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

[L5.7] TESTS REPORT ON THE SECURITY AND EFFICIENCY OF THE COMMUNICATIONS

RAPPORT SUR LA MISE EN ŒUVRE SUR PLATEFORME D'ESSAIS DE TESTS DE CYBERSÉCURITÉ POUR LA CONNECTIVITÉ.

Main authors: Nathan CHOPINET, Virginie DENIAU, Romain GICQUAUD, Christophe GRANSART, Sammy HADDAD, Romanos ZACHARAS

Keywords: Tests, Connectivity, Performance, Interoperability, V2X.

Abstract. In this deliverable we present the tests conducted on Collaborative Intelligent Transport Systems equipment's (C-ITS) providing V2X communication services. These tests had several objectives as identified in deliverable PRISSMA 5.4: evaluate performance, security and interoperability aspects of V2X communications devices. We present here the different test platforms used and the results obtained during these tests. Those tests do not directly target AI components, however they are meant to assess the security of critical support functions to AI components in AI based autonomous C-ITS systems.

Résumé. Ce livrable présente les différents tests menés sur des équipements de communication C-ITS fournissant des services de communication V2X. Ces tests avaient les objectifs suivants identifiés dans le livrable PRISSMA 5.4, valider la performance, sécurité et interopérabilité de services de communication V2X. Ces tests ne ciblent pas directement les composents IA des systems de transports autonomes, mais leurs fonctions critiques d'échanges d'information technologies C-ITS support des principals fonctions d'améllioriation des performances et sécuirté de ces systèmes.

Table of Content

1 INTRODUCTION

In this deliverable we present the tests conducted on different Collaborative Intelligent Transport Systems equipment's (C-ITS) providing V2X communication services.
Three different tests environment have been used to tests C-ITS equipment's presented in more details in section 2:

- onboard units
- roadside units

The tests implied different C-ITS equipment owned by the PRISSMA partners. The goal of these tests was not to qualify those specific products for which the developers were not involved, and no specific support provided. But rather to demonstrate the type and associated efficiency of the performed tests themself. Efficiency in term of (i) capabilities to demonstrate one specific property, (ii) cost and difficulty to perform the test.
These tests had several objectives as identified in PRISSMA deliverable 5.4, evaluate performance, security, and interoperability aspects of V2X communications devices.
The different test platforms used to perform those tests are described in section 2. Four different platforms have been used to allow us to perform several types of tests not all possible on one platform e.g.: in door vs outdoor, interoperability and performance tests on product of same vendor, vs different vendors. These different set-ups allowed us to compare test results on different products under different conditions allowing us to compare them and get a deeper analysis on the results and meaningfulness of the test approach.
The list of the tests performed on the different platforms and their results are presented respectively in sections 3.
For the tests performed on the 4th platform (cf. section 2.3) only partial documentation has been provided for the tests, and no technical support has been provided by the developers who is not involved in the project. These tests have been performed in pure black box testing conditions. So, they allowed us to demonstrate some limitations of such approaches. In fact, one major limitation arises during the tests on this platform, the impossibility for us despite important efforts to configure the security functions of the C-ITS communications, one of the main tests targets. The equipment configuration did not include any ETSI 103 097 certificates. Even so, Eviden not member of PRISSMA had graciously loan PRISSMA partner a full a free C-ITS PKI access for these tests (same PKI implementation as European deployments supervised by the Commission), we did not manage to configure the equipment to correctly connect to it and activate the signing and encrypting functions in this black box context, necessary for the interoperability and security tests. Thus, section 3.1.3, presents the initial intended test plan that in the end could not be performed. More details about security tests on the platform 4 equipment's that have been performed are synthetized in the deliverable l5.6.

2 Test Platforms

2.1 Test Platform 1: jamming

The test bench is designed to evaluate the impact of jamming signals on the communication between OBU and RSU devices.
In our work, we used RSU and OBU designed by Lacroix to emulate the real-world components of an ITS-G5 system. Three other main components have also been required in our architecture: 1) the AWG70001A Tektronix generates jamming signals, 2) the J7211A Agilent controls the level of these signals, and 3) the FSW67 R&S analyzes the power of each signal interactions. This set up allows to study the performance and reliability of these systems under adverse conditions. The complete set up, shown in the following figure is composed of:

- AWG70001A Tektronix: This is an Arbitrary Waveform Generator (AWG) capable of generating signals with a sample rate up to 50 GS/s and 10-bit vertical resolution. This equipment is used to generate interference patterns (jamming) in order to evaluate the robustness of the OBU and RSU communication systems against such interference;
- J7211A Agilent: This device is an attenuation control unit used to manage signal levels within test setups. This device allows us controlling the power ratio between the communication signals and the jamming signal;
- FSW67 R&S: This is a spectrum analyser used to measure the power of the jamming and communication signals received by the RSU;
- RSU Lacroix: The RSU Lacroix is used to emulate infrastructure-based communications;
- OBU Lacroix: The OBU Lacroix also know as Neavia V2V is used to emulate the vehicle-based component of the vehicular communication system;
- Splitters: These are used to divide and combine the signals between different paths in the test setup, enabling simultaneous monitoring and measurements by multiple devices;
- Switch NETGEAR: This network switch is used to manage Ethernet connections within the test bench, likely to network the different test components for coordinated control and data collection;
- Dell Ubuntu LTS 22.04: A computer with Ubuntu Linux 22.04 LTS operating system is the control centre of the test bench, running software to coordinate the tests, collect data from the OBU, and analyse the results.

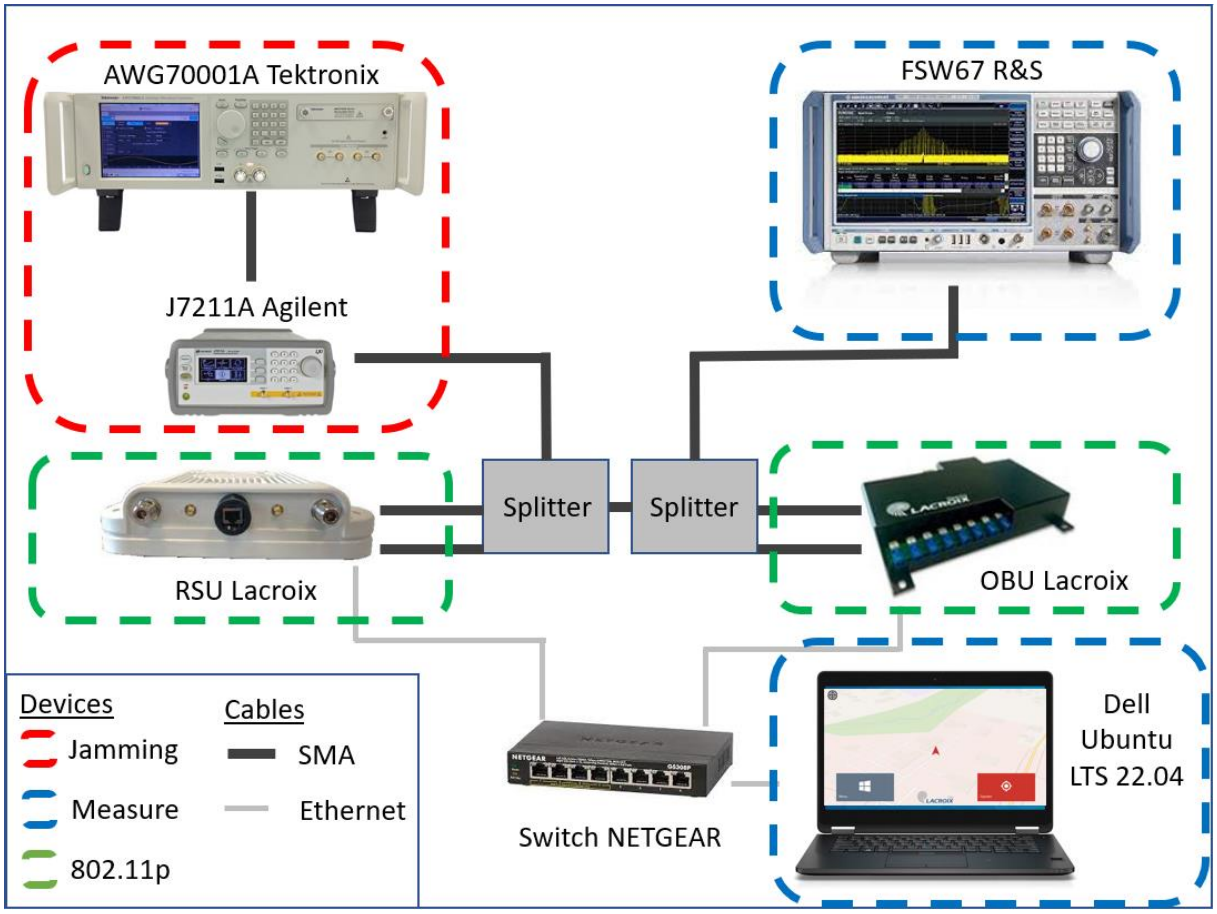


Figure 1 Test Platform 1: jamming quality of service

The OBU user interface, which is accessible on the computer, allows controlling the communicating card. It allows for the retrieval of GPS positioning, crucial for navigational and tracking purposes within intelligent transport systems. Furthermore, the interface provides the flexibility to select the types of messages and time intervals for broadcast, in order to create specific communication scenarios. This also permits the reception of incoming messages and their export in CSV format, which opens data analysis and post-processing tasks.

