, device drivers, visualizers, message-passing, package management, and more.[21]

Additionally, Micro-ROS extends ROS2 support to microcontrollers, enabling the development of resource-constrained robotic applications.[22]

ROS-supported peripherals streamline the integration of diverse sensors and actuators into ROS-enabled systems, enhancing efficiency and simplifying development.

Our research found that one of the V2X projects conducted by RWTH Aachen University in Germany utilizes ROS2 to collect V2X data from roadside units (RSUs) equipped with cameras and LiDAR sensors for their research.[23]

Examples of commercially available ROS-compatible peripherals include Velodyne LiDARs, SICK LiDARs, EAI YDLIDAR, Oyster OS-1 3D LiDARs, Slamtech RPLiDAR, Raspberry Pi Camera Modules, Astra cameras, Spinnaker cameras, ZED stereo cameras for depth and motion tracking, Intel RealSense ROS and D400 series cameras, NMEA NavSat-based GPS devices, NovAtel GPS systems, and TI mmWave radars (List of ROS enabled devices).[24 - 27]

ROS Advantages:

Peer-to-peer communication: In ROS, a peer-to-peer architecture enables each component to communicate directly with any other node as required.

Free and open-source: As an open-source platform, ROS offers a wide range of existing drivers and data processing code for various use cases. This makes it significantly easier to propose and implement new features tailored to the needs of ITS applications.

Thin: ROS is designed to be as lightweight as possible—avoiding interference with your main() function—allowing code developed for ROS to be easily used with other robotics software frameworks. Consequently, ROS is highly compatible and has already been successfully integrated with frameworks such as OpenRAVE, Orocos, and Player.

ROS-agnostic libraries: The preferred development model is to write ROS-agnostic libraries with clean functional interfaces.

Language independence: The ROS framework is straightforward to implement in any modern programming language. It has been successfully implemented in Python, C++, and Lisp, with experimental libraries also available in Java and Lua.

Easy testing: ROS includes a built-in unit and integration testing framework called **rostest**, which simplifies the process of setting up and tearing down test fixtures.

Scaling: ROS is well-suited for both large-scale runtime systems and complex development processes.

ROS Disadvantages:

Data type: ROS2 is designed to transfer raw sensor data rather than metadata. As a result, connecting a camera with built-in analytics capabilities may not fully utilize its features.

Complexity and cost: As an IP-based communication protocol, sensors require network hardware, a supporting software stack, and the necessary software packages to enable compatibility.

6.1.4. Consultation with Leo Levit - Steering Committee Chairman, ONVIF

Subject matter experts were consulted to provide further context and inform our findings. From our discussions we gained the following insights.

Most camera manufacturers develop proprietary APIs, For ex., AXIS offers VAPIX, Bosch offers RCP+. However, creating and maintaining these APIs is costly, which led to the development of ONVIF—a standard for camera surveillance. ONVIF enables essential functions like video streaming, pausing, saving, and deleting, with multiple profiles such as Profile V for video, A for audio, and M for metadata.

Our discussion with Leo focused on using Profile M to extract information from sensors like cameras or radars and communicate with RSUs. For instance, relying solely on VAPIX would limit compatibility to AXIS devices, whereas ONVIF allows interoperability across sensors from different manufacturers. Notably, all major industry players support ONVIF, enhancing flexibility and integration.

It’s important to note that ONVIF was originally designed for video management and saving footage, not for using cameras as sensors. While it can be adapted for this purpose, it wasn’t its intended function, so thorough testing is necessary to ensure its effectiveness in such applications.

6.1.5. Conclusions derived from the activities of WP2

Our tests demonstrate that it is feasible to utilize existing protocols such as ONVIF Profile M for RSU-DU communication. However, the lack of a universally accepted ITS-specific standard remains a barrier to achieving full interoperability across vendors.

We also found that devices like the AXIS Q1656-DLE and D2210-E reliably transmit key metadata such as object ID, timestamp, position, speed and direction. These findings demonstrate that a minimal, standardized messaging structure can facilitate effective communication for the use cases for VRU protection.

Moreover, integrating detection units with alert mechanisms, as demonstrated with the AXIS D4100-E, highlights the potential for seamless collaboration between components to enhance safety systems.

It is, however, necessary to develop or adapt communication frameworks that prioritize vendor-agnostic interoperability while ensuring efficiency, security and scalability specifically for ITS applications.

6.2. WP3: Evaluate alerting systems for Road Side Units (RSU) using I2V

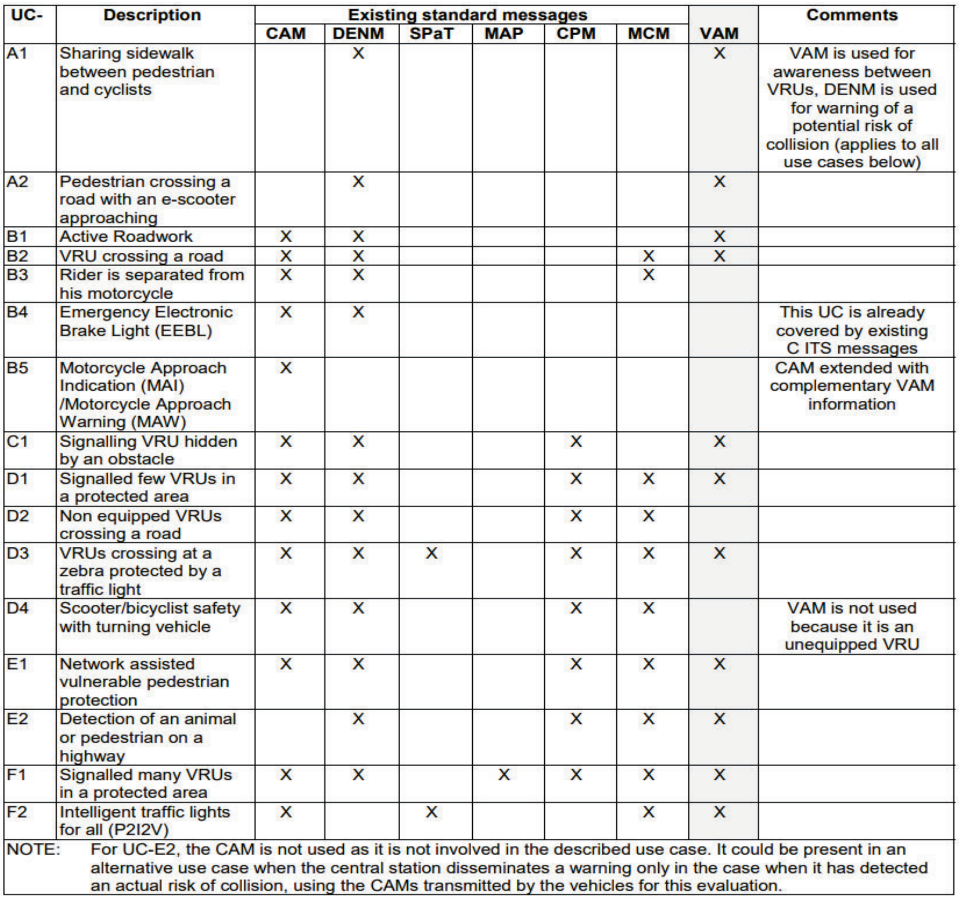
This work package focuses on the **analysis** of I2V/V2X messaging standards, with a particular emphasis on their role in enhancing the safety of Vulnerable Road Users (VRUs). It involves a comparative study of existing messaging protocols, evaluating their effectiveness in VRU protection and identifying potential gaps or areas for improvement.

We also aim to identify a minimal functional dataset required for effective V2X communication in VRU protection use cases.

The following section offers a detailed overview of the key steps carried out in this work package.

6.2.1. Exploration of I2V/V2X Messaging Standards and Protocols for Vulnerable Road User (VRU) Protection

The ETSI Specifications TS 103 300-2 and TS 103 300-3 (*Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness*)[25-29] outlines all the available message types for use cases involving VRUs.



