TRAFICOM
Finnish Transport and Communications Agency

Piloting cybersecure and interoperable cellular C-ITS services

Niko Kynsijärvi, Timo Majala
Johan Scholliers, Kimmo Kauvo, Sami Lehtonen

Nordic WAY

Co-funded by
the European Union

Traficom Research Reports
Traficomin tutkimuksia ja selvityksiä
Traficoms forskningsrapporter och utredningar

12/2024

TRAFICOM
Finnish Transport and Communications Agency

Date of publication
29.5.2024

Title of publication
Piloting cybersecure and interoperable cellular C-ITS services

Author(s)
Niko Kynsijärvi, Timo Majala, Johan Scholliers, Kimmo Kauvo, Sami Lehtonen

Commissioned by, date
Traficom

Publication series and number
Traficom Research Reports 12/2024

ISSN (e-publication) 2342-0294
ISBN (e-publication) 978-952-311-923-9

Keywords
C-ITS, C-V2X, 3GPP, EU CCMS, V2X, LTE-V2X

Abstract

C-ITS stands for Cooperative Intelligent Transport Systems, which enable ITS-stations to interact and cooperate by exchanging secured and trusted messages. There are two channels for exchanging these messages: long-range utilizing commercial cellular networks and short-range using direct communication. In Europe, ITS-G5 technology has been most used short-range technology, but recently 3GPP's C-V2X has emerged as a potential alternative.

The objectives of this study were divided into three sections. 1) Deploy and demonstrate EU-wide EU CCMS system, 2) Test and demonstrate the operation of C-V2X (LTE-V2X) technologies defined by 3GPP, and 3) Investigate the applicability and compatibility of C-Roads platform specifications together with C-V2X technologies. To achieve these objectives, C-Roads platform specified C-ITS service was implemented at a traffic-light controlled intersection.
The test intersection was equipped with an LTE-V2X capable Road Side Unit (RSU) that could directly communicate with a vehicle equipped with an LTE-V2X On Board Unit (OBU). C-ITS messages from the Traffic Light Controller were simultaneously transmitted to both the RSU and the Tampere C-ITS Node (TLEX platform). From the Tampere C-ITS Node, messages were distributed to a mobile application through Nodeon Finland's C-ITS service provider back-end system. The communication between RSU and OBU was secured using ETSI certificates issued by a Root Certificate Authority included in the EU CCMS.

Tests were conducted to study and evaluate the performance of short-range communication together with long-range communication. These tests examined factors such as security and overall latency. Results from these tests indicated that the latencies were in the same range for both communication methods. However, long-range communication did not include the signing of messages, leaving potential effects resulting from out of these results.

Based on the results, conclusions and recommendations are provided both for C-ITS station operators and authorities. The LTE-V2X technology used is expected to have a relatively short lifetime as it is being replaced with NR-V2X technology. In the future, the deployment of C-ITS will require a transition to security level 2 of EU CCMS, creating requirements for C-ITS station operators and devices. One of these requirements will be ISO 27001 compliance.

The results indicated that both short- and long-range communication solutions provided a well-functioning platform for informative C-ITS applications. Each of these solutions had its own unique set of advantages and disadvantages. The large-scale deployment of short-range C-ITS stations would require physical installations, ongoing maintenance, and active operation by the responsible party. As for long-range solutions, the next phases of the development of connected and automated driving may generate a demand for guaranteed quality of communication, a feature not currently provided by best-effort mobile networks.

To ensure the interoperability and compatibility of C-ITS services across Europe, it is important that Finnish authorities in the future work even more closely within the joint initiative of European Member States and road operators, C-Roads.

Contact person Anna Schirokoff	Language English	Confidentiality rating Public	Pages, total 72

Distributed by Traficom	Published by Traficom

TRAFICOM
Liikenne- ja viestintävirasto

Julkaisupäivämäärä
29.5.2024

Julkaisun nimi
C-ITS Pilotti: Kyberturvallisuus, yhteentoimivuus ja matkaviestinteknologiat

Tekijät
Niko Kynsijärvi, Timo Majala, Johan Scholliers, Kimmo Kauvo, Sami Lehtonen

Toimeksiantaja ja asettamispäivämäärä
Trafiom

Julkaisusarjan nimi ja numero **Traficomin tutkimuksia ja selvityksiä 12/2024**	ISSN (verkkojulkaisu) 2342-0294 ISBN (verkkojulkaisu) 978-952-311-923-9