2.2 Test Platform 2: jamming and quality of service

The test bench is designed to evaluate the impact of jamming signals on the communication between OBU and RSU devices.
In our work, we used RSU and OBU designed by Lacroix to emulate the real-world components of an ITS-G5 system. Three other main components have also been required in our architecture: 1) the AWG70001A Tektronix generates jamming signals, 2) the J7211A Agilent controls the level of these signals, and 3) the FSW67 R&S analyzes the power of each signal interactions. This set up allows to study the performance and reliability of these systems under adverse conditions. The complete set up, shown in the following figure is composed of:

- AWG70001A Tektronix: This is an Arbitrary Waveform Generator (AWG) capable of generating signals with a sample rate up to 50 GS/s and 10-bit vertical resolution. This equipment is used to generate interference patterns (jamming) in order to evaluate the robustness of the OBU and RSU communication systems against such interference;

- J7211A Agilent: This device is an attenuation control unit used to manage signal levels within test setups. This device allows us controlling the power ratio between the communication signals and the jamming signal;
- FSW67 R&S: This is a spectrum analyzer used to measure the power of the jamming and communication signals received by the RSU;
- Codha wireless equipment: the Codha modems could act as RSU or OBU. The configuration is done through parameters on the linux OS;
- Splitters: These are used to divide and combine the signals between different paths in the test setup, enabling simultaneous monitoring and measurements by multiple devices;
- Switch NETGEAR: This network switch is used to manage Ethernet connections within the test bench, likely to network the different test components for coordinated control and data collection;
- Dell Ubuntu LTS 22.04: A computer with Ubuntu Linux 22.04 LTS operating system is the control center of the test bench, running software to coordinate the tests, collect data from the OBU, and analyze the results.

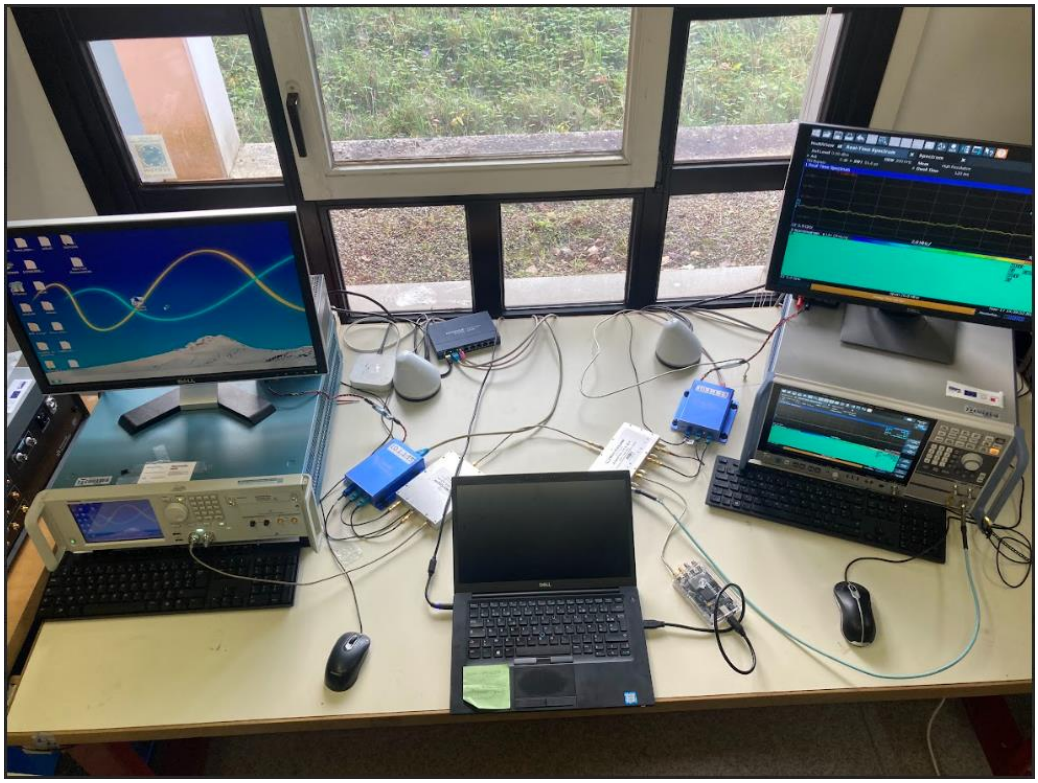


Figure 2 Test Platform 2: jamming quality of service

The codha equipment are managed through a SSH shell or using a serial port connection. Selection of the RSU or OBU mode is done by script to configure the modems in a proper way. We used the iperf3 software which is dedicated to evaluating network throughput. iPerf3 is a tool for active measurements of the maximum achievable bandwidth on IP networks. It supports tuning of various parameters related to timing, buffers and protocols (TCP, UDP, SCTP with IPv4 and IPv6). For each test it reports the bandwidth, loss, and other parameters. IEEE 802.11p is mainly using broadcasting packets through UDP as transport protocol, we used the same configuration to evaluate the throughput.

2.3 Test Platform 3: Secure interoperability

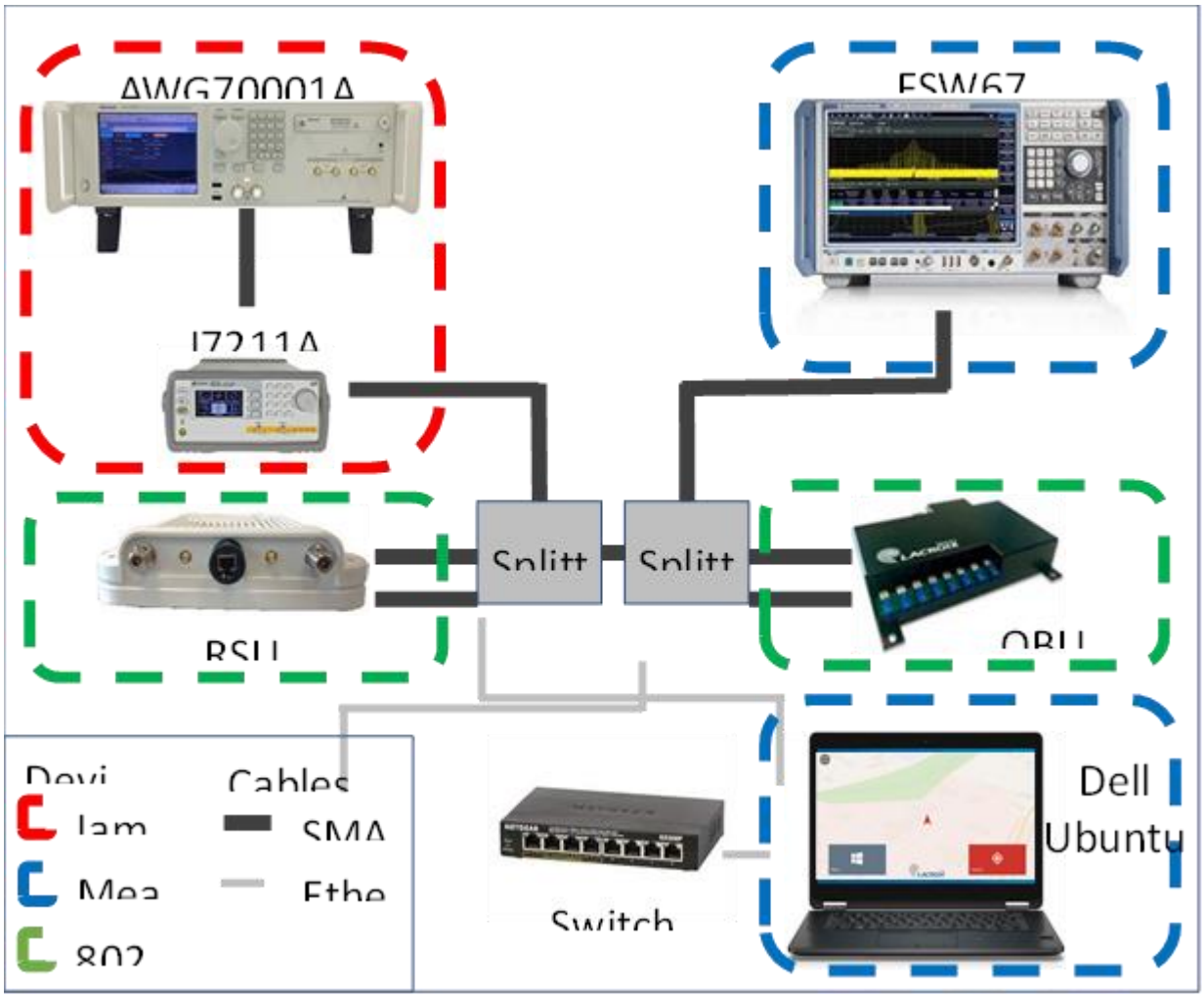


Figure 3 Paltform 3 configuration in connected mode with heterogeneous equipment

The test bed is similar to the previous one. We mixed equipment from various providers: Lacroix and Codha.
We used the wireshark tool to make eavesdropping of exchanges to understand the communications.