UC-	Description	Existing standard messages							Comments
		CAM	DENM	SPaT	MAP	CPM	MCM	VAM	
A1	Sharing sidewalk between pedestrian and cyclists		X					X	VAM is used for awareness between VRUs, DENM is used for warning of a potential risk of collision (applies to all use cases below)
A2	Pedestrian crossing a road with an e-scooter approaching		X					X	
B1	Active Roadwork	X	X					X	
B2	VRU crossing a road	X	X				X	X	
B3	Rider is separated from his motorcycle	X	X				X		
B4	Emergency Electronic Brake Light (EEBL)	X	X						This UC is already covered by existing C ITS messages
B5	Motorcycle Approach Indication (MAI) /Motorcycle Approach Warning (MAW)	X							CAM extended with complementary VAM information
C1	Signalling VRU hidden by an obstacle	X	X			X		X	
D1	Signalled few VRUs in a protected area	X	X			X	X	X	
D2	Non equipped VRUs crossing a road	X	X			X	X		
D3	VRUs crossing at a zebra protected by a traffic light	X	X	X		X	X	X	
D4	Scooter/bicyclist safety with turning vehicle	X	X			X	X		VAM is not used because it is an unequipped VRU
E1	Network assisted vulnerable pedestrian protection	X	X			X	X	X	
E2	Detection of an animal or pedestrian on a highway		X			X	X	X	
F1	Signalled many VRUs in a protected area	X	X		X	X	X	X	
F2	Intelligent traffic lights for all (P2I2V)	X		X			X	X	
NOTE:	For UC-E2, the CAM is not used as it is not involved in the described use case. It could be present in an alternative use case when the central station disseminates a warning only in the case when it has detected an actual risk of collision, using the CAMs transmitted by the vehicles for this evaluation.								

Table 2. C-ITS messages for ETSI VRU use case [28]

According to the specification, the applicable message types include **DENM**, **CPM**, **MCM**, and **VAM**.

DENM is particularly useful for scenarios where an animal or person is detected on the road. Referencing ETSI TS 103 300-2[28], Table 10 provides a detailed description of causes and assigned codes for ETSI use cases. However, DENM is not ideal for sending notifications about a VRU approaching a crossway because it is designed to send messages about hazards already on the road like road works, lane closure, black ice, etc.[30]

Due to the low inertia and unpredictable behaviour of VRUs, it is challenging to use MCM effectively to send messages aimed at avoiding VRUs on the road. This limitation is elaborated in ETSI TR 103 578.[31]

Considering these limitations of DENM and MCM, as well as insights from research studies such as *Enhancing the Safety of Vulnerable Road Users: Messaging Protocols for V2X Communication*[32] and *Towards Cooperative VRUs: Optimal Positioning Sampling for Pedestrian Awareness Messages*[33], two key messaging protocols were identified as critical for improving the safety and protection of vulnerable road users (VRUs):

Collective Perception Messages (CPM)[34] and **VRU Awareness Messages (VAM)**[28]. Together, these protocols provide both passive and active mechanisms to improve situational awareness, reduce collisions, and foster safer road environments.

Collective Perception Messages (CPM): Local sensors on vehicles and roadside units passively detect VRUs. The collected data is shared through dedicated messages that include lists of VRUs and other objects, enabling enhanced situational awareness.

VRU Awareness Messages (VAM): VRUs actively broadcast messages to alert nearby road users of their presence, improving safety in their vicinity.

6.2.1.1. VRU Awareness Message (VAM)

VAM data is collected by devices embedded in various VRU equipment, such as handheld devices, bicycle computers, helmets, safety vests, baby strollers, or pet collars. This data includes parameters like position, heading, speed, lane position, acceleration, environmental conditions, angular dynamics, and device usage. Alternatively, a roadside unit (RSU) can detect VRUs through sensors and transmit VAM data on their behalf. In such cases, the RSU must be capable of identifying the type of VRU and determining details such as heading, speed, and acceleration.

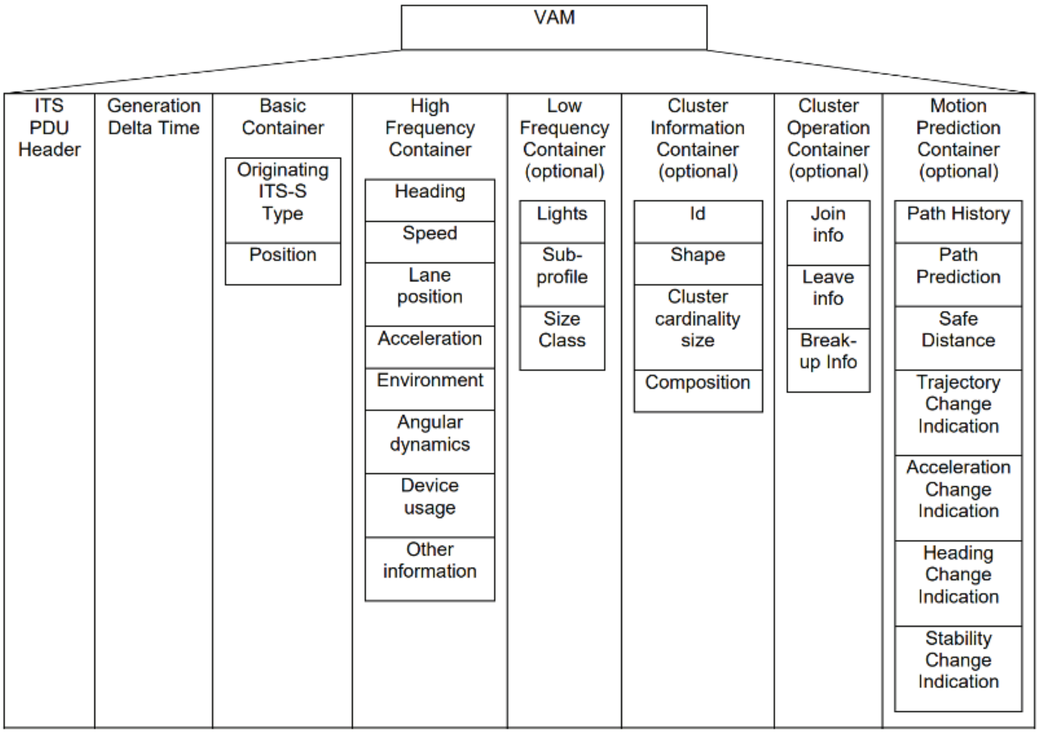
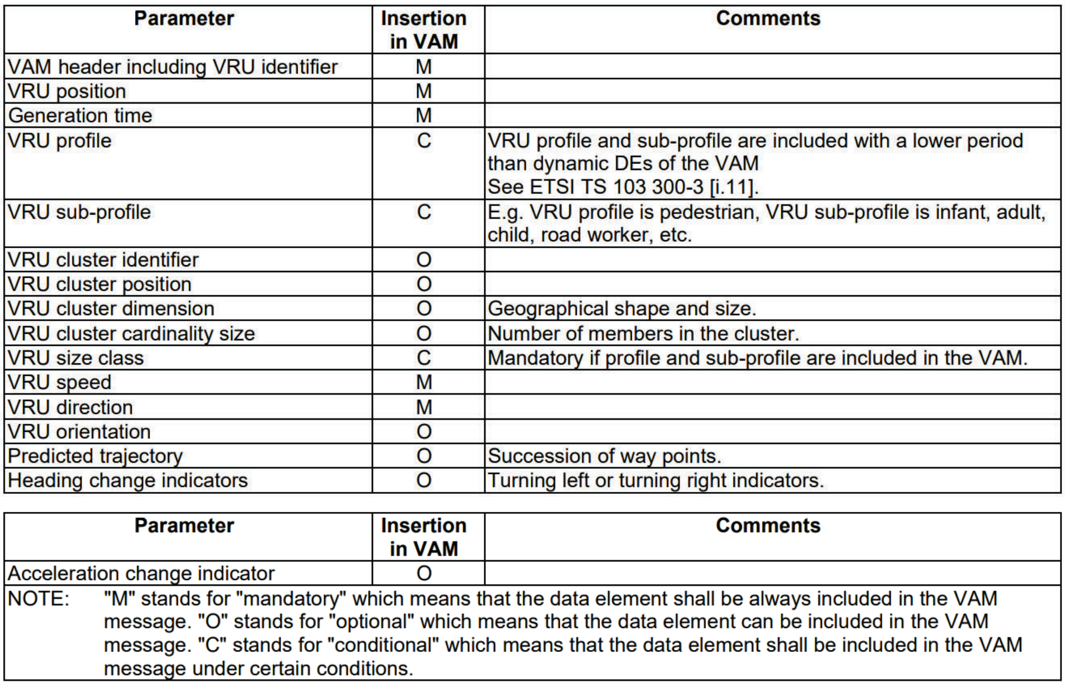


