PRISSMA Project
Plateforme de Recherche et d'Investissement pour la Sûreté
et la Sécurité de la Mobilité Autonome
04/2021 - 04/2024

[L5.4] INTEROPERABILITY AND PERFORMANCE OBJECTIVES FOR AUTONOMOUS VEHICLE SYSTEMS

DEFINITION DES OBJECTIFS DE D'INTEROPERABILIE ET PERFORMANCE DANS LES ECOSYSTEMES VEHICULAIRES

AUTONOMES

Main author: Sammy HADDAD

Keywords: Communication, V2X, Interoperability, Objectives, Validation

Abstract. In this deliverable, we present ideas for identifying performance and interoperability requirements, as well as evaluation objectives for autonomous vehicle systems. Since no resources were allocated to the task, this document does not provide a full analysis but rather offers guidance and illustrations on how to proceed.

Résumé. Dans ce livrable, nous présentons des idées pour identifier les exigences de performance et d'interopérabilité, ainsi que les objectifs d'évaluation pour les systèmes de véhicules autonomes. Étant donné qu'aucune ressource n'était initialement allouée à cette tâche, ce document ne fournit pas une analyse complète mais offre des indications sur la marche à suivre.

[L5.4] interoperability and performance objectives for autonomous vehicle systems

Table of content

[L5.4] interoperability and performance objectives for autonomous vehicle systems

1 INTRODUCTION

Communication performance and interoperability will be key to future ARTS enhancement. ARTS are not only composed of an autonomous vehicle; they consist of a complete set of architecture components that manage and provide information to the vehicle to enhance overall traffic efficiency, as well as user security and safety.

Use cases such as safe intersection crossing or pedestrian safety (at bus stops, near schools, etc.), where vehicle sensors alone cannot perceive all potential safety hazards, will require real-time information sharing between vehicles, vehicles and the infrastructure, and so on, to help the vehicle gain a better understanding of the current situation.

Ensuring reliable real-time communication and interoperability between the wide variety of potential actors involved in safety-critical use cases is essential. For this, evaluation objectives must be defined by a comprehensive safety and security evaluation methodology for ARTS.

This deliverable will discuss the most important factors to consider when designing such evaluation objectives. Specifically, we will address the following points:

- Minimal requirements related to real-time constraints
- Realistic validation
- Interoperability validation

Project resource limitations do not allow us to provide a detailed set of requirements, but we offer some guidance on how to develop them.

[L5.4] interoperability and performance objectives for autonomous vehicle systems

2 MINIMAL REQUIREMENTS RELATED TO REAL-TIME CONSTRAINTS

2.1 Communications: Definition of thresholds vs limits identifications

2.1.1. Risk analysis based threshold identifications

The reason to evaluate some communication performances is clearly to avoid risk and mitigate dangerous situations. But for that, one needs to identify those situations. For autonomous vehicles, the most obvious risk to avoid is a collision, either with another vehicle or, worse, with other vulnerable road users (pedestrians, cyclists, scooters, etc.).

To avoid such risks, it is necessary to identify what information exchange should prevent the incident:

- Data to be shared to avoid the incident
- Source of the data acquisition
- Communication path to be followed by the data

Generic studies should be performed on main C-ITS use cases to try to identify these limits based on standardized architecture and communication methods (such as the default architecture presented in deliverable 5.2). Some of these studies could lead to the identification of shared performance requirements.