2.4 Test Platform 4: Secure interoperability

For interoperability and security, the tests have been performed on two roadside units (RSU) and on one onboard unit (OBU). More precisely the Targets of Evaluation (TOE) were:

- RSU Lacroix RailDin
- RSU Lacroix
- OBU YoGoKo

The equipment has been provided by UTAC (as PRISSMA project collaborator), along with part of the documentation. For Lacroix equipment we had:

- RSU UEV EU - Configuration parameters Ed.17
- API RSU and OBU Ed.19

- Road unit User manual Ed.22

For YoGoKo equipment we had:

- YoGoKo-ITSUI APK
- Update binaries
  - 4.0.0.0_4.6.2.0.bin
  - 4.6.2.0_4.7.0.0_eu.bin
  - 4.6.7.0_5.0.1.2_eu.bin
- Quick setup guide YBOX-VEHI-2203 V1.0 (equivalent of the evaluated version)

To send and receive data from this equipment we used both RJ45 and radio connections. For radio connection between evaluators computers and C-ITS stations targt we used an Ethus USRP N210.
Only partial documentation has been provided for the tests as well as no technical support from the developers. These tests have been performed in black box testing conditions.
One main limitation of this test platform has been the impossibility for us to configure the security functions of the C-ITS communications. The equipment configuration did not include any ETSI 103 097 certificates. Even so, Eviden not member of PRISSMA had graciously loan PRISSMA partner a full a free C-ITS PKI access for these tests, we did not manage to configure the equipment to correctly connect to it and activate the signing and encrypting functions in this black box context, necessary for the interoperability and security tests.

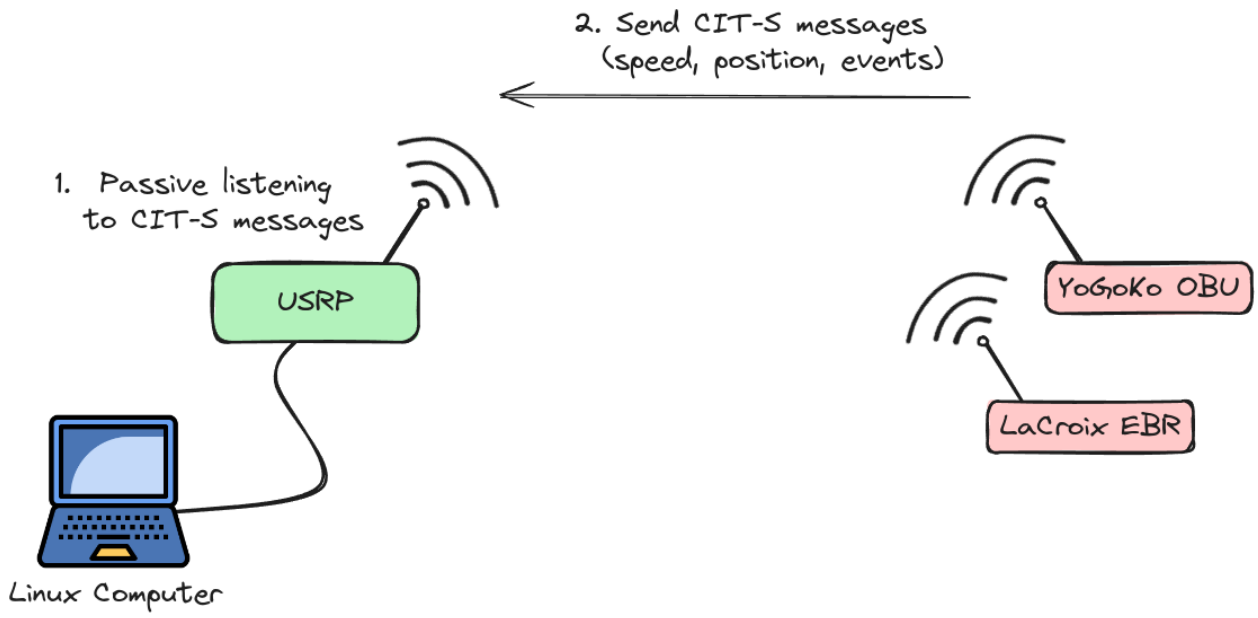


Figure 4 Test platform 3 – Radio connection configuration.

2.5 Test Platform 5: Outdoor performances

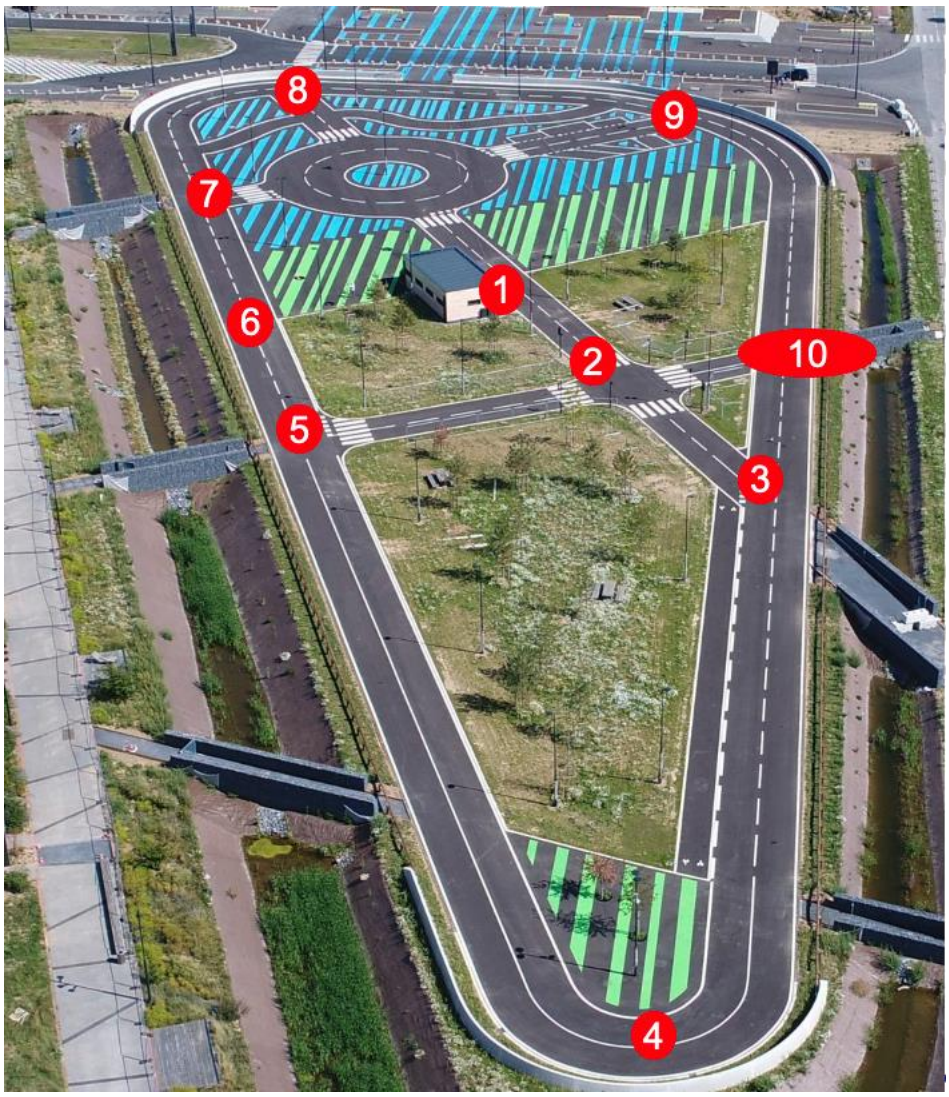


Figure 5 Gyrovia test track

Track tests have been performed at the Gyrovia track located in the North of France.
Several positions, 10 actually (cf Figure 5), have been identified on the track to be used as reference marks for tests.
The RSU was in position 1 and a moving truck equipped with on IEEE 802.11p compatible equipment drove to the 9 other positions to perform reception quality test of reception of ETSI messages to perform at each of them a static position reception test.

3 TESTS AND RESULTS

3.1 Performance and quality of service

3.1.1. Jamming tests on Lacroix equipment – Platform 1

Jamming on V2X communication – platform 1
Test purpose:
The goal of these tests are to find the limit where a jamming signal start to interfere with the communication signals between an OBU and a RSU. Vehicular communications offer a means of improving or optimizing transport networks. They can be used to share real-time information on the state of the road network, to better manage traffic in the event of an accident or incident, to make it easier for emergency services to intervene. However, as with all communication networks, the security of exchanges must be guaranteed. In particular, vehicular exchanges can be subject to various types of attacks such as man in the middle, black hole or jamming. This test presents an evaluation of the vulnerability of the IEEE 802.11p, ITS-G5 physical layer, to jamming attacks, using a dedicated test bench that emulates such communication. The research focuses on understanding how such attacks affect communication by observing high layer of communication indicator.
Initial conditions:
Cf. Section 2.1 for platform 1 description.
Tools used:
Cf. Section 2.1 for platform 1 description.
Test description:
Commercial jammers can affect multiple frequency bands, such as the LTE, 5G, 802.11ax, Bluetooth bands, etc. Some

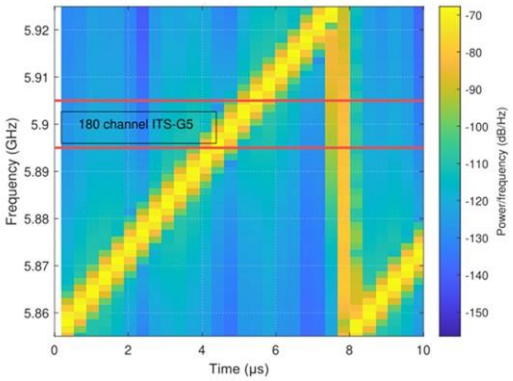


Fig. 3. Spectrogram of a 8µs Sweep Time jamming signal.

jamming signals generated by commercial jammers, have been characterized. They are chirp signals that sweeps across a pre-defined frequency range within a set time known as the Sweep Time (ST). These jamming signals can be modeled by the following equation 1.

$$s(t) = A\cos\left(2\pi\left(\frac{f_2 - f_1}{SweepTime} \times t + f_1\right) \times t\right) \quad (1)$$

where A is the amplitude of the jamming signal, f_1 and f_2 define the bandwidth of the jamming signal. ST is a parameter that defines how long the jamming signal covers the frequency band and how often it passes over the communication frequency band. The impact of the jamming signal is significantly linked to the ST value. In consequences, in our study we carried out tests with different values of ST.