Figure8. General structure of a VAM [29]



Parameter	Insertion in VAM	Comments
VAM header including VRU identifier	M	
VRU position	M	
Generation time	M	
VRU profile	C	VRU profile and sub-profile are included with a lower period than dynamic DEs of the VAM See ETSI TS 103 300-3 [i.11].
VRU sub-profile	C	E.g. VRU profile is pedestrian, VRU sub-profile is infant, adult, child, road worker, etc.
VRU cluster identifier	O	
VRU cluster position	O	
VRU cluster dimension	O	Geographical shape and size.
VRU cluster cardinality size	O	Number of members in the cluster.
VRU size class	C	Mandatory if profile and sub-profile are included in the VAM.
VRU speed	M	
VRU direction	M	
VRU orientation	O	
Predicted trajectory	O	Succession of way points.
Heading change indicators	O	Turning left or turning right indicators.
Acceleration change indicator	O	
NOTE: "M" stands for "mandatory" which means that the data element shall be always included in the VAM message. "O" stands for "optional" which means that the data element can be included in the VAM message. "C" stands for "conditional" which means that the data element shall be included in the VAM message under certain conditions.		

Table 3. VAM data elements [28]

6.2.1.2. Collective Perception Messages (CPM)

Collective Perception Message (CPM) data is captured by vehicles or roadside units (RSUs) using sensors and then transmitted to nearby vehicles. CPM enables vehicles and infrastructure to perceive objects beyond their line of sight, such as around curves or behind buildings. Connected infrastructure or vehicles can detect non-connected vehicles and vulnerable road users (VRUs), sharing this information with others to enhance situational awareness.

CPM data includes the number of detected objects, unique object IDs, measurement time delays, and positions. Additional information, such as object speed and acceleration, can be included for improved performance.

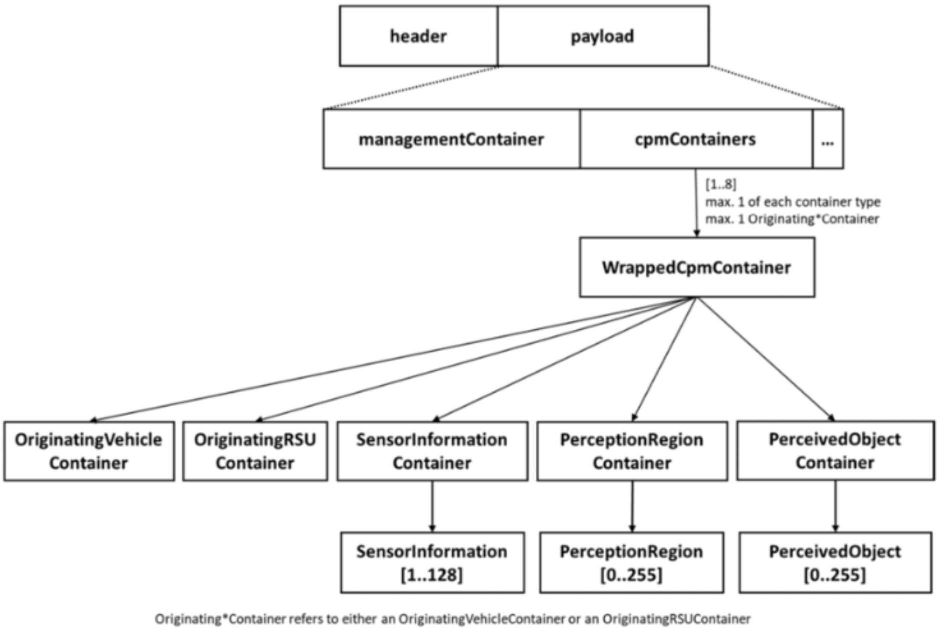

header
payload
managementContainer
cpmContainers
...
[1..8]
max. 1 of each container type
max. 1 Originating*Container
WrappedCpmContainer
OriginatingVehicle Container
OriginatingRSU Container
SensorInformation Container
PerceptionRegion Container
PerceivedObject Container
SensorInformation [1..128]
PerceptionRegion [0..255]
PerceivedObject [0..255]
Originating*Container refers to either an OriginatingVehicleContainer or an OriginatingRSUContainer

Figure9 General Structure of a CPM [34]

6.2.2. Evaluation of Minimum Data Requirements

To mitigate collision risks between vulnerable road users (VRUs) and motor vehicles, it is essential to obtain the position and motion dynamics of VRUs, including their trajectories and speeds. By integrating this data with information from the vehicle's onboard sensors, the motor vehicle can either alert the driver or autonomously execute evasive manoeuvres when necessary.

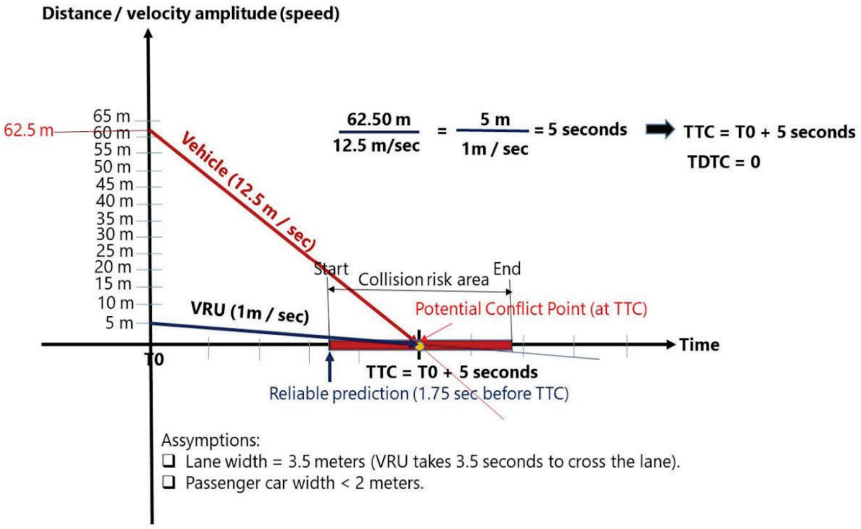


Figure10 Example of TTC Calculation [28]

6.2.3. Comparison of CPM and VAM

V2X Message Type	CPM	VAM
Message Origin	V2X-enabled smart infrastructure, V2X enabled vehicle	VRU with V2X capable devices, V2X-enabled smart infrastructure on behalf of the VRU.
Minimum set of data Required by V2X	Number of detected objects, a unique object ID, measurement time delay, Position	Type of the VRU, Heading, Speed, Acceleration, Lane position, Device usage.
Extra data for TTC calculations	Speed and Direction	-

Table4. Comparison between CPM and VAM messages

CPM is more suitable for our use case as it can consolidate information from multiple users into a single message, helping to reduce network congestion. Furthermore, vehicles can receive CPM messages from nearby vehicles and combine the data to create a more comprehensive situational awareness. In addition, RSU sensors can utilize CPM messages to detect non-V2X-enabled vehicles and transmit that information to V2X-equipped VRUs.

For this use case, the minimum data required by the roadside unit (RSU) is the accurate current time and position of the VRU. However, including additional information such as speed and acceleration can enhance performance.

Also note that it is feasible to use messages like DENM and MCM in conjunction with CPM to alert and prevent imminent collisions effectively.