Asiasanat
C-ITS, C-V2X, 3GPP, EU CCMS, V2X, LTE-V2X

Tiivistelmä

Vuorovaikutteiset älykkäät liikennejärjestelmät (engl. C-ITS) ovat liikennejärjestelmiä, jotka kykenevät kommunikoimaan muiden älykkäiden liikennejärjestelmien kanssa vaihtamalla eurooppalaisen luottamusmallin mukaisia C-ITS-viestejä. Tämä viestinvaihto voidaan toteuttaa käyttämällä kaupallisia matkapuhelinverkkoja tai suoraa järjestelmien välistä kommunikaatiota. Euroopassa suora kommunikaatio on toteutettu yleisesti ITS-G5 teknologialla, joskin viime aikoina 3GPP:n standardoima C-V2X teknologia on alkanut yleistymään potentiaaliseksi vaihtoehdoksi.

Tämän työn tavoitteet on jaettu kolmeen osaan: 1) Testata ja demonstroida EU:n laajuista EU CCMS järjestelmää, 2) testata 3GPP:n C-V2X (LTE-V2X) teknologian toimintaa ja 3) tutkia C-V2X teknologian yhteensopivuutta C-Roads mukaisten palvelujen kanssa. Näiden tavoitteiden saavuttamiseksi liikennevalo-ohjattuun risteykseen toteutettiin C-Roads spesifikaatioiden mukainen C-ITS-palvelu.

Testiristeys varusteltiin LTE-V2X kyvykkäällä tienvarsiyksiköllä (RSU), joka kommunikoi suoraan LTE-V2X ajoneuvoyksiköllä (OBU) varusteltuun ajoneuvoon. Liikennevalojen ohjauskojeesta tulevia C-ITS-viestejä välitettiin samaan aikaan tienvarsiyksikköön sekä Tampereen C-ITS solmupisteeseen (TLEX-alusta). Tampereen C-ITS solmupisteestä viestit jaeltiin mobiilisovellukseen Nodeonin kehittämän C-ITS palveluntarjoajakerroksen kautta. Viestintä tienvarsiyksikön ja ajoneuvoyksikön välillä oli suojattu käyttäen ETSI:n standardoimia varmenteita, joiden jakelu toteutettiin EU CCMS -järjestelmään kuuluvan juurivarmentajan (RCA, Root Certificate Authority) toimesta.

Testejä suoritettiin lyhyen- ja pitkän kantaman kommunikaatiokanavien suorituskykyjen arvioimiseksi esimerkiksi viiveiden ja tietoturvallisuuden osalta. Testien tulokset viittaavat molempien kommunikaatiokanavien viiveiden olevan samaa luokkaa. Tässä yhteydessä on kuitenkin hyvä huomioida~~,~~ ettei pitkän kantaman kommunikaatiossa suoritettu viestien allekirjoitusta, joten allekirjoituksen mahdolliset vaikutukset eivät näy näissä testituloksissa.

Tulosten perusteella esitetään suosituksia ja johtopäätöksiä niin C-ITS operaattoreille kuin viranomaisille. Projektissa käytetylle LTE-V2X teknologialle odotetaan varsin lyhyttä elinkaarta, koska se tullaan korvaamaan tulevaisuudessa uudella NR-V2X teknologialla. Tulevaisuudessa C-ITS järjestelmien käyttöönotto edellyttää siirtymistä EU CCMS -järjestelmän tasolle 2. Tämä luo uusia vaatimuksia C-ITS operaattoreille ja järjestelmille, kuten ISO 27001 kyberturvallisuusstandardin noudattaminen.

Tulokset osoittavat, että molemmat, kaupallisen matkapuhelinverkon kautta tapahtuva pitkän kantaman kommunikaatio sekä lyhyen kantaman ratkaisu, voivat tarjota varsin hyvin toimivan alustan informatiivisten C-ITS-palvelujen käyttöönotolle. Jatkossa haasteet laajamittaisen lyhyen kantaman laiteinfrastruktuurin toteuttamisen osalta voivat liittyä huomattavaan määrään fyysisten laitteiden asennuksia sekä niiden jatkuvaan ylläpitoon ja operointiin. Pitkän kantaman ratkaisun mahdolliset ongelmat voivat liittyä yhteistoiminnallisen ja automatisoituvan liikenteen kehityksen tuleviin vaiheisiin, joiden toiminta saattaa vaatia verkkoalustalta palvelun laatuun ja verkon peittoon liittyviä takuita, jota mobiiliverkko ei tällä hetkellä pysty takaamaan.