Concerning the frequency band swept by jamming signals in our study, we focused over the 70 MHz band from 5.855 GHz to 5.925 GHz, which is dedicated to 802.11p vehicular communications. To generate these jamming signals with the AWG, we preliminary defined the signal with equation 1 in Matlab and stored it in a .txt file. The jamming *.txt* file was then loaded in the AWG to be generated continuously. The Fig. 2 represents a jamming signal with a 8µs sweep time generated in Matlab.

Expected results:

Identification of the number of messages sent and correctly received.

Observed results:

First, we checked the repeatability of the measurements. Then, we study the susceptibility of the 802.11p vehicular communication facing different jammer STs and SJRs.

A. Repeatability of the tests

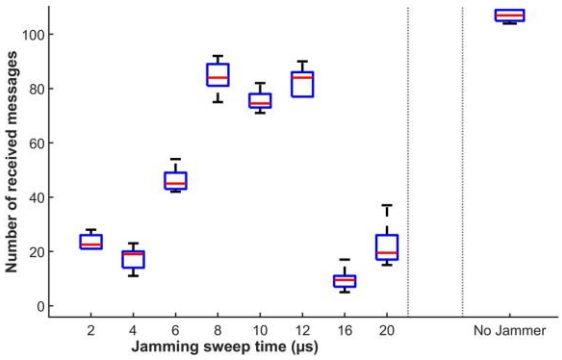


Figure 6 10 measurements Boxplot of the number of received communication messages in 10 seconds exposed to jamming with a SJR=80dB and with sweep times values from 2µs to 20µs.

In order to observe the repeatability of the measurement results, we fixed the SJR at 80dB and performed 10 repeated tests for each sweep time value. We plot the results in Fig. 5 as a boxplot where the y-axis is the number of received messages from 0 to 110 (all the messages sent by RSU are received) and the x-axis is the jamming sweep time (µs). For these tests, we choose the jamming sweep time values of 2 µs, 4 µs, 6 µs, 8 µs, 10 µs, 12 µs 16 µs and 20 µs. We completed it with the number of received messages without jamming signal, on the right-hand side of the graph. In these results, the median is represented by a red line, in a blue box-plot delimited by first and third quartile. We can see the difference between the first and third quartile, generally does not exceed 10 messages. Knowing that without jamming, the difference between the first and third quartile reaches 5 messages, the repeatability of the measurement in the presence of jamming is satisfying. Taking into

account the satisfying repeatability of the results, in the next section, we analyse the results for different values of SJR and ST, in performing only one test per configuration.

B. Impact of the sweep time and the SJR

In order to study the impact of the sweep time for different SJR, we varied the jamming power to reach SJR of 75 dB, 80 dB and 85 dB. We measured the Number of Received Messages (NRM) for each jamming sweep time and with those 3 SJR values and we plot it in Fig. 6. The y-axis represents the number of messages received to the On-Board Unit during 10 seconds with the presence of jamming signal. The x-axis indicates the sweep time of the applied jamming signal. For the 85 dB SJR, we observe that the NRM varies between 15 received messages for ST = 4 µs to 105 received messages for ST= 16 µs. For the 80 dB SJR, the NRM varies between from 12 messages received for ST= 16 µs to 83 received messages with ST = 12 µs. For the 75 dB SJR, all the results are between 1 and 0 received messages except 4 µs, 6 µs jamming.
To analyse these results, we identify tree zones called [A], [B] and [C] separated by red lines in the figure. In zone [A], the communication is clearly affected regardless of the SJR and a maximum of half the messages sneak through the jamming. In zone [B], we notice a significant difference between the number of messages received with SJR of 75 dB in relation to the results with SJR of 80 dB and 85 dB. With SJR = 75 dB the NRM is close to zero while it is approximately 80 with SJR of 80 dB and 85 dB. In zone [C], 80 dB and 75 dB are significantly affected where 85 dB is almost not disturbed by the jamming signal.

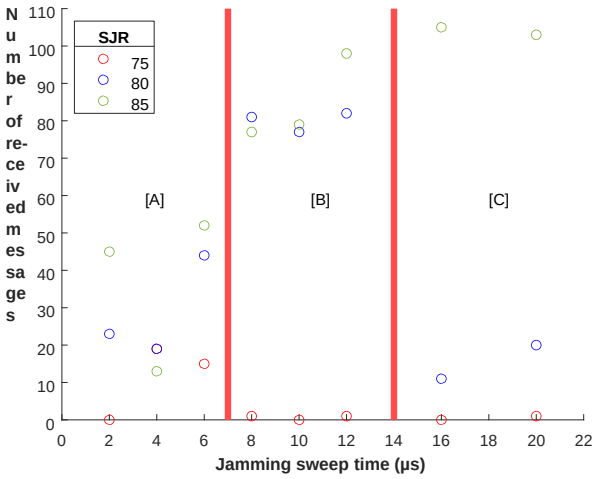


Figure 7 Plot of measurement of number of messages in 10 seconds of communication SJR=75 dB SJR=80 dB SJR= 85 dB exposed to jamming with sweep time from 2 µs to 20 µs separated in 3 sets A, B and C

C. Interpretation of the results

To interpret these results, we studied the frequency occupation of the jamming signal in the ITS-G5 band, applying a time-frequency analysis similar to the input processing of the 802.11p receiver. The input processing of the 802.11 p receiver consists in a FFT performed over a time window corresponding to the symbol time, i.e. a 8 µs-time window. Figure 7 illustrates the number of jamming cycles included in a 8 µs time window, according to the ST of the jamming signal. We note in particular that when the ST is 2 µs, 4

jamming signal cycles are included in the 8 µs symbol time, whereas with ST = 16 µs, only half a cycle is included in the 8 µs symbol time period. That means that in case of a quick jamming signal with ST = 2 µs, the pattern is repeated inside the 8µs time windows, and this impacts the spectrum occupation obtained by the Fast Fourrier Transform (FFT) carried out by the 802.11p receiver. Indeed, a repeated signal in the time becomes a frequency comb. To illustrate this comment, we plotted in Fig. 8, 9, 10 and 11, the FFT of the different sweep time jamming signals, with a FFT time windows of 8 µs corresponding to the 802.11p symbol time.

For ST = 2 µs, in Fig. 8, the whole 802.11p band is occupied with a maximal power of -26 dBm over certain subcarriers frequency. However, in Fig. 12 which is a zoom in a 10 MHz band, we note that the distribution corresponds to a frequency comb that does not cover all the successive 802.11p **subcarriers** (80 subcarriers spaced by 125 kHz in a 10 MHz band). The difference between the frequency comb lines is 500 kHz = 1/2 µs. This means that one subcarrier out of 4 is affected by the jamming signal, but with a high level of jamming power.

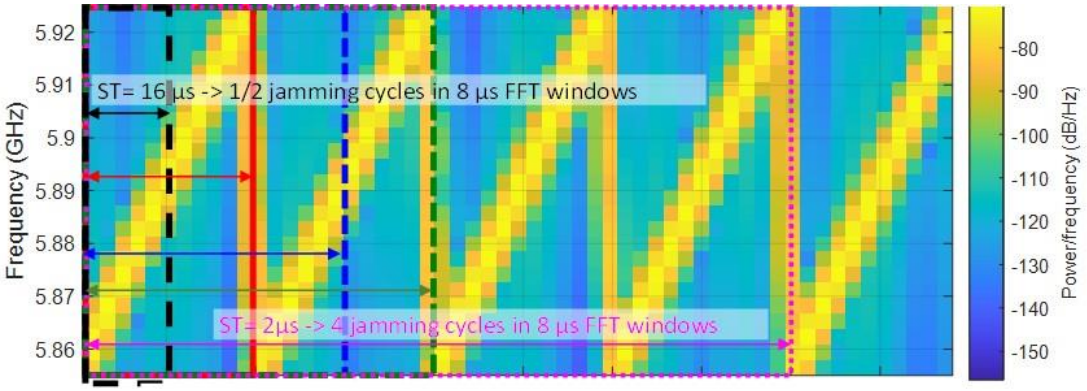


Figure 8 Number of jamming cycles included in the 8 µs FFT window according to the jamming sweeptime

For a ST = 6 µs, in Fig. 9, the spectrum is not homogeneous across the entire band. Indeed, in a 8 µs period, the jamming swept two times the first third of the band and only one time the **rest** of the frequency band. With a ST= 8 µs in Fig. 10, the spectrum is relatively homogeneous at -30 dB because the sweep time corresponds precisely to the duration of one cycle.

For ST = 16 µs, in Fig. 11, half the band is occupied because the jamming signal does not scan the entire 802.11p band during the 8 µs FFT windows. In this graph, the 180 frequency channel of the communication is not covered by the jamming signal due to the FFT is calculated with a time windows set at the start of the jamming chirp slope. In a real situation, the same portion of the band will be covered, but with a random shift of the start frequency in the band.