6.2.4. Analysis of Real-World V2X Messages

To conduct our study effectively, acquiring the appropriate devices and equipment was critical. Initially, we sought to obtain V2X data from field-deployed devices. In this context, we initiated discussions with AstaZero, exploring potential collaboration to access sample data. AstaZero exclusively uses roadside units (RSUs) manufactured by Commsignia, having not employed devices from other vendors. While the Commsignia RSU model is relatively straightforward, it requires a licensing agreement for a proprietary software suite essential for application development. Moreover, AstaZero has developed its own proprietary C/C++ program to enable message reception into the RSU. However, due to the licensing restrictions and proprietary nature of the RSU, borrowing the unit from AstaZero for our study is not feasible.

Additionally, we recognize the importance of analyzing V2X messages, particularly Cooperative Perception Messages (CPM) containing data on Vulnerable Road Users (VRUs). To facilitate this, in the absence of our own test data, IEEE datasets from existing research were used. Our focus was on identifying real-world CPM messages that include meaningful VRU-related data.

We explored the *“A Multi-Modal Real-World Dataset of ETSI ITS V2X Messages in Public Road Traffic”* dataset[23], which comprises V2X data from 2,388 static stations and recordings from moving vehicles across 1,988 km. However, this dataset is limited to DENMs, MAPEMs, and SPATEMs, with **no CPM messages available**.

To address these limitations, we investigated alternative solutions, including open-source hardware, software, and simulation systems for RSUs.

Among the hardware solutions, we identified two devices from Nfiniity[35] suitable for V2X applications:

- **CUBE EVK**: A development kit designed for automotive and technology companies, comprising a V2X module, development board, and software development kit (SDK) for evaluating and developing V2X applications.

- **CUBE V2X**: A compact and lightweight V2X module integrating DSRC, Wi-Fi connectivity, sensors, and a microcontroller for processing and transmitting V2X data.

On the software side, we examined open-source frameworks such as:

1. **Vanetza Stack**: A highly customizable and extensible software framework for Vehicular Ad-hoc Networks (VANETs) and V2X communication. It includes libraries and tools for developing V2X applications, such as geonetworking, facilities, and application layers. Vanetza's modular design enables developers to add features and functionality easily.[36]

2. **Artery Framework**: A simulation software framework supporting V2X simulations based on ETSI ITS-G5 protocols, such as GeoNetworking and BTP. Artery enables equipping individual vehicles with multiple ITS-G5 services, providing common facilities for these services. It includes basic services like Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs). Licensed under GPL version 2, Artery permits both private and commercial usage.[37]

6.2.5. Assessment of Current Adoption and Limitations

We were unable to find any commercially available device capable of sending Vulnerable Road User (VRU) Awareness Messages (VAM). While there are C-V2X chipsets available, for example, from Qualcomm[38], the associated hardware remains in the development phase. Research projects like *Awareness Messages by Vulnerable Road Users and Vehicles: Field Tests via LTE-V2X*[39] have demonstrated the use of modified Onboard Units (OBUs) to transmit VAM messages; however, these systems are bulky and energy-intensive. Furthermore, we did not identify any Cooperative Perception Messages

(CPMs) containing VRU data in publicly available V2X datasets, potentially due to the computational complexity involved in VRU detection.

Challenges in V2X Deployment

A discussion of some prominent challenges in V2X deployment follows:

Lack of Standardized Public Key Infrastructure (PKI)

Based on our discussions with AstaZero and Halmstad University, as well as insights from the study *Operation of Public Key Infrastructures: State-of-the-art and best practices*[40] by the Conference of European Directors of Roads (CEDR), we observed that the adoption of a common EU PKI has not been achieved in most European countries. Challenges include decisions between national and European PKIs, cross-border data sharing, and PKI implementation and maintenance.

Vehicle manufacturers and regions relying on different PKIs, rather than a unified EU PKI, face interoperability issues that can hinder communication between vehicles and infrastructure.

Spectrum Allocation

The limited spectrum available for RSUs poses a challenge for V2X communication. Research like *Resource Allocation in V2X Communication: State-of-the-Art and Research Challenges*[41] highlights the competition from other industries for the same spectrum. Additionally, regulatory delays in allocating sufficient bandwidth in certain regions hinder the deployment and scalability of V2X systems.

Infrastructure Deployment Costs

The widespread deployment of infrastructure-to-vehicle (I2V) systems demands significant investment in RSUs and OBUs. According to the *Cost Analysis of V2I Deployment* report[42], the process is time-consuming and financially intensive, posing a barrier to large-scale adoption.

Interoperability

Ensuring interoperability between V2X systems across regions remains a key challenge. Studies such as *US-EU V2V V2I Message Set Standards Collaboration*[43] highlight differences in V2X deployment strategies between the US and EU, further complicating global standardization efforts.

Consumer Adoption Challenges

The adoption of V2X-enabled vehicles is slow due to the long lifecycle of existing vehicles. A report by the European Automobile Manufacturers Association[44] reveals that the average age of vehicles in the EU is 12.3 years, with older averages in countries like

Greece and Estonia (up to 17 years). This prolonged transition delays the full-scale implementation of V2X technology.

Regulatory and Policy Frameworks

Harmonizing regulatory and policy frameworks across European countries is critical for V2X success. This requires collaboration among stakeholders to create unified standards, which is currently a time-consuming and complex process.[45]

Privacy and Security Concerns

Securing V2X communications while maintaining user privacy is essential. Studies such as *A Survey of Security and Privacy Issues in V2X Communication Systems*[46] and *Security Issues and Challenges in V2X: A Survey*[47] highlight vulnerabilities in V2X systems, emphasizing the need for robust security mechanisms that do not compromise efficiency.

6.2.6. Consultation with Mattias Gudasic - CTO, Sigma Technology Embedded Group

Subject matter experts were consulted to provide further context and inform our findings.

The differences between the primary communication strategies for RSUs were explained, highlighting their respective advantages and shortcomings. The key takeaway was that IEEE 802.11p is emerging as the de facto industry standard and is therefore the recommended approach for communication. However, LTE remains a valuable alternative worth considering.

Mattias also pointed us to the most relevant ETSI standards related to communication standards and pointed out important differences in implementation between continents, e.g. North America and Europe.

6.2.7. Conclusions derived from the activities of WP3

It is feasible to alert vehicles using the existing ETSI V2X standards[25,34] without requiring any technological modifications. However, a limitation lies in the fact that vehicle manufacturers do not universally adopt the common EU PKI (ETSI EN 319 411-1), which may lead to a lack of trust in data transmitted by roadside units (RSUs).

Our research suggests that a minimum dataset required for generating effective V2X messages comprises the following elements:

- **Number of detected objects:** Providing a count of detected objects allows for an initial assessment of the traffic situation.
- **Unique object ID:** Assigning a unique identifier to each object enables tracking and differentiation of individual entities within the V2X communication stream.

- **Timestamp:** Including a precise timestamp ensures that the information is current and relevant for real-time decision-making.
- **Position:** Accurate positioning data, adhering to ETSI specifications, is crucial for establishing the location of objects within the traffic environment.
- **Speed:** Communicating the speed of objects allows for the prediction of their future movement and potential trajectory.
- **Direction:** Information about the direction of movement further enhances the understanding of object behavior and potential interactions.

This hypothesis, however, requires validation through real-world testing to assess its efficacy in terms of reliability, usefulness, and scalability. Field trials will provide valuable insights into the practical applicability of this minimum dataset and its ability to support robust and effective V2X communication for enhanced road safety and potential standardisation in the context of VRUs.

6.3. WP4: Evaluate policy and regulation for RSUs

This work package conducted a walk-through of the multifaceted legal, privacy, and ethical implications that arise from the utilization of diverse technologies within the framework of an open Roadside Unit (RSU) platform architecture, specifically tailored to the Swedish context. This analysis encompasses a wide array of legal considerations, including data protection regulations, privacy laws, and potential liabilities. Furthermore, it delved into the ethical dimensions associated with data collection, storage, and processing within the RSU ecosystem, needed to ensure compliance with established ethical guidelines and principles.

To address these, this work package also included interviews with stakeholders like the Traffic and Mobility Administration of Lund and Staffanstorps Kommun, and Future by Lund (An innovation platform for the smart, creative and sustainable societies of the future). We also consulted with subject matter experts regarding TIPPSS guidelines.