Euroopan laajuisten C-ITS palvelujen yhteentoimivuuden ja -sopivuuden varmistamiseksi on olennaista, että Suomen viranomaiset tiivistävät jatkossa yhteistyötään entisestään Euroopan jäsenvaltioiden ja tieliikenteen harjoittajien yhteishankkeessa, C-Roadsissa.

Yhteyshenkilö Anna Schirokoff	Raportin kieli Englanti	Luottamuksellisuus Julkinen	Kokonaissivumäärä 72
Jakaja Traficom	Kustantaja Traficom		

Liikenne- ja viestintävirasto

Utgivningsdatum
29.5.2024

Publikation
C-ITS Pilot: Cybersäkerhet, interoperabilitet och mobilnätsteknik

Författare
Niko Kynsijärvi, Timo Majala, Johan Scholliers, Kimmo Kauvo, Sami Lehtonen

Toimeksiantaja ja asettamispäivämäärä
Traficom

Publikationsseriens namn och nummer **Traficoms undersökningar och utredningar 12/2024**	ISSN (elektronisk publikation) 2342-0294 ISBN (elektronisk publikation) 978-952-311--923-9

Ämnesord
C-ITS, C-V2X, 3GPP, EU CCMS, V2X, LTE-V2X

Sammandrag

Samverkande intelligenta transportsystem (eng. C-ITS) är transportsystem som kan kommunicera med andra intelligenta transportsystem genom utbyte av C-ITS-meddelanden enligt den europeiska förtroendemodellen. Detta meddelandeutbyte kan genomföras genom att använda kommersiella mobilnät eller direkt kommunikation mellan systemen. I Europa har direkt kommunikation i allmänhet genomförts med tekniken ITS-G5, men på senare tid har tekniken C-V2X, som standardiserats av 3GPP, börjat bli allmännare som potentiellt alternativ.

Målen för detta arbete har delats in i tre delar: 1) Testa och demonstrera de EU-omfattande EU CCMS-systemen, 2) testa funktionen för tekniken 3GPP C-V2X (LTE-V2X) och 3) undersöka kompatibiliteten för tekniken C-V2X med tjänster enligt C-Roads. För att uppnå dessa mål genomfördes en C-ITS-tjänst enligt C-Roads specifikationer i en trafikljusstyrd korsning.

Provningskorsningen utrustades med en LTE-V2X-begåvad vägkantsenhet (RSU) som kommunicerar direkt med ett fordon utrustat med ombordenheten LTE-V2X (OBU). C-ITS-meddelandena från trafikljusens styrinstrument förmedlades samtidigt till vägkantsenheten och till C-ITS-knutpunkt (TLEX-plattformen) i Tammerfors. Meddelandena till C-ITS-knutpunkten i Tammerfors distribuerades till en mobilapplikation via skiktet av C-ITS-tjänsteleverantörer som Nodeon utvecklat. Kommunikationen mellan vägkants- och ombordenheten skyddades genom att använda ETSI-standardiserade certifikat, vars distribution genomfördes av en rotcertifikatutfärdare (RCA, Root Certificate Authority) som hör till systemet EU CCMS.

Testerna utfördes för att bedöma prestandan för kommunikationskanalerna med kort och lång räckvidd, till exempel beträffande fördröjningar och informationssäkerhet. Resultaten av testerna tyder på att fördröjningarna i båda kommunikationskanalerna är i samma klass. I detta sammanhang är det dock bra att observera att ingen signatur av meddelandena gjordes i kommunikationen med lång räckvidd, så eventuella effekter av signaturen syns inte i dessa testresultat.

Utifrån resultaten presenteras rekommendationer och slutsatser för såväl C-ITS-operatörer som myndigheter. En ganska kort livscykel förväntas för tekniken LTE-V2X som användes i projektet, eftersom den kommer att ersättas med den nya tekniken NR-V2X i framtiden. I framtiden kräver ibruktagandet av C-ITS-systemen en övergång till nivå 2 i EU:s CCMS-system. Detta skapar nya krav för C-ITS-operatörer och system, till exempel iakttagande av cybersäkerhetsstandarden ISO 27001.

Resultaten visar att både kommunikationen med lång räckvidd och kort räckvidd som sker via kommersiella mobilnät kan erbjuda en mycket välfungerande plattform för ibruktagandet av informativa C-ITS-tjänster. I fortsättningen kan utmaningarna för utbyggnaden av en omfattande infrastruktur för utrustningen för kort räckvidd hänföra sig till ett betydande antal installationer av fysisk utrustning samt till kontinuerligt underhåll och drift av den. Eventuella problem med lösningen för lång räckvidd kan hänföra sig till kommande skeden i utvecklingen av samverkande och automatiserade transporter, vars funktion kan kräva garantier i anknytning till nätplattformens kvalitet på tjänsten och täckning av nätet, vilket mobilnätet för närvarande inte kan garantera.