Thanks to these observations, we associate, the zone [A], [B] and [C] of Fig. 6 behaviour to the FFT results over a 8 µs time window. In zone [A], whatever the SJR, the number of lost messages is significant. This is potentially due to the fact that only a part of the subcarriers is affected but systematically with a high level of jamming power. In the zone [B], the sweep time is equal or near the 8 µs FFT time windows, given a spectrum occupation relatively homogeneous over all the 802.11p frequency band. In this zone [B], we note a significant difference between the SJR of 75 dB and the SJR of 80 and 85 dB. That means that

with a SJR of 75 dB, a critical SJR is reached, provoking a whole incapability of the communication chain to demodulate the signal. In zone [C], the same situation that zone [B] can be observed but not all the time, due to only a percentage of the communication channel is covered by the jamming signal during a symbol time due to the relatively slow sweep time. However, this situation is not more favourable for the communication. Indeed, in [C], with the SJR of 80 dB, the major part of the message are lost. This can be explained by the jamming power a little bit higher than in the frequency spectrum of the zone [B], and with a quasi-constant value between the successive sub carriers. Anyway, a precise explanation would require complementary tests and notably to analyse the impact over a longer duration than a symbol.

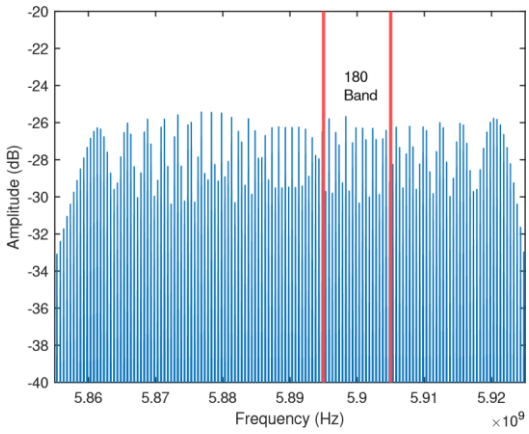


Figure 10 FFT of a 2 µs ST jamming signal over the 802.11p frequency band

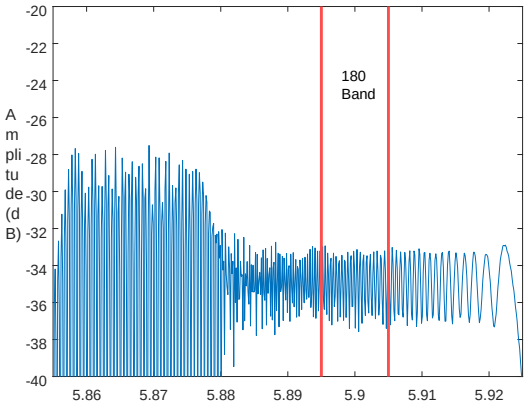


Figure 9 FFT of a 6 µs ST jamming signal over the 802.11p frequency band corresponding to a frame

Conclusions / analysis in comparison with initial objective

IEEE 802.11p is sensible to jamming attacks, even if the jamming signal is low compared with the communication signal.

3.1.2. Jamming and performance tests on V2X communication – Platform 2

Jamming and performance tests on V2X communication – platform 2

Test purpose:

As for the previous test the first goal here is to find the limit where a jamming signal start to interfere with the communication signals between an OBU and a RSU.
Vehicular communications offer a means of improving or optimizing transport networks. They can be used to share real-time information on the state of the road network, to better manage traffic in the event of an accident or incident, to make it easier for emergency services to intervene. However, as with all communication networks, the security of exchanges must be guaranteed. In particular, vehicular exchanges can be subject to various types of attacks such as man in the middle, black hole or jamming. This test presents an evaluation of the vulnerability of the IEEE 802.11p, ITS-G5 physical layer, to jamming attacks, using a dedicated test bench that emulates such communication. The research focuses on understanding how such attacks affect communication by observing high layer of communication indicator.
Our second goal here is to use the same platform to evaluate the messages throughput using the iperf linux tool in the context of intentional perturbations

Initial conditions:

Cf. Section 2.2 for platform 2 description.

Tools used:

Cf. Section 2.2 for platform 2 description.

Test description:

Commercial jammers can affect multiple frequency bands, such as the LTE, 5G, 802.11ax, Bluetooth bands, etc. Some

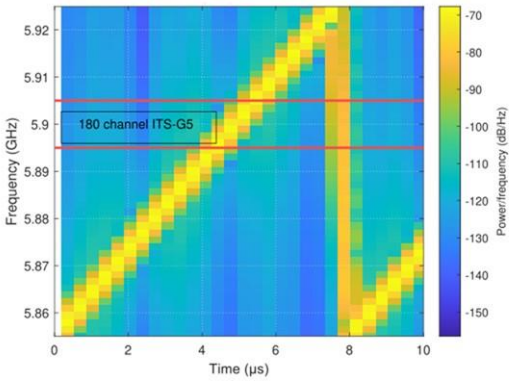


Fig. 3. Spectrogram of a 8µs Sweep Time jamming signal.

jamming signals generated by commercial jammers, have been characterized. They are chirp signals that sweeps across a pre-defined frequency range within a set time known as the Sweep Time (ST). These jamming signals can be modeled by the following equation 1.

$$s(t) = A\cos\left(2\pi\left(\frac{f_2 - f_1}{SweepTime} \times t + f_1\right) \times t\right) \quad (1)$$

where A is the amplitude of the jamming signal, f_1 and f_2 define the bandwidth of the jamming signal. ST is a parameter that defines how long the jamming signal covers the frequency band and how often it passes over the communication frequency band. The impact of the jamming signal is significantly linked to the ST value. In consequences, in our study we carried out tests with different values of ST.

Concerning the frequency band swept by jamming signals in our study, we focused over the 70 MHz band from 5.855 GHz to 5.925 GHz, which is dedicated to 802.11p vehicular communications. To generate these jamming signals with the AWG, we preliminary defined the signal with equation 1 in Matlab and stored it in a .txt file. The jamming *.txt* file was then loaded in the AWG to be generated continuously. The Fig. 3 represents a jamming signal with a 8µs sweep time generated in Matlab.

In the same time, the communication throughput of the perturbed signal is evaluated using iperf in the context of intentional perturbations.

Expected results:

Identification of the number of messages sent and correctly received and communication throughput evaluation.

Observed results:

Jamming

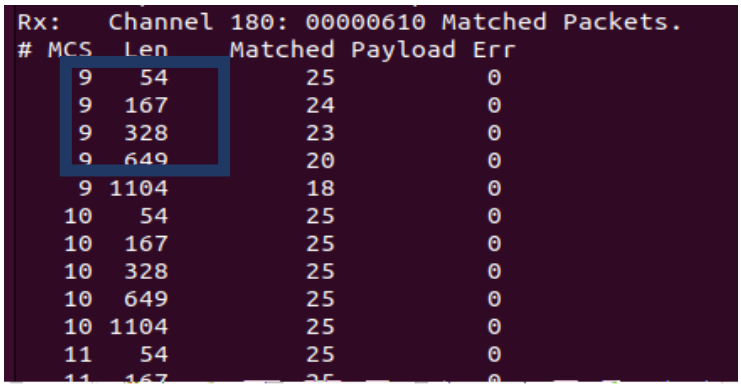


Table 1Example of exchanged messages with no jamming

The test application sends a repetition of messages of various size.
We used the number of received messages and the MCS indicator to study the quality of the transmission. The MCS (Modulation and Coding Scheme) varies according to the quality of the channel. This parameter is defined in the IEE 802.11 general standard.
In the following figures, the X axis is the sweep time of the jammer and the Y axis is the number of messages received.