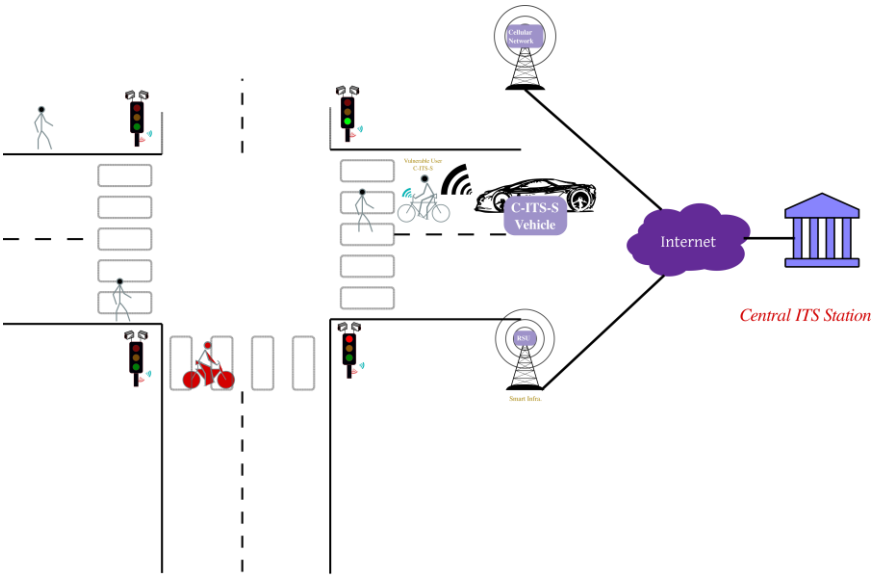

Figure 1: Intersection crossing safety risk

In the project, we did not have the resources to conduct the study; however, we can provide an example here. Let's consider the use case presented in

[L5.4] interoperability and performance objectives for autonomous vehicle systems

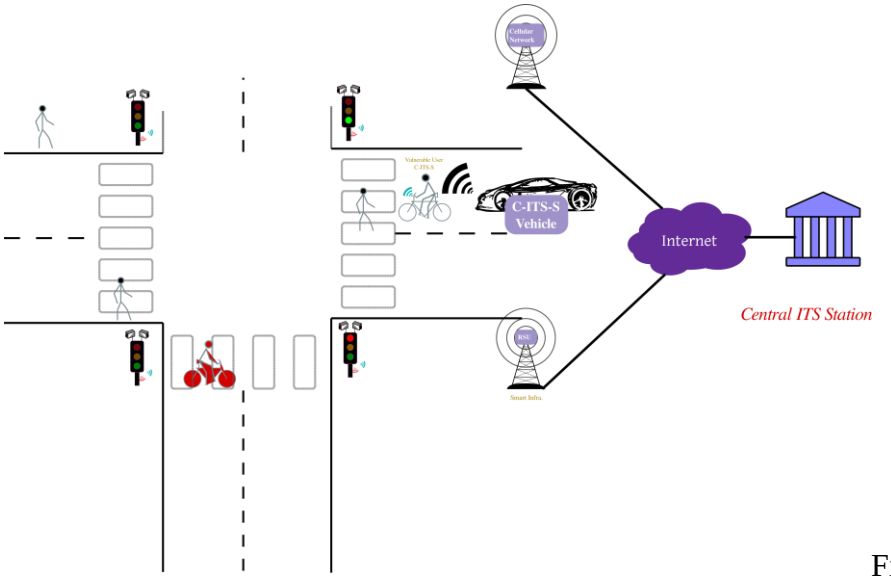

Figure 1. The (autonomous) vehicle on the right of the picture wants to turn left but cannot see the cyclist already on the road due to obstacles in front of it. To take the safest path and efficiently adapt its speed, the vehicle must receive information that the cyclist is on the road.

f the cyclist is detected by the infrastructure, then the information path would be:

1. **C1** - The infrastructure (traffic light) detects the cyclist.
2. **T1** - The information is sent to the central station.
3. **C2** - The central station fuses the incoming information.
4. **T2** - The central station forwards the information to the infrastructure (RSU) next to the vehicle.
5. **T3** - The RSU in turn broadcasts the information to the vehicles around.
6. **C3** - The vehicle fuses the incoming information and calculates its trajectory and speed.