6.3.1. Legal Compliance

Traffic Laws and Regulations

Traffic laws and regulations ensure compliance with all relevant Swedish traffic laws and regulations, including those related to data collection, communication protocols, and vehicle-to-infrastructure (V2I) interactions. Key regulations in this area include:

General Data Protection Regulation (GDPR)[48]: This EU-wide regulation sets strict rules for the processing of personal data, including data collected in the context of traffic. It emphasizes the importance of data minimization, lawful processing grounds, and individual rights such as access, rectification, and erasure.

Swedish Data Protection Act[49]: This national legislation complements the GDPR, providing further specific rules for data processing in Sweden.

Camera Surveillance Act[50]: The Swedish Camera Surveillance Act (2018:1200) regulates the use of surveillance cameras in public spaces.

Key aspects of the Camera Surveillance Act are detailed below**:**

Permits: In most cases, authorities (and under limited circumstances private entities with similar duties) require a permit from the Swedish Authority for Privacy Protection to use camera surveillance in publicly accessible areas.
Changes to the Camera Surveillance Act will take effect on May 1, 2025. The amendments will simplify the installation of cameras in public areas by removing the permit requirement for municipalities and regions.

Comments from stakeholders in this regard include:

Lund: *The GDPR and Sweden's IMY make setting up cameras challenging because of the permit restrictions.*

Future by Lund: *When it comes to mandates for changes in the streets, the Kommun (municipality) has significant authority over their own roads. However, it's important to know which party owns which roads, as some roads are owned by Trafikverket (the Swedish Transport Administration). For instance, in Veberöd, there's a main street owned by Trafikverket, but after a certain point, it transitions to Kommun ownership. Ownership shifts depending on the road, and for streets inside the city, they are typically owned by the Kommun.*

Legal basis: Camera surveillance must have a legal basis, such as preventing crime, protecting public safety, or maintaining order. Legal basis for camera surveillance in Traffic Safety encompasses monitoring traffic flow, intersections, and pedestrian crossings to ensure the safety of all road users.

Proportionality: The use of cameras must be proportionate to the intended purpose.

Data protection: The act emphasizes the importance of data protection principles, such as data minimization and the rights of individuals.

Liability and Insurance: Analyze liability and insurance considerations related to data usage, system failures, and potential accidents involving the RSU platform.

Intellectual Property Rights: Evaluate and address intellectual property rights issues related to the use of open-source software, algorithms, and data within the platform.

6.3.2. Data Privacy:

GDPR Compliance: Analyze data collection, processing, and storage practices within the RSU platform to ensure strict adherence to the General Data Protection Regulation (GDPR). This includes:

Data Minimization: Ensure only necessary data is collected and processed.

Future by Lund: *In our project's cameras are used for detecting objects and identifying them as road users while complying fully with GDPR. The data collected is broad and non-specific, such as counting humans, cycles, and bikes, without collecting personal data. For instance, the system only sends out aggregated data like "50 new cars in the last five minutes". There was a case where collecting license plate numbers was considered, but it was not implemented due to GDPR concerns. The plan was to store the data for five minutes and then discard it. The key is to keep the data general and avoid collecting specific details about individuals.*

Purpose Limitation: Clearly define the purposes for data collection and use.

Staffanstorp*: Using cameras for traffic data collection is generally acceptable under GDPR, as long as it respects privacy regulations. Drones are sometimes used by third-party contractors for traffic counting, which is also considered an appropriate use of technology. However, it's crucial to avoid collecting any personally identifiable information, as that would violate GDPR.*

Data Subject Rights: Guarantee individuals' rights to access, rectify, erase, and restrict the processing of their data.

6.3.3. Data Security

Cybersecurity Threats: Identify potential cybersecurity threats to the RSU platform, including hacking, data breaches, and denial-of-service attacks.

Security Measures: Recommend and implement robust security measures, such as encryption, intrusion detection systems, and access control mechanisms, to safeguard the platform and user data.

Vulnerability Assessment: Regularly conduct vulnerability assessments and penetration testing to identify and address security weaknesses.

6.3.4. Ethical Considerations

Fairness and Equity: Ensure the RSU platform is designed and implemented in a fair and equitable manner, avoiding any potential biases or discriminatory outcomes.

Transparency and Accountability: Promote transparency and accountability in all aspects of the RSU platform, including data collection, processing, and usage.

Public Trust: Build and maintain public trust in the RSU platform by demonstrating a commitment to privacy, security, and ethical considerations.

Future by Lund: *A public sign with a QR code was displayed in Veberöd as part of a sensor project. The QR code directed to a website that explained the project and how the data was being managed.*

6.3.5. Consultation with Oscar Amador Molina - Postdoctoral Fellow at Center for Research on Embedded Systems, Halmstad University

Subject matter experts were consulted to provide further insight into privacy and security considerations.

One of the key challenges highlighted was the delicate balance between trust and privacy. Increasing the number of sensors in ITS can enhance trust by improving data reliability, while simultaneously raising privacy concerns, as more sensors increases the likelihood of tracking sensitive information such as license plates. This underscores the need for robust privacy-preserving mechanisms, such as anonymization and tokenization, to prevent long-term tracking while maintaining trust in the system's accuracy.

Another topic discussed was the issue of message validity, and the tension between trust and privacy. For example, messages about roadworks can improve safety when accurate, but anyone could potentially send false messages, which could lead to confusion or hazardous situations. To mitigate this, systems must prioritize mechanisms that allow trusted authorities, such as traffic authorities or police, to invalidate false or rogue messages in real time. Certification authorities will have a critical role, as well as the management of trusted nodes, where devices associated with verified authorities are granted higher priority in the communication hierarchy.

There are also challenges in determining whether a sensor is reliable, and whether the data can be trusted even if it originates from a trusted device. For example, an RSU may detect a VRU as a person, while a truck's OBU classifies the same VRU as a person on a scooter. Such discrepancies lead to redundant and/or conflicting information. In such a case it might be better to have an undefined classification of the VRU, as either way they are equally vulnerable. Although this approach may sacrifice some precision, it ensures information remains actionable and consistent.

Oscar pointed us to the most relevant and recent ETSI standards related to TIPPSS.

6.3.6. Regulatory Challenges and Stakeholder Perspectives on Computer Vision in Traffic Safety Systems

Engagement with various municipalities and stakeholders in the traffic safety systems domain reveals that strict regulations related to GDPR, and personal privacy significantly influence the setup of computer vision systems or cameras for such purposes. Notably, interpretations of permission requirements differ based on the level of familiarity with these systems.

We identified these distinct scenarios:

Scenario 1: High Domain Familiarity

Entities with extensive experience in computer vision projects and a deep understanding of the regulatory framework indicate that traffic-related projects do not necessitate the collection of personally identifiable data. In these cases, the information gathered is typically demographic in nature—for example, counts of vehicles, cyclists, and pedestrians. To remain compliant with regulations, it is essential to ensure that:

- No personally identifiable information is collected.
- Images are either discarded or processed locally (without leaving the primary device) after extracting the necessary demographic or statistical data.

Adherence to these principles is critical for securing permissions from the relevant authorities.

Scenario 2: Limited Domain Familiarity

Entities with less experience in traffic safety projects involving computer vision have expressed several common observations:

- GDPR and Sweden's Integritetsskyddsmyndigheten (IMY) regulations are viewed as complicating the implementation of camera systems.
- The reliance on historical data from the Swedish accident database 'Strada' for accident analysis is considered inefficient for future road safety planning.
- Some manufacturers rebrand cameras as "sensors" with specific safety classifications to streamline compliance.
- There is a tendency to delegate GDPR-related responsibilities to project implementers, often perceiving these requirements as a bureaucratic challenge.

This variation in understanding and interpretation of GDPR requirements may act as a barrier to the broader adoption of computer vision technologies for traffic safety initiatives.

6.3.7. Conclusions derived from the activities of WP4

Leveraging advanced ITS technologies for road safety in Sweden requires a deep understanding of its robust privacy regulations. This ensures that stakeholders can effectively balance innovation with compliance, fostering the ethical and secure application of technology to protect individuals.