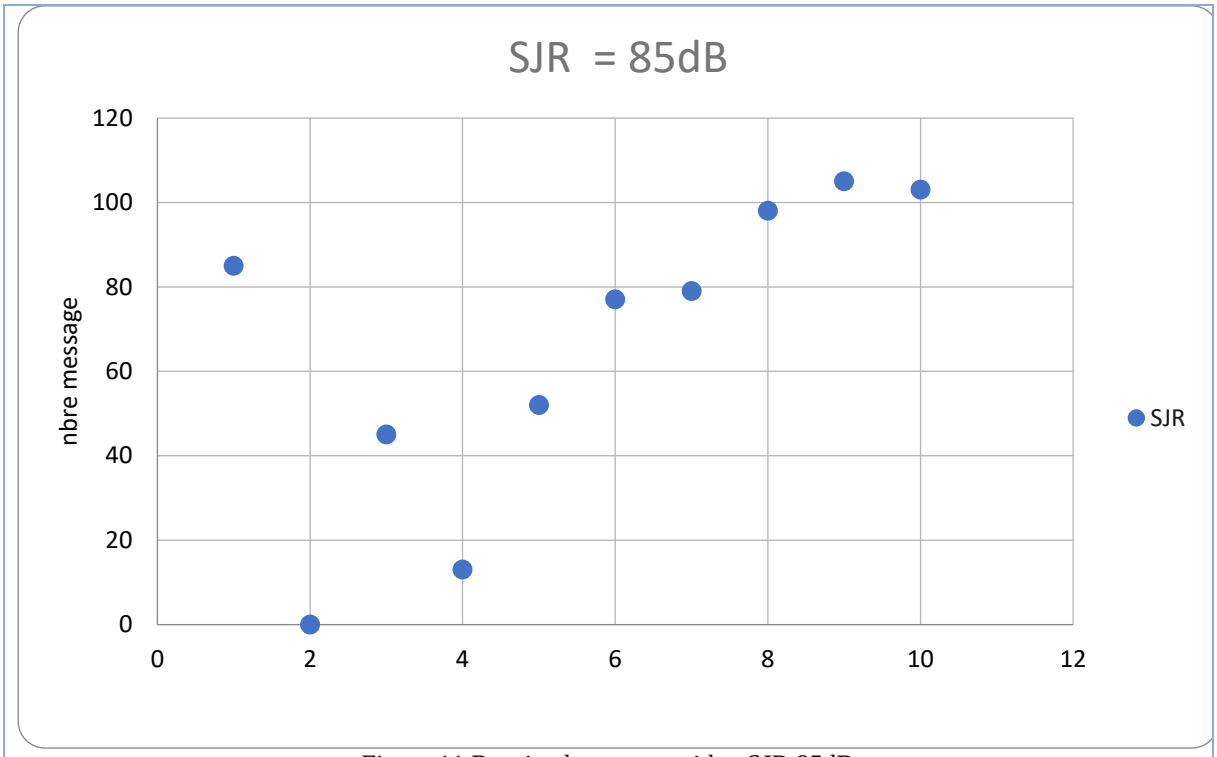


Figure 11 Received message with a SJR 85dB

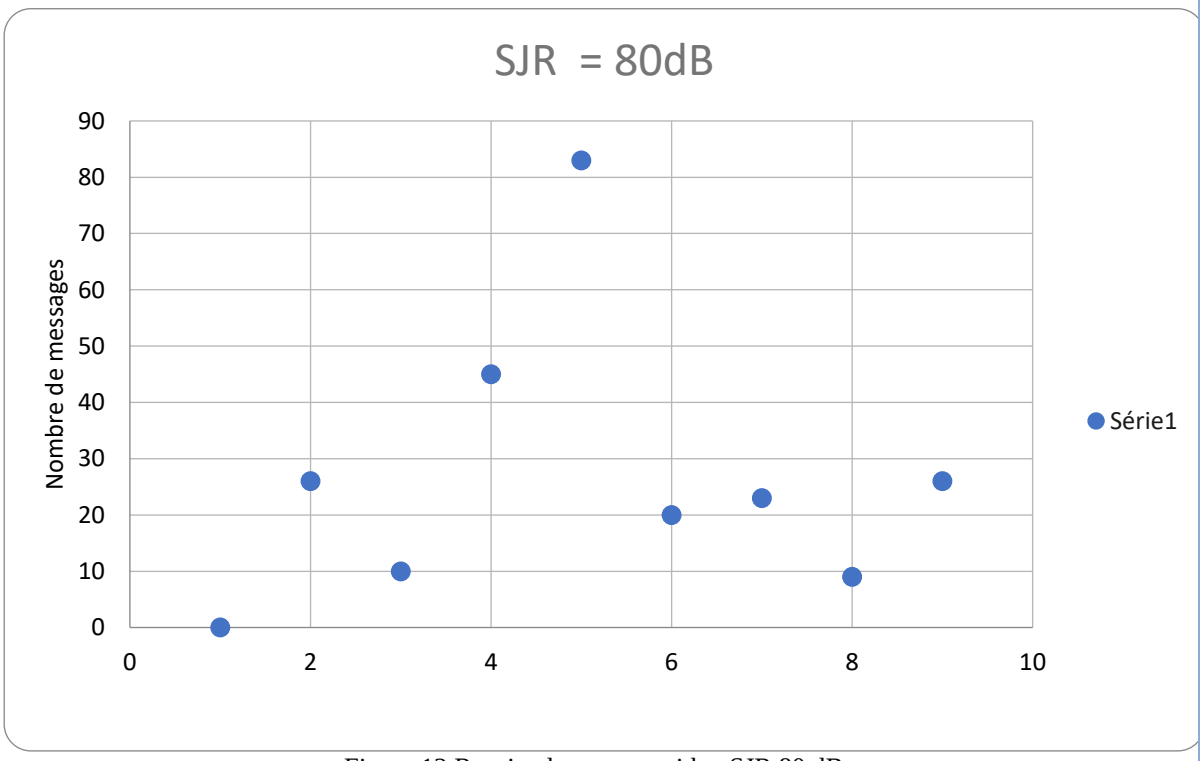


Figure 12 Received message with a SJR 80 dB

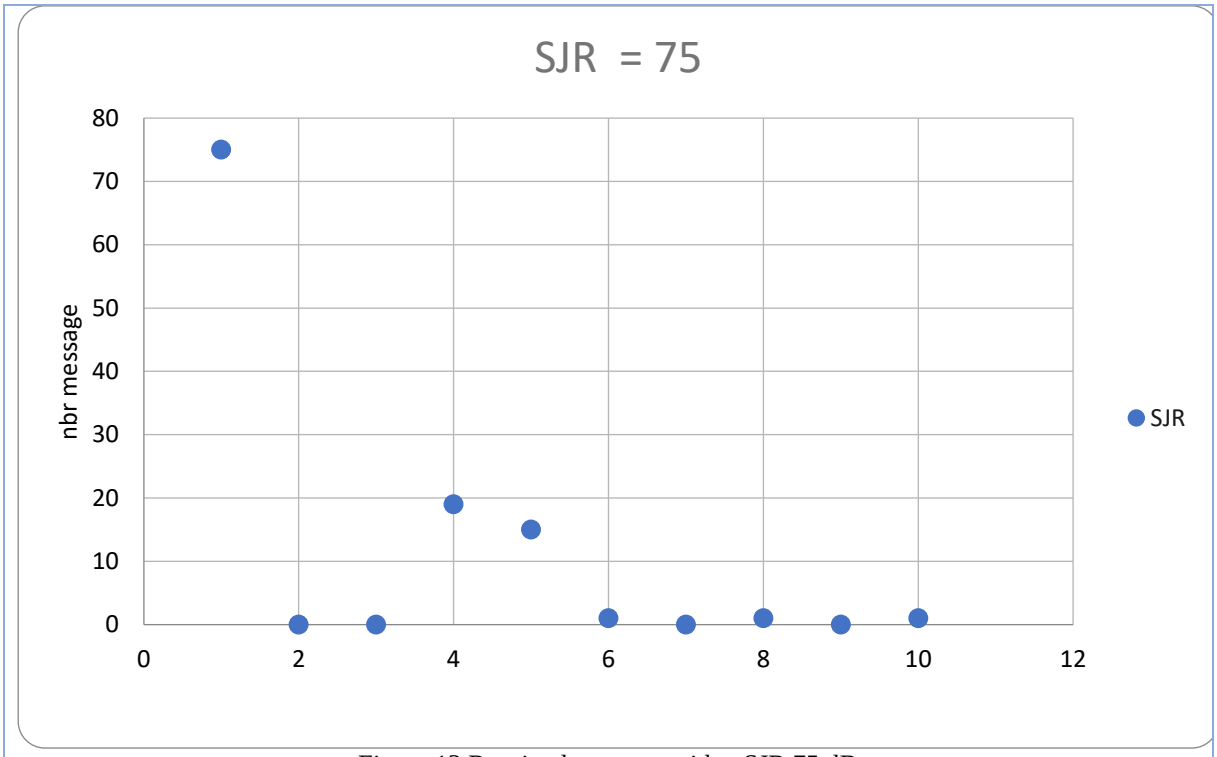


Figure 13 Received message with a SJR 75 dB

With a SJR of 75dB, most of the messages are not delivered. The conclusion is that the cards are very sensitive to jamming signal, even if the jamming signal doesn't have a lot of power.

Throughput

First, we have tested the throughput without jamming obtaining the following results presented in **Table** 2.

	No Jam	
Time (s)	MBytes	Débit (Mbit/sec)
1	0,45	3,74
2	0,47	3,93
3	0,48	4,04
4	0,48	3,98
5	0,5	4,19
6	0,49	4,1
7	0,48	4,05
8	0,49	4,09
9	0,49	4,1
10	0,5	4,16

Table 2 Communications throughput without perturbations

The throughput in clean conditions is between 3.7 Mbit/s and 4.20 Mbit/s. This will be used as our reference point for the rest of the tests.

Next, we have tested different sweep time with different jamming power. We present the obtained results in the following Table 3.