Thus, based on this scenario, the overall communication steps must be completed in less time than the time to collision between the vehicle and the cyclist. Knowing that the vehicle's speed can be maximized to the current speed limit of the area, its minimum time and stopping distance (Mbt) can be calculated, which can then be translated into a maximum time for the entire information process. At the very least, this means:

$$T1+T2+T3<Mbt$$

Ensuring that T1,T2, and T3 are all smaller than Mbt/3 could provide a simple threshold approximation, which can, of course, be further tightened by other constraints estimating the longest possible T1+T2+...+Tn path.

Thus, a risk analysis based on the most common scenarios should be performed to identify the strongest constraints to avoid all identified unacceptable risks. Of course, weights can be further provided on each Cx component based on its theoretical maximum or statistical values, etc., yielding a first general maximization of the form:

$$w1T1+wT2*(Mbt/n)+\ldots+wTN*(Mbt/n)<Mbt$$

This approximation does not include computational time, which is non-negligible, especially if secure protocols are used (e.g., message signatures, anonymity, etc.). More complex approximations should include these computational constraints (wCx) to get something of the form:

$$w1+wT2*(Mbt/n)+\ldots+wTN*(Mbt/n)+wC1*(Mbt/n)+\ldots+wCN*(Mbt/n)<Mbt$$

where n=Nt+Nc, respectively the number of transmissions (Nt) and computational constraints (Nc) identified in the scenario.

This analysis should be performed for the transmission time as well as for all meaningful KPIs identified in deliverable 5.1, namely:

- Latency, i.e. time elapsed between the sending of a message by an ITS-S and its reception (ms)
- E2E delay (ms)
- Inter-Packet Gap as the time, calculated at the receiver, between successive successful packet receptions from a particular transmitter (ms)
- System recovery, the speed at which a DUT recovers from an overload condition (ms)
- Reset, the speed at which a DUT recovers from a device or software reset (ms)
- Max number (Message/s) and load (Ko/s) of messages that can be received and treated by the C-ITS-S
- Throughput of forwarding ITS messages functions (Message/s and load Ko/s)

2.1.2. Component capacity evaluation

When specific thresholds cannot be defined, it is still possible to evaluate the limits of the communication capacities of equipment. This might not be sufficient to ensure safety, but if an end user (transport service provider, regulators, etc.) can perform their own risk and performance analysis and define their own thresholds, providing them with product maximum capacities validation can be sufficient. They could then choose products based on these quantified limits, adapted to their own risk analysis.

2.2 Test conditions

The relevance of performance validation greatly relies on the conditions under which the validations are made and how representative they are of real conditions. Performing communication performance evaluation between fixed Vehicle C-ITS Stations (VCS, also called Onboard Units) might be of limited relevance for components to be installed on moving vehicles. They can still provide a theoretical maximum, but this might not suffice for all equipment.

[L5.4] interoperability and performance objectives for autonomous vehicle systems