Trust, Identity, Privacy, Protection, Safety, and Security (TIPPSS) are critical factors in the development and deployment of I2V communication systems, especially when integrating advanced sensor technologies for VRU safety. Addressing these aspects is essential to ensure the reliability, acceptance, and long-term success of any solution. While the principles of TIPPSS are integral to the success of sensor-based I2V systems, a comprehensive analysis of these factors requires extensive evaluation across technical, legal, and operational domains. Given the scope of this early-stage research, an in-depth TIPPSS assessment is beyond the current focus but remains a valuable direction for future work.

7. Dissemination and publications

7.1. Dissemination

How are the project results planned to be used and disseminated?	Mark with X	Comment
Increase knowledge in the field	X	The prestudy has provided valuable insights into the gaps within the existing technological environment and a deeper understanding of the feasibility of addressing these gaps.
Be passed on to other advanced technological development projects	X	The findings from the prestudy can serve as a foundation for further developing the concepts explored here.
Be passed on to product development projects	X	The concept of vendor agnostic RSU platforms has the potential to be developed into a product.
Introduced on the market		
Used in investigations / regulatory / licensing / political decisions	X	Exploring a messaging standard between DUs and RSUs to facilitate V2X communication within the VRU protection framework is worthwhile.

7.2. Publications

There are no publications produced for this pre-study apart from this report.

8. Conclusions and future research

8.1. Conclusions

The pre-study has provided deeper insight into the problem area of protecting Vulnerable Road Users using I2V technology.

While existing standards from the surveillance industry can facilitate communication between Detection Units and Roadside Units (RSUs), there is a clear need to develop communication standards tailored specifically for VRU protection. Further research in this area could lead to the evolution of more minimal and targeted message structures, enhancing efficiency and interoperability.

Standardization in this domain has the potential to promote open architectures for RSUs, encouraging wider adoption and improving cost-effectiveness.

Additionally, vehicles can be alerted using existing ETSI V2X standards without requiring technological modifications. However, a significant challenge remains: the lack of universal adoption of the common EU PKI (ETSI EN 319 411-1) by vehicle manufacturers. This inconsistency could undermine trust in data received from RSUs, posing a barrier to effective implementation.

8.2. Limitations

As a pre-study, this project was conducted within a limited scope, despite efforts to broadly address all pertinent issues. Our investigation into aspects of TIPPSS represents only an initial exploration that nonetheless provides a foundational framework for the project. Additionally, the review of existing standards relevant to the DU-RSU communication space is not exhaustive.

While the use of donated AXIS Communications devices in WP2 enabled us to demonstrate the efficacy of using standards like ONVIF for transmitting VRU safety messages, this reliance on a single vendor's equipment represents a key limitation of the study. While we are grateful for their generous donation, using equipment from a single vendor compromises the vendor neutrality objective of this research. Future work should prioritize procuring devices from a range of vendors to ensure broader applicability and more robust results.

8.3. Future Research

Given the complexity of this landscape, extensive future research is required.

This study underscores the importance of further field research to validate the concepts explored. A key next step is to develop a proof-of-concept system. This system would demonstrate the feasibility of integrating various Detection Units (DUs) with an open architecture RSU in real-time, showcasing its potential to enhance road safety and traffic efficiency through the timely and accurate dissemination of data to vehicles. Further research utilizing this proof-of-concept system could investigate different communication protocols between the RSU and DUs to analyse their latency, flexibility, reliability, and scalability.

Furthermore, future studies should define and implement a minimum set of event data necessary for effective I2V communication, establishing its efficacy in real-world scenarios. Further studies should also explore the feasibility of a standardized DU-RSU communication protocol for road safety applications. This exploration could involve analyzing real-world Collective Perception Messages (CPMs) collected from vehicles equipped with V2X technology to better understand VRU use cases and optimize communication strategies for enhanced safety and efficiency.

9. Participating parties and contact persons

Party	Logo	Contact
Mittlogik Solutions	MITTLOGIK	Sudha Padmanabhan sudha.padmanabhan@mittlogik.se Phone: +46 76 022 92 36
Sigma Technology Embedded Network	SIGMA Technology	Danilo Chinchilla danilo.chinchilla@sigmatechnology.com Phone: +46 70 988 57 61
RISE	RI. SE	Maria Ulan maria.ulan@ri.se Phone: +46 10 228 41 87

References

1	Transportstyrelsen (2025) *210 personer omkom i vägtrafiken 2024*. Available at: https://www.transportstyrelsen.se/sv/om-oss/pressrum/nyhetsarkiv/2025/210-personer-omkom-i-vagtrafiken-2024 (Accessed: 28 Jan. 2025).
2	Trafikverket. (n.d.). *Vision Zero - no fatalities or serious injuries through road accidents*. Retrieved from https://www.roadsafetysweden.com/about-the-conference/vision-zero---no-fatalities-or-serious-injuries-through-road-accidents/ (Accessed 26 Feb. 2025).
3	European Telecommunications Standards Institute (ETSI) (2019) *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*. ETSI.
4	Nordic Way (2023) *Nordic Way 3 – Final Report*. Available at: https://nordicway.dk/kunde/ (Accessed: 29 Jan. 2025).
5	5G Automotive Association (5GAA). (n.d.). *5GAA*. Retrieved from https://5gaa.org/ (Accessed 18 Feb. 2025).
6	5GAA (2025) *C-V2X Roadmap White Paper*, 5G Automotive Association. Available at: https://5gaa.org/content/uploads/2025/01/5gaa-wi-cv2xrm-iii-roadmap-white-paper.pdf (Accessed: 31 Jan. 2025).
7	Car-2-Car Communication Consortium (C2C-CC) (2023) *Roadmap: Day 2 and Beyond (Version 1.2)*. Available at: https://www.car-2-car.org/fileadmin/documents/General_Documents/C2CCC_WP_2072_RoadmapDay2AndBeyond_V1.2.pdf (Accessed: 31 Jan. 2025).
8	Autotalks (2022) *VRU Protection: Saving Lives with Vehicle-to-Vulnerable Road User Communication.* Available at: https://auto-talks.com/wp-content/uploads/2022/05/VRU-protection-3.pdf (Accessed: 28 Jan. 2025).
9	MittLogik Solutions AB, Sigma Technology Embedded Network and RISE. (2024). *Safer Crossways using I2V*. Application submitted to Vinnova for the project call Traffic-Safe Automation - FFI - Spring 2024.
10	Santos, D., Silva, J. and Rodrigues, J. (2018). *Enabling trust and security: TIPPSS for IoT*. ResearchGate. Available at: https://www.researchgate.net/publication/324548774_Enabling_Trust_and_Security_TIPPSS_for_IoT (Accessed: 31 Jan. 2025).
11	ONVIF. (n.d.). *About ONVIF*. Available at: https://www.onvif.org/about-onvif/ (Accessed 3 Feb. 2025).