Jampow	ATT	43		53		63	
-42	SJR	**80**		**90**		**100**	
Time (s)		MBytes	Débit	MBytes	Débit	MBytes	Débit
1		0,02	0,16	0,02	0,2	0,27	2,29
2		0	0	0	0	0,31	2,57
3		0,01	0,07	0,05	0,45	0,3	2,55
4		0	0	0,01	0,07	0,37	3,08
5		0	0	0,11	0,93	0,33	2,75
6		0,01	0,07	0,11	0,9	0,31	2,6
7		0,01	0,12	0,05	0,45	0,33	2,77
8		0	0,1	0,06	0,46	0,31	2,58
9		0,01	0	0	0	0,33	2,8
10		0,02	0,12	0,02	0,17	0,32	2,68
v		4µs					
Jampow	ATT	45		55		65	
-40	SJR	**80**		**90**		**100**	
Time (s)		MBytes	Débit	MBytes	Débit	MBytes	Débit
1		0,02	0,13	0,11	0,95	0,45	3,76
2		0,01	0,08	0,07	0,59	0,44	3,7
3		0	0,02	0,04	0,3	0,44	3,66
4		0,02	0,16	0,06	0,52	0,44	3,72
5		0,01	0,12	0,08	0,64	0,47	3,97
6		0,02	0,2	0,07	0,57	0,43	3,6
7		0,02	0,15	0,06	0,51	0,48	4,04
8		0,01	0,05	0,13	1,05	0,45	3,81
9		0,01	0,1	0,07	0,6	0,45	3,81
10		0,01	0,08	0,05	0,45	0,46	3,87
		6µs					
Jampow	ATT	46		56		66	
-39	SJR	**80**		**90**		**100**	
Time (s)		MBytes	Débit	MBytes	Débit	MBytes	Débit
1		0,02	0,19	0,41	3,41	0,47	3,94
2		0,03	0,29	0,41	3,42	0,49	4,1
3		0,03	0,25	0,44	3,71	0,48	4,02
4		0,02	0,15	0,41	3,41	0,48	4,01
5		0	0,02	0,44	3,66	0,49	4,09
6		0,03	0,27	0,42	3,5	0,49	4,09
7		0	0,2	0,43	3,65	0,48	3,98
8		0,02	0,21	0,41	3,48	0,48	4,05
9		0,02	0,2	0,42	3,52	0,47	3,97

10		0,02	0,17	0,41	3,48	0,48	4,01
		8µs					
Jampow	ATT	47		57		67	
-38	SJR	**80**		**90**		**100**	
Time (s)		MBytes	Débit	MBytes	Débit	MBytes	Débit
1		0,02	0,2	0,38	3,21	0,45	3,81
2		0,01	0,05	0,43	3,61	0,49	4,1
3		0	0	0,41	3,48	0,49	4,08
4		0	0	0,44	3,73	0,49	4,12
5		0,03	0,27	0,44	3,66	0,48	4,04
6		0	0,03	0,41	3,41	0,46	3,88
7		0	0,01	0,45	3,81	0,48	4,01
8		0,02	0,14	0,43	3,6	0,48	4,01
9		0,01	0,07	0,42	3,52	0,48	4,07
10		0,01	0,08	0,43	3,63	0,49	4,09
		10µs					
Jampow	ATT	48		58		68	
-37	SJR	**80**		**90**		**100**	
Time (s)		MBytes	Débit	MBytes	Débit	MBytes	Débit
1		0,06	0,46	0,41	3,44	0,47	3,92
2		0,04	0,32	0,43	3,57	0,47	3,96
3		0,05	0,42	0,41	3,44	0,47	3,94
4		0,04	0,37	0,41	3,41	0,48	4,04
5		0,06	0,49	0,45	3,75	0,49	4,11
6		0,04	0,37	0,44	3,7	0,49	4,14
7		0,06	0,5	0,41	3,46	0,48	4,01
8		0,07	0,5	0,4	3,39	0,49	4,14
9		0,06	0,54	0,45	3,76	0,47	3,96
10		0,07	0,57	0,42	3,49	0,5	4,23
		12µs					
Jampow	ATT	49		59		69	
-36	SJR	**80**		**90**		**100**	
Time (s)		MBytes	Débit	MBytes	Débit	MBytes	Débit
1		0,03	0,29	0,44	3,73	0,45	3,79
2		0,01	0,12	0,43	3,64	0,48	4,03
3		0	0	0,44	3,68	0,45	3,81
4		0	0	0,44	3,67	0,48	4,01
5		0,03	0,28	0,41	3,41	0,5	4,23
6		0	0	0,45	3,74	0,51	4,24
7		0	0,3	0,44	3,71	0,49	4,12
8		0,04	0,08	0,44	3,66	0,49	4,04
9		0,01	0,17	0,44	3,71	0,48	4,15

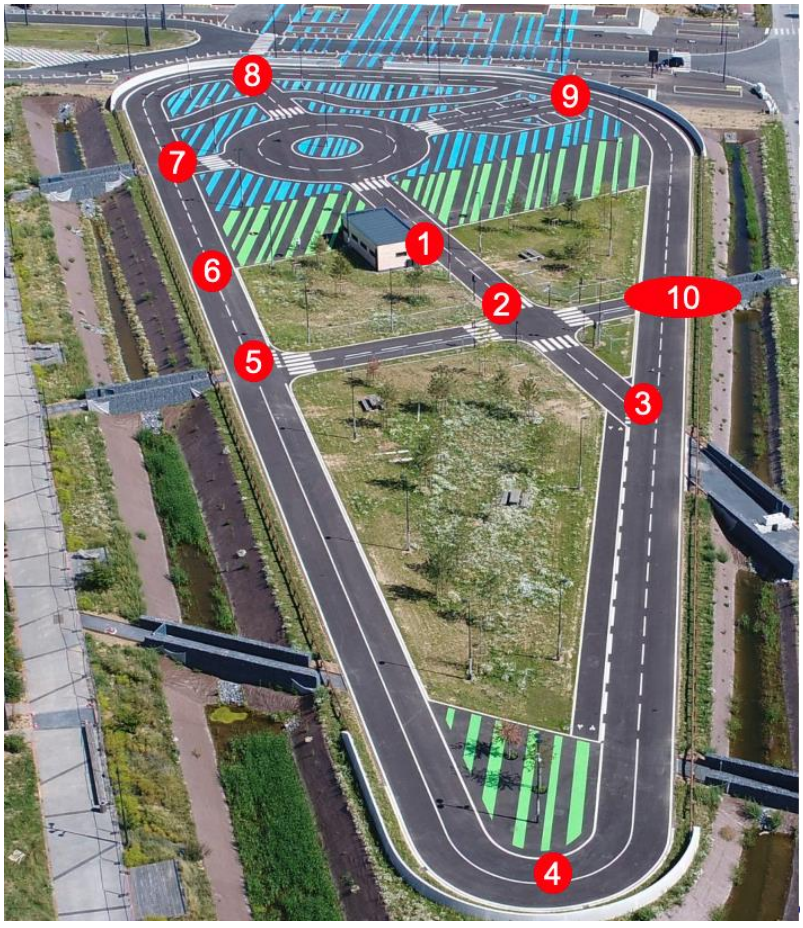
10		0,02	0,16	0,44	3,72	0,49	4,14
		16µs					
Jampow	ATT	50		60		70	
-35	SJR	**80**		**90**		**100**	
Time (s)		MBytes	Débit	MBytes	Débit	MBytes	Débit
1		0,04	0,32	0,39	3,31	0,43	3,59
2		0,03	0,22	0,46	3,86	0,48	4,05
3		0,01	0,1	0,46	3,83	0,47	3,96
4		0,03	0,28	0,46	3,88	0,51	4,31
5		0,04	0,24	0,44	3,66	0,49	4,13
6		0,02	0,3	0,46	3,85	0,45	3,8
7		0,04	0,19	0,45	3,75	0,5	4,18
8		0,05	0,34	0,43	3,61	0,48	4,07
9		0,02	0,45	0,45	3,76	0,49	4,12
10		0,02	0,2	0,43	3,61	0,5	4,2
		20µs					
Jampow	ATT	51		61		71	
-34	SJR	**80**		**90**		**100**	
Time (s)		MBytes	Débit	MBytes	Débit	MBytes	Débit
1		0,04	0,31	0,43	3,65	0,47	3,96
2		0,04	0,32	0,44	3,67	0,48	4,01
3		0,03	0,23	0,48	4,04	0,48	4,06
4		0,05	0,38	0,44	3,66	0,48	4,05
5		0,06	0,54	0,48	4,01	0,49	4,09
6		0,05	0,38	0,44	3,72	0,47	3,93
7		0,03	0,24	0,46	3,88	0,49	4,12
8		0,03	0,23	0,47	3,95	0,49	4,05
9		0,08	0,66	0,46	3,89	0,49	4,12
10		0,06	0,45	0,45	3,95	0,48	4,05

Table 3 Evaluated throughput under different jamming conditions

Conclusions / analysis in comparison with initial objective

IEEE 802.11p is sensible to jamming attacks, even if the jamming signal is low compared with the communication signal.
The conclusion is similar to the one in the previous test: the throughput decreases when the SJR increases. So the IEEE 802.11 is very sensitive to jamming.

3.1.3. Outdoor propagation tests

Jamming and performance tests on V2X communication – platform 2
Test purpose:
Identify propagation capabilities of the V2X equipment by measuring reception power based on the emitter distance to the receptor.
Initial conditions:
Cf. Section 2.5 for platform 5 description.
Tools used:
Cf. Section 2.5 for platform 5 description.
Test description:
A truck is moved to different positions at various positions and distance from the fix receptor. Singal analysis is performed for each position by analyzing received messages rate.
Expected results:
Messages rate received by the RSU.
Observed results:
The X axis (on top) is the number of tests that we made for the communication. The Y axis is the position of the OBU on the track.    Tests have been made 10 times for 1000 packets transmitted. ETSI messages were mainly received when the communication between the RSU and the OBU was in Line of Sight (LoS).

	Packet Delivery Rate en %				*10 mesures sur 1000 packets*					
Position / **Iteration**	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10
It. 1	5,7	4,3	3,5	4,1	3,7	3,4	3,4	3,3	3	3,9
It. 2	26	28	27	26	22	26	27	27	27	27
It. 3	89	89								
It. 4										
It. 5	99	99	99							
It. 6										
It. 7										
It. 8	87	86								
It. 9	99									
It. 10	21	20	20	20	22	21	20	19	10	10

The X axis (on top) is the number of tests that we made for the communication. The Y axis is the position of the OBU on the track.
Tests have been made 10 times for 1000 packets transmitted. ETSI messages were mainly received when the communication between the RSU and the OBU was in Line of Sight (LoS).
As expected, the 3 closest positions (p1, p2 and p3) have better results than others.
Also, out of sight position (p5, p6, et p7) have results similar to the furthest positions (p4, p8, p9, and p10).