Returning to the previous case study presented in

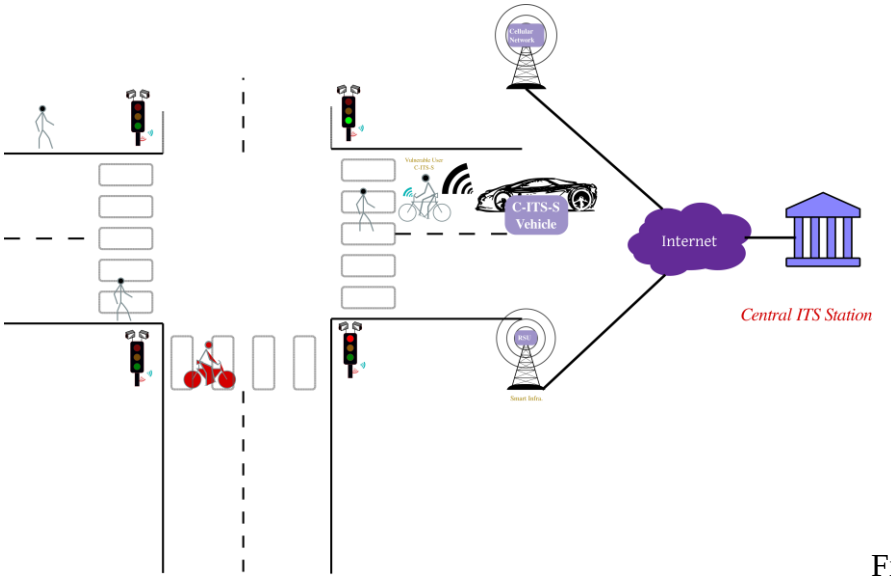

Figure 1, consider a vehicle approaching the same intersection but with dozens of vehicles and pedestrians, either stationary or moving, equipped with ITS-S within their communication range, as presented in Figure 2. In this scenario, many more environmental constraints appear, and nominal performance tests in controlled environments that are not representative of more complex environments might not be as relevant as they should be.

Thus, when performing evaluations, parameters representing different potential environmental conditions should vary, as illustrated in

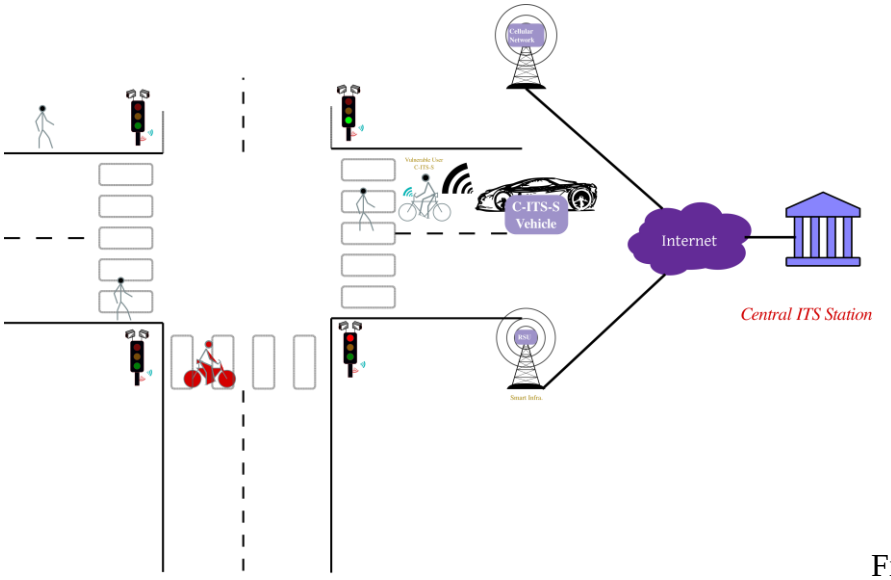

Figure 1 and Figure 2 (e.g., more complex environments, communication loads, etc.).

[L5.4] interoperability and performance objectives for autonomous vehicle systems