12	Axis Communications. (n.d.). *AXIS Q1656-DLE*. Available at: https://www.axis.com/products/axis-q1656-dle (Accessed: 31 Jan. 2025).
13	Axis Communications. (n.d.). *AXIS D2210-VE Radar*. Available at: https://www.axis.com/products/axis-d2210-ve-radar (Accessed: 31 Jan. 2025).
14	Axis Communications. (n.d.). *AXIS D4100-E Network Strobe Siren*. Available at: https://www.axis.com/products/axis-d4100-e-network-strobe-siren (Accessed: 31 Jan. 2025).
16	MQTT.org. (2024). *MQTT - The Standard for IoT Messaging*. Available at: https://mqtt.org/ (Accessed 29 Jan. 2025).
17	RISE. (n.d.). *AstaZero*. Available at: https://astazero.ri.se/ (Accessed 31 Jan. 2025).
18	Commsignia. (n.d.). Available at: https://www.commsignia.com/ (Accessed 31 Jan. 2025).
19	Boustedt, K., Ronelöv, E., Westling, M. and Blidkvist, J. (2023). *V2X and connected infrastructure - V2X2*. Project within FFI TSAF Dec 2019. Vinnova. Available at: https://www.vinnova.se/en/p/v2x-and-connected-infrastructure---v2x2/ (Accessed 3 Feb. 2025).
20	ONVIF. (n.d.). *ONVIF Profile M Specification v1.1*. Available at: https://www.onvif.org/wp-content/uploads/2024/04/onvif-profile-m-specification-v1-1.pdf (Accessed 31 Jan. 2025).
21	ROS Wiki. (n.d.). *Documentation*. Available at: https://wiki.ros.org/Documentation (Accessed 31 Jan. 2025).
22	micro-ROS. (n.d.). Available at: https://micro.ros.org/ (Accessed 31 Jan. 2025).
23	Kueppers, G., Busch, J.-P., Reiher, L. and Eckstein, L. (2024) *A multi-modal real-world dataset of ETSI ITS V2X messages in public road traffic* [Dataset]. RWTH Aachen University, Germany. Available at: https://v2aix.ika.rwth-aachen.de/ (Accessed 9 December 2024) and https://arxiv.org/pdf/2403.10221 (Accessed 9 Dec. 2024).
24	RobotShop. (n.d.). *ROS Compatible Robots & Parts*. Available at: https://eu.robotshop.com/collections/ros-compatible-robots-parts (Accessed 27 Jan. 2025).
25	The Construct. (n.d.). *Available ROS2 Hardware*. Available at: https://www.theconstruct.ai/82-available-ros2-hardware/ (Accessed 27 Jan. 2025).
26	IntelRealSense. (n.d.). *realsense-ros*. Available at: https://github.com/IntelRealSense/realsense-ros (Accessed 27 Jan. 2025).
27	kimsooyoung. (n.d.). *mmwave_ti_ros*. Available at: https://github.com/kimsooyoung/mmwave_ti_ros (Accessed 27 Jan. 2025).

28	ETSI (2024) *Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 2: Functional Architecture and Requirements definition; Release 2*. ETSI TS 103 300-2 V2.3.1. Available at: https://www.etsi.org/deliver/etsi_ts/103300_103399/10330002/02.03.01_60/ts_10330002v020301p.pdf (Accessed 13 Jan. 2025).
29	ETSI (2023) *Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 3: Specification of VRU awareness basic service; Release 2*. ETSI TS 103 300-3 V2.2.1. Available at: https://www.etsi.org/deliver/etsi_ts/103300_103399/10330003/02.02.01_60/ts_10330003v020201p.pdf (Accessed 13 Jan. 2025).
30	ETSI (2014) *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service*. ETSI EN 302 637-3 V1.2.1. Available at: https://www.etsi.org/deliver/etsi_en/302600_302699/30263703/01.02.01_30/en_30263703v010201v.pdf (Accessed 13 Jan. 2025).
31	ETSI (2024) *Intelligent Transport Systems (ITS); Vehicular Communications; Manoeuvre Coordination Service (MCS); Pre-standardization study; Release 2*. ETSI TR 103 578 V2.1.1. Available at: https://www.etsi.org/deliver/etsi_TR/103500_103599/103578/02.01.01_60/tr_103578v020101p.pdf (Accessed 13 Jan. 2025).
32	Lobo, S., Festag, A. and Facchi, C. (2022) 'Enhancing the safety of vulnerable road users: Messaging protocols for V2X communication', *IEEE Vehicular Technology Magazine*, 17(3), pp. 119-119. doi: 10.1109/MVT.2022.3182044.
33	Martín-Pérez, J., Amador, O., Rydeberg, M., Olsson, L. and Vinel, A. (2023) 'Towards cooperative VRUs: Optimal positioning sampling for pedestrian awareness messages', *arXiv*. Available at: https://arxiv.org/abs/2312.14072v1 (Accessed 13 Jan. 2025).
34	ETSI (2023) *Intelligent Transport System (ITS); Vehicular Communications; Basic Set of Applications; Collective Perception Service; Release 2*. ETSI TS 103 324 V2.1.1. Available at: https://www.etsi.org/deliver/etsi_ts/103300_103399/103324/02.01.01_60/ts_103324v020101p.pdf (Accessed 9 Dec. 2024).
35	nfiniity GmbH (n.d.) *Products*. Available at: https://www.nfiniity.com/#portfolio (Accessed 3 Feb. 2025).
36	Vanetza (n.d.) *Open-source implementation of the ETSI C-ITS protocol suite*. Available at: https://www.vanetza.org/ (Accessed 3 Feb.. 202).
37	Artery (n.d.) *V2X ETSI ITS-G5 protocols simulations*. Available at: http://artery.v2x-research.eu/ (Accessed 3 Feb. 2025).

38	Qualcomm Technologies, Inc. (2024) *C-V2X: Cellular Vehicle-to-Everything*. Available at: https://www.qualcomm.com/products/automotive/c-v2x (Accessed 9 Dec. 2024).
39	Lusvarghi, L., Grazia, C.A., Klapez, M., Casoni, M. and Merani, M.L. (2023) 'Awareness messages by vulnerable road users and vehicles: Field tests via LTE-V2X', *IEEE Transactions on Intelligent Vehicles*, 8(10), pp. 4418-4433. doi: 10.1109/TIV.2023.3280744.
40	Trusted Integrity and Authenticity for Road Applications (2024) *Operation of Public Key Infrastructures: State-of-the-art and best practices*. Available at: https://www.cedr.eu/docs/view/671a13dc92f58-en (Accessed 12 Dec. 2024).
41	Nair, A. and Tanwar, S. (2024) 'Resource allocation in V2X communication: State-of-the-art and research challenges', *Physical Communication*, 64(102351). doi: 10.1016/j.phycom.2024.102351.
42	Nokes, T., Baxter, B., Scammell, H., Naberezhnykh, D. and Provvedi, L. (2020) *Cost analysis of V2I deployment*. Available at: https://5gaa.org/content/uploads/2020/09/5GAA_Ricardo-Study-V2I-Cost-Analysis_Final_110820.pdf (Accessed 9 Dec. 2024).
43	Bai, S. (2013) *US-EU V2V V2I message set standards collaboration*. Available at: https://docbox.etsi.org/workshop/2014/201402_ITSWORKSHOP/S02_ITS_SomeBitsFromtheWorld/HONDA_BAI.pdf (Accessed 9 Dec. 2024).
44	European Automobile Manufacturers' Association (2024) *Vehicles on European roads*. Available at: https://www.acea.auto/files/ACEA-Report-Vehicles-on-European-roads-.pdf (Accessed 9 Dec. 2024).
45	European Commission. (n.d.). *Intelligent Transport Systems - Cooperative, Connected and Automated Mobility (ITS-CCAM) and Electromobility (RP2020) - Interoperable Europe*. Retrieved from https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation/intelligent-transport-systems-cooperative-connected-and-automated-mobility-its-ccam-and (Accessed 18 Feb. 2025)
46	Yoshizawa, T., Singlee, D., Muehlberg, J.T., Delbruel, S., Taherkordi, A., Hughes, D. and Preneel, B. (2023) 'A survey of security and privacy issues in V2X communication systems', *ACM Computing Surveys*, 55(9), pp. 1-36. doi: 10.1145/3558052.
47	Ghosal, A. and Conti, M. (2020) 'Security issues and challenges in V2X: A survey', *Computer Networks*, 169. doi: 10.1016/j.comnet.2019.107093.
48	European Parliament and Council. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Available at:

	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Accessed 31 Jan 2025).
49	*Lag (2018:218) med kompletterande bestämmelser till EU:s förordning om skydd för fysiska personer med avseende på behandling av personuppgifter och om fritt flöde av personuppgifter och om upphävande av direktiv 95/46/EG (dataskyddslag)* [Swedish Data Protection Act (2018:218)]. (2018). Available at: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218/ (Accessed 31 Jan. 2025).
50	Svensk författningssamling, 2018. *Kamerabevakningslag (2018:1200)*. Available at: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/kamerabevakningslag-20181200_sfs-2018-1200/ (Accessed 31 Jan. 2025).