Conclusions / analysis in comparison with initial objective

The results of these tests characterize quite clearly the capabilities of the OBU and RSU to communicate. In this project we did not defined thresholds because more feedback on average or acceptable performances must be provided. We do not conclude on those characteristics, but rather on the meaningfulness of the test that indeed allowed us to get necessary information to do so in the future.

3.2 Interoperability and security of communications

This section presents the different interoperability tests that we tried to perform unsuccessfully on the test platforms 3 and 4. That's why the table results use a grey colour theme to represent this fact. The lack of interoperability success should not be interpreted as a default of the tested products, but rather as the expression that (i) interoperability is in fact not a straightforward property, (ii) black box tests have limitations.
Based on project partners expertise, developer supports should have most likely helped to fix interoperability issues faced by the platforms.

3.2.1. Secure interoperability – Platform 3

Tests on secure association validation

Test purpose:

Evaluate V2X communication performances.
Initial conditions:
Cf. Section 2.3 for platform 3 description.
Tools used:
Cf. Section 2.3 for platform 3 description.
Test steps:
We used the wireshark tool to make eavesdropping of exchanges to understand the communications. Wireshark is is a powerful network analysis tool that is similar to tcpdump. It decodes captured packets and understands the different structures of communication protocols. Wireshark uses pcap to capture packets, so it only supports the network types supported by pcap. In this work, Wireshark is employed to parse and decode IEEE 802.11p frames and ETSI messages.
Expected results:
Only correctly signed certificates should be accepted.
Observed results:
It has been observed that during experiments IEEE 802.11p frames were emitted but nothing was received by the remote equipment. Important efforts have been made to set up correctly the platform, but without developer support testers did not managed to succeed to have the Lacroix and Codha equipment to interoperate.
Conclusions / analysis in comparison with initial objective
N/A.

3.2.2. Secure interoperability – Platform 4

The aim is to assess the safety of C-ITS equipment, and to create a methodology and a set of tests to perform. This methodology can then be reused to determine the associated level of IT risk.
An initial set of tests has been defined. It was based on initial work performed in SCA IRT system project and extended for PRISSMA. However, some technical issues related to black box testing context did not allow us to perform all those tests. One main limitation has been the impossibility for us to configure the security functions of the C-ITS communications. The equipment configuration did not include any ETSI 103 097 certificates. Even so, Eviden (not member of PRISSMA) has graciously loan PRISSMA partner a full C-ITS PKI access for this test, we did not manage to configure it and activate the signing and encrypting functions in this black box context.

Tests on secure association validation
Test purpose:
Ensure that the equipment cannot accept an invalid certificate as a parameter (expired, malformed, with an unsupported protocol, etc.).
Initial conditions:

Cf. Section 2.4 for platform 4 description.
Tools used:
Cf. Section 2.4 for platform 4 description.
Test steps:
1. Take a valid certificate and check that it is accepted by the application. 2. Changing a field contained in the signed part. 3. Check that the certificate is denied. 4. Repeat on all fields. 5. Send a self-signed certificate and verify rejection.
Expected results:
Only correctly signed certificates should be accepted.
Observed results:
N/A, we have not been able to upload certificates to the interface.
Conclusions / analysis in comparison with initial objective
N/A.

Functions: **Certificate management**	**Reference:** **Author: RGI** **Test purpose:** Ensure that the equipment cannot accept an invalid certificate as a parameter (expired, malformed, with an unsupported protocol, etc.).

Initial conditions:
Access to the OBU interface where certificates are loaded.
Tools used:
Burpsuite
Test steps:
6. Take a valid certificate and check that it is accepted by the application. 7. Changing a field contained in the signed part. 8. Check that the certificate is denied. 9. Repeat on all fields. 10. Send a self-signed certificate and verify rejection.
Expected results:
Only correctly signed certificates should be accepted.
Observed results:
N/A, we have not been able to upload certificates to the interface.
Conclusions / analysis in comparison with initial objective
N/A.

Functions:	**Reference**: **Author**: RGI **Test purpose:** Verify the constraints imposed by EtsiTs103097.

Certificate management
Initial conditions:
Access to the OBU interface where certificates are loaded.
Tools used:
Titan: https://forge.etsi.org/rep/ITS/ITS/tree/STF525
Test steps:
1. "_CertificateId_" is either of type "_name_" or "_none". 2. cracaId_ = 000000'H 3. crlSeries = 0'D 4. includes a "_validityPeriod". 5. at least one component "_appPermissions_" or "_certIssuePermissions_" shall be present and define signing permission. 6. the component "_encryptionKey_" of type "_PublicEncryptionKey_". 7. the digest of certificate has been calculated using proper hash algorithm (SHA-256 or SHA-384) after certificates canonicalization. 8. Check that end_validity is greater than "start_validity". 9. Check that all AIDs containing in the in the "its_aid_list" are unique. 10. The subject_name variable-length vector has a maximum length of 32 bytes.
Expected results:
All constraints must be implemented and compliant.
Observed results:
N/A, no certificates were present on the system, and we could not add any.
Conclusions / analysis in comparison with initial objective
N/A.

Functions: Message protection	**Reference**:	**Author**: RGI
	Test purpose: Ensure that the equipment accept only correctly signed messages.	

Initial conditions:
Access to the OBU interface where certificates are loaded and to the EBR.
Tools used:
GNURadio with (https://github.com/bastibl/gr-ieee802-11) *Titan (https://forge.etsi.org/rep/ITS/ITS/tree/STF525)*
Test steps:
1. Intercept signed OBU radio messages. 2. Modify the message without changing the signature (or without the signature). 3. Check whether the message is accepted by the ToE.

Expected results:
Only correctly signed certificates should be accepted.
Observed results:
N/A, we have not been able to upload certificates through the interface.
Conclusions / analysis in comparison with initial objective
N/A.

Functions: PKI managment	**Reference**:	**Author**: RZA
	Test purpose: Verify that the TOE send secured requests to the PKI when enrolling or requesting for new EC.	

Initial conditions:
ToE system access.
Tools used:
Titan: https://forge.etsi.org/rep/ITS/ITS/tree/STF525
Test steps:
1. Modify the current EC information provided in the PKI request to verify that a new EC based on known attacker information cannot be sent to the TOE. 2. Add additional unsigned or unencrypted field to the request to make the PKI generate a new certificate based on those rogue elements known to the attacker. 3. Replace the data encryption key sent to the PKI and used to encrypt the answer containing the replied EC. 4. Eave drop the PKI request and try to extract the data encryption key to latter disclose EC sent to the TOE.
Expected results:
EC Exchanges are carried out securely, regardless of the fields or data sent to the ToE.
Observed results:
N/A.
Conclusions / analysis in comparison with initial objective
N/A. We have not been able to upload certificates to the interface.

Functions: PKI managment	**Reference**:	**Author**: RZA
	Test purpose: Verify that the TOE send secured requests to the PKI when requesting for new ATs.	

Initial conditions:
ToE system access.
Tools used:

Titan: https://forge.etsi.org/rep/ITS/ITS/tree/STF525
Test steps:
1. Try to modify the current EC information provided in the PKI request to verify that AT based on attacker information cannot be sent to the TOE. 2. Add additional unsigned or unencrypted field to the request to make the PKI generate a new certificate based on those rogue elements. 3. Replace the data encryption key sent to the PKI and used to encrypt the answer containing the replied EC. 4. Eave drop the PKI request and try to extract the data encryption key.
Expected results:
EC Exchanges are carried out securely, regardless of the fields or data sent to the ToE.
Observed results:
N/A.
Conclusions / analysis in comparison with initial objective
N/A. We have not been able to upload certificates to the interface.

4 CONCLUSION

In conclusion, the project involved several tests, but these should be viewed as validation of the evaluation process rather than the validation of the products composing the 5 platforms presented in section 2.
No definitive conclusions about the test targets should be drawn from the results. First this is not the goal of this deliverable, and second from our point of view the tests conditions were not appropriate for that. This actually clearly emphases the need identified in PRISSMA deliverable 5.3 to have more in-depth validation of critical ARTS components that require a more important involvement of the developer, who should provide more information and help (not accessible within PRISSM resources) concerning their products.
It is worth noting that despite significant efforts, the testing only covered a portion of the entire system functionalities, demonstrating that the tests are time-consuming and challenging to exhaustively conduct.
Nonetheless, they have yielded significant insights. There is a need to improve the efficiency and maturity of these tests. Some attacks remain uncounterable (cf jamming tests results in sections and must be addressed through detection and procedural measures. While blackbox testing is appealing due to its ease of setup, it has substantial limitations in evaluating critical components. The results also highlight that achieving interoperability is complex and not straightforward.

REFERENCES

[1] O.C. Zienkiewicz, R.C. Taylor, *The finite element method, Vol. I, 4th Edition*. McGraw Hill, 1989.

[2] J.T. Oden, T. Belytschko, I. Babuska, T.J.R. Hughes, Research directions in computational mechanics. *Computer Methods in Applied Mechanics and Engineering*, **192**, 913-922, 2003.