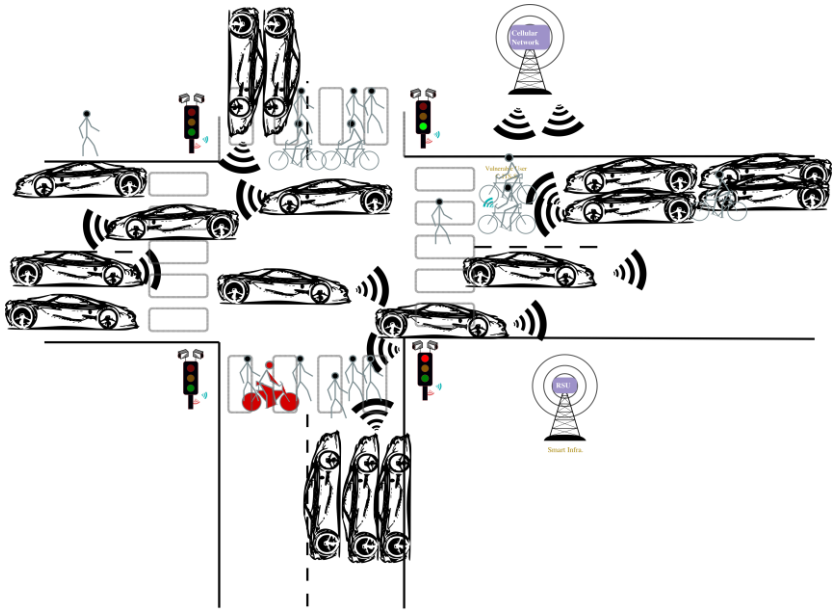

Figure 2: Crowded Intersection

- **Performing both indoor and outdoor tests**:
  - **Indoor tests** can be appropriate to ease the test coverage enlargement. Usually, indoor tests are more controllable and easier to parameterize, thus they can be performed with different parameter values.
  - **Outdoor tests**, on the other hand, allow validating that theoretical indoor results hold in the open air. They also allow performing tests with different constraints (e.g., line of sight or not, weather conditions, etc.).
- **Perturbations**:
  - Based on risk analysis, the main types of perturbations should be identified, and tests associated with the most critical ones should be performed (e.g., radio jamming, GNSS disconnection, objects in the line of sight, bad weather, etc.).
- **Load**

[L5.4] interoperability and performance objectives for autonomous vehicle systems

- As illustrated by

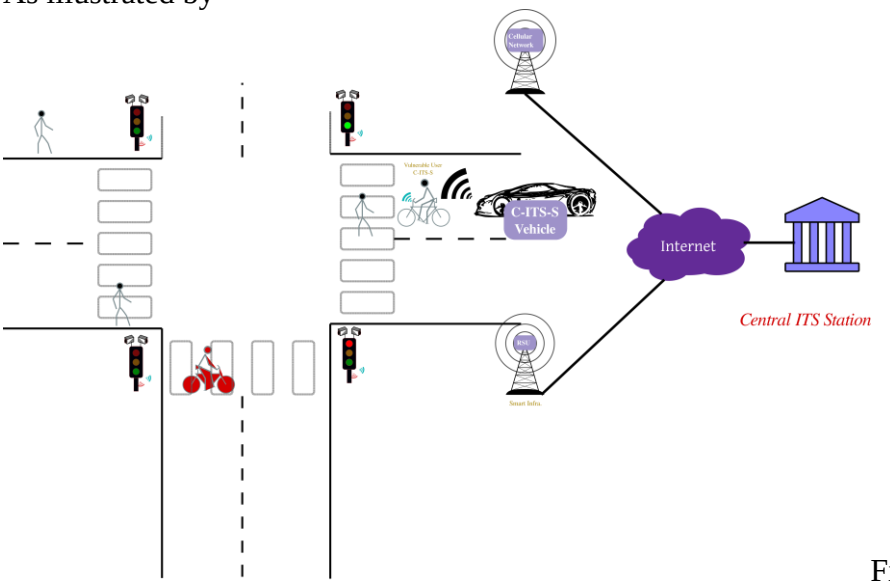

Figure 1 and Figure 2, it is obvious that when testing communications, the load of the communication media, greatly impact the performance. If not all configuration or network loads can produced or simulated for tests, still different level should be tested.

2.3 Empirical feedback

The method proposed in this section is designed to provide initial approximations of performance threshold requirements. However, like any other safety-critical service, these requirements will need to be updated based on empirical feedback. It is not yet possible to foresee all potential risks, threats, errors, and complex situations for which existing requirements may prove to be insufficient. While accidents, if regrettable, should be used as opportunities to reassess existing performance requirements and update them to enhance safety enforcement.

[L5.4] interoperability and performance objectives for autonomous vehicle systems

3 INTEROPERABILITY

The ways to validate interoperability are not numerous. You mostly have two choices:

- **Validation using a reference unit**:
- **Validation with a sufficiently significant number of other implementations**