Glossary

Term	Definition
Intelligent Transportation Systems (ITS)	ITS aims to provide services that enhance the safety, efficiency, and sustainability of transportation systems. They leverage advanced telematics and hybrid communications, including IP-based communications and Ad-Hoc direct communication between vehicles and infrastructure. Benefits of ITS ● Improved Safety: ITS can reduce accidents and improve road safety. ● Increased Efficiency: ITS can optimize traffic flow and reduce congestion. ● Environmental Benefits: ITS can reduce emissions and promote sustainable transportation. ● Enhanced User Experience: ITS can provide real-time information and improve the overall travel experience. As ITS continues to evolve, we can expect to see new and innovative applications that improve the safety, efficiency, and sustainability of transportation systems.
Cooperative-ITS (C-ITS)	C-ITS is a key component of ITS, enabling vehicles to communicate with each other and with infrastructure. This technology has the potential to greatly improve road safety and efficiency, and is a crucial step towards the realization of autonomous driving.
Roadside Units (RSUs)	Roadside Units (RSUs) are a component of Intelligent Transportation Systems (ITS) and connected vehicle environments, serving as communication hubs that facilitate data exchange between vehicles and infrastructure. Equipped with technologies like DSRC or C-V2X, RSUs provide wireless connectivity, process and analyze data from various sources, and support traffic management and safety applications. By relaying real-time information about road conditions, traffic congestion, and accidents, and broadcasting alerts about potential hazards, RSUs play a vital role in creating a seamless and intelligent transportation network that integrates with road users, traffic lights, road signs, and other infrastructure components. [https://www.isarsoft.com/knowledge-hub/rsu]
V2X (Vehicle-to-Everything)	V2X (Vehicle-to-Everything) communications refer to the technology that enables vehicles to communicate with other vehicles, infrastructure, pedestrians, and other entities in their surroundings. This technology allows vehicles to share information and coordinate their actions to improve safety, efficiency, and convenience. V2X communications involve the exchange of data between vehicles and other entities, such as:

- Vehicle-to-Infrastructure (V2I) - e.g. traffic lights, lane markers and parking metres.
- Vehicle-to-Device (V2D) - Bluetooth / WiFi-Direct, e.g. Apple's CarPlay and Google's Android Auto.
- Vehicle-to-Grid (V2G) - information exchange with the smart grid to balance loads more efficiently.
- Vehicle-to-Building (V2B), also known as Vehicle-to-Home (V2H)
- Vehicle-to-Load (V2L) - use the large battery in an electric vehicle to power or charge something else
- Vehicle-to-Network (V2N) - communication based on Cellular (3GPP) / 802.11p.
- Vehicle-to-Cloud (V2C) - e.g. OTA updates, remote vehicle diagnostics (DoIP).
- Vehicle-to-Pedestrian (V2P) - Pedestrian and bicycles, vulnerable road users (VRUs)
- Vehicle-to-Vehicle (V2V) - real-time data exchange with nearby vehicles.

There are different technologies used for Vehicle-to-Everything (V2X) messages. One technology is WLAN-based, specifically Dedicated Short-Range Communications (DSRC), which is a mature technology that offers short-range communication with less latency, but requires more new infrastructure. Another technology is Cellular-based, known as Cellular Vehicle-to-Everything (CV2X), which utilizes LTE/5G technology.

Different V2X messages by ETSI

- Basic Safety Messages (BSMs): These contain critical safety information like position, speed, and acceleration.
- Maneuver Coordination Messages MCM - vehicles to know what other vehicles intend to do ahead of time. [https://www.etsi.org/deliver/etsi_TR/103500_103599/103578/02.01.01_60/tr_103578v020101p.pdf]
- Cooperative Adaptive Cruise Control CACC [https://www.etsi.org/deliver/etsi_tr/103200_103299/103299/02.01.01_60/tr_103299v020101p.pdf]
- Decentralized Environmental Notification Messages (DENMs): Used for hazard warnings (e.g., accidents, roadwork). [https://www.etsi.org/deliver/etsi_en/302600_302699/30263703/01.02.01_30/en_30263703v010201v.pdf]
- Traffic Signal Phase and Timing Messages (SPaT): Provide traffic signal status [https://www.etsi.org/deliver/etsi_ts/103100_103199/10319101/01.01.01_60/ts_10319101v010101p.pdf]
- Map Data Messages: Include road maps and lane information.[https://www.etsi.org/deliver/etsi_tr/102800_102899/102863/01.01.01_60/tr_102863v010101p.pdf]

	● Periodic Cooperative Awareness Messages (CAMs): Regularly broadcast information about nearby vehicles and infrastructure.[https://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.03.01_30/en_30263702v010301v.pdf] ● Collective Perception Messages - CPM [https://www.etsi.org/deliver/etsi_ts/103300_103399/103324/02.01.01_60/ts_103324v020101p.pdf] ● Messages For Vulnerable Road Users VRU - VAM [https://www.etsi.org/deliver/etsi_ts/103300_103399/10330002/02.01.01_60/ts_10330002v020101p.pdf] ● And more….
Vulnerable Road Users (VRUs)	Vulnerable Road Users (VRUs) refer to individuals who are more susceptible to injury or harm while using the road, due to their lack of protection or limited ability to defend themselves. Examples of VRUs include: **VRU Profile 1 -** Pedestrian. Typical VRUs in this profile: pedestrians, i.e. road users not using a mechanical device for their trip. It includes for example pedestrians on a pavement, but also children, prams, disabled persons, blind persons guided by a dog, elderly persons, persons walking beside their bicycle. **VRU Profile 2 -** Bicyclist. Typical VRUs in this profile: bicyclists and similar e.g. light vehicles riders,possibly with an electric engine. It includes bicyclists, but also wheelchair users, horses carrying a rider, skaters, e-scooters, personal transporters, etc. **VRU Profile 3 -** Motorcyclist. Typical VRUs in this profile: motorcyclists, which are equipped with engines that allow them to move on the road. It includes users (driver and passengers, e.g. children and animals) of Powered Two Wheelers (PTW) such as mopeds (motor scooters), motorcycles or side-cars. **VRU Profile 4 -** Animals presenting a safety risk to other road users. Typical VRUs in this profile: dogs, wild animals, horses, cows, sheep, etc. Some of these VRUs might have their own ITS-S (e.g. dog in a city or a horse) but most of the VRUs in this profile will not be able to send the VAM and only be indirectly detected, especially wild animals in rural areas and highway situations.

Trust and Identity	Ensuring that data transmitted between sensors, RSUs, and vehicles originates from verified and trusted sources is crucial. Misidentification or spoofing of devices could lead to false alerts or security vulnerabilities. It is vital to establish trusted identities for all connected components to prevent spoofing or manipulation of data. Using Public Key Infrastructure (PKI) with robust certificate management is essential to validate the authenticity of devices and their messages. Integrating this into the RSU architecture will help guarantee that alerts and warnings originate from verified sources, mitigating the risks of misinformation and enhancing system reliability. However, even with trusted devices, the reliability of the information is also an issue. How can we trust that the data sent for a trusted device is reliable? If two different devices classify the same object differently, which one do we trust?
Privacy	The use of sensor data, especially when detecting VRUs, must comply with data protection regulations to safeguard individual privacy. This includes managing how location data and behavioral patterns are collected, processed, and shared. The data from the RSUs should only be composed of metadata, and should exclude any personally identifiable information (PII). Adopting edge computing principles - processing sensitive data locally on the RSU before anonymized transmission - aligns with GDPR. This should minimize privacy risks while still enabling advanced analytics.
Protection and Security	Safeguarding the system against cyber threats is vital. Unauthorized access or tampering with RSU communications could compromise system integrity and endanger road users. Secure communication protocols and regular system updates are necessary to mitigate these risks. Blockchain to ensure no data manipulation? ITS recommends using end-to-end encryption, secure boot mechanisms and regular firmware updates to ensure system integrity. Implementing blockchain for secure logging of RSU events could enhance data integrity by providing tamper-proof records.
Safety	The core objective of the project is to enhance safety for VRUs. This requires that all integrated systems operate reliably and deliver timely, accurate information to prevent collisions. Otherwise they can risk becoming distractions.Testing protocols should be implemented to ensure all integrated components operate within strict safety thresholds, particularly in scenarios with limited visibility or high traffic complexity.