A reference unit acts as a standardized benchmark against which other units are tested. This method ensures that the unit under test can correctly communicate and operate with a known, controlled standard. Using a reference unit simplifies the validation process, as it provides a consistent and reliable point of comparison. However, it is essential to ensure that the reference is itself thoroughly tested and updated to reflect any changes in standards or protocols, and is not a source of bias test due to to too specific implementation choices or standards interpretation (greatly depending on the implemented standard maturity).
On the other hand, validation with other implementation method involves testing the unit with various other units from different manufacturers or different models to ensure broad compatibility. It helps in identifying potential issues that may not be apparent when testing against a single reference unit, such as variations in implementation or edge cases.
Also, a last approach could also be considered, to combine both test with a refence unit and other (potentially less many) implementations:

- **Hybrid validation**

3.1.1. Reference unit validation

Using a reference unit for interoperability validation is often the first step in ensuring compatibility. This method has several key advantages:

1. **Consistency**: A reference unit provides a consistent and repeatable test environment, which is crucial for identifying specific interoperability issues.
2. **Controlled Environment**: Testing against a reference unit allows for a controlled environment where variables can be minimized, making it easier to pinpoint the source of any issues.
3. **Standard Compliance**: Are de facto standards, even if reference units are typically designed to be fully compliant with industry standards, but even if they don’t, ensuring that any unit validated unite can interoperate with the reference unit is likely to be compliant to the reference unit standard.

However, there are also limitations to this approach. A reference unit may not cover all possible real-world scenarios and variations, which could lead to gaps in the validation process. Also, the reference unit must be regularly updated to reflect changes in standards and protocols, requiring ongoing maintenance and support. Finally, the reference unit if not carefully designed or validated can introduce accuracy or bias issues. In fact, the reference unit must be itself perfectly conform to standard and should not introduce any implementation bias, based on their developers’ choices (enforcing specific technologies, adding nonmandatory APIs or functionality, etc.).

3.1.2. Validation with other implementations

Validating interoperability with a wide range of other implementations offers a more comprehensive approach:

1. **Real-World Scenarios**: This method allows for testing in diverse and real-world scenarios, uncovering issues that may not be evident in a controlled environment.
2. **Diverse Implementations**: Different manufacturers may interpret and implement standards slightly differently, so testing with multiple implementations ensures broader compatibility.
3. **Robustness**: This approach helps ensure that the unit under test is robust and capable of handling various communication styles, protocols, and edge cases.

But Coordinating tests with multiple implementations can be logistically challenging and time-consuming. This approach requires access to various units and potentially involves more extensive testing resources. It often implies that validated product developers have to support to some extent later validation with their validated product.

3.1.3. **Hybrid approach**

A combined approach leveraging both reference unit validation and validation with other implementations is often the most effective strategy:

- **Initial Testing**: Begin with reference unit validation to ensure basic compliance and functionality.
- **Extended Testing**: Follow up with validation against multiple other implementations to cover a broader range of scenarios and ensure robust interoperability.
- **Continuous Improvement**: Regularly update both the reference unit and the pool of other implementations to reflect changes in technology, standards, and real-world conditions.

By combining these methods, you can achieve a thorough and reliable interoperability validation process that ensures your equipment can operate effectively and safely within the intended environment.

[L5.4] interoperability and performance objectives for autonomous vehicle systems

4 CONCLUSION

In this deliverable, we have presented a scenario-based risk analysis method to aid in the design of communication performance requirements. We did not apply it during the project and were unable to formulate an initial set of such requirements due to resource constraints. However, we believe this proposition to be useful, or at least an interesting starting point for discussion in future related work.

As stated in section 2.3, without more empirical data, initially regulated thresholds might not be as relevant as they could be. The first approach to follow should probably be the one suggested in section 2.1.2: assessing communication component maximum capabilities so that every system owner or responsible party can choose their system's components based on their own risk analysis and performance requirements. This also allows for comparison of product performance when making choices.

Regarding interoperability, we do not define in this document the approach to be followed but have presented what, to our knowledge, are the three main alternatives. The easiest to implement and potentially the most efficient is the use of a reference unit. However, the possibility of choosing this validation approach is closely related to the maturity of domain standardization. If C-ITS standardization activities have been extensive and the standards have already reached a good level of maturity, the relatively limited operational feedback from C-ITS deployment does not guarantee the relevance of this approach.