För att säkerställa interoperabiliteten och kompatibiliteten mellan de transeuropeiska C-ITS-tjänsterna är det väsentligt att de finländska myndigheterna i fortsättningen intensifierar sitt samarbete ytterligare i det gemensamma projektet C-Roads mellan de europeiska medlemsstaterna och vägtrafikoperatörerna.

Kontaktperson Anna Schirokoff	Rapportens språk Engelska	Sekretessgrad Offentlig	Sidantal 72
Distribution Traficom	Förlag Traficom		

GLOSSARY

ADAS	Advanced Driver Assistance Systems
ASN.1	Abstract Syntax Notation One
CA	Certificate Authority
CAM	Cooperative Awareness Message
CCAM	Cooperative Connected and Automated Mobility
CCMS	C-ITS Credential Management System
C-ITS	Cooperative Intelligent Transport Systems
CPA	C-ITS Certificate Policy Authority
CPOC	C-ITS Point of Contact
CPS	Collective Perception Service
CSMS	Cyber Security Management System
C-V2X	Cellular Vehicle-to-Everything (includes both cellular and short-range communications)
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
ECTL	European Certificate Trust List
ETSI	European Telecommunications Standards Institute
GLOSA	Green Light Optimal Speed Advisory
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
I2V	Infrastructure-to-Vehicle
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Standard Organization
ITS	Intelligent Transport System
ITS-G5	European standard for vehicular communications based on the IEEE-1609.x and IEEE-802.11p standards
IVIM	Infrastructure to Vehicle Information

LAN	Local Area Network
LTE	Long Term Evolution
LTE-V2X	3GPP specified V2X technology that encapsulates both direct and mobile network communications
LTE-V2X Direct	3GPP short range communication technology, specified in 3GPP Release 14
MAC	Medium Access Control
MAPEM	MAP (infrastructure topology) extended message
MEC	Multi-Access Edge Computing
MHz	Megahertz
MNO	Mobile Network Operator
NIS	Network and Information Systems Directive
NIS2	Network and Information Systems Directive 2
NR	New Radio
NR-V2X Direct	3GPP short range communication technology, specified in 3GPP Release 16/17
ntp	The Network Time Protocol is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks
OBU	On-Board Unit
OEM	Original Equipment Manufacturer
PCI DSS	Payment Card Industry Data Security Standard
PKI	Public Key Infrastructure
QoS	Quality of Service
RCA	Root Certificate Authority
RSU	Road-Side Unit
R-ITS-S	Roadside ITS Station
SI	Signalized Intersections
SLA	Service Level Agreement
SME	Small and medium-sized enterprises
SOG-IS	Senior Officials Group – Information Systems Security

SPATEM	Signal Phase and Timing extended message
SREM	Signal Request Extended Message
SSEM	Signal Status Extended Message
SSP	Service Specific Permissions
TF	Task Force
TLC	Traffic Light Controller
TLEX	Platform to connect roadside equipment to information brokers, provided by Monotch, deployed in Tampere
TLS	Traffic Light Signal
V-ITS-S	Vehicle ITS Station
TLM	Trust List Manager
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
V2V	Vehicle-to-Vehicle
V2X	Vehicle-To-Everything
WG	Work Group
3GPP	3rd Generation Partnership Project
5GAA	The 5G Automotive Association
5G-V2X	C-V2X based on 5G NR technologies

FOREWORD

Road transport authorities have for several years developed and tested exchanging messages between vehicles and vehicles and infrastructure both nationally and in cooperation with other countries. In Finland, message exchange using mobile networks has especially been developed in cooperation with other Nordic countries in the so-called NordicWay project. During the years it was understood that such services, i.e. C-ITS or Co-operative Intelligent Transport System services, are an integral and fundamental part of enabling automated driving.

The aim of this study was to prove the compatibility of the security credential management system of EU’s C-ITS system with the 5.9 Ghz mobile network technologies and long-distance, either commercial or private, mobile networks, as well as the compatibility of the aforementioned with the C-ITS services defined in C-Roads. Additionally, the aim of the project was to support and further the implementation of services according to the ITS Directive in Finland. A pilot was carried out in the project in a real road transport environment in Finland.

The principal and client of the project was the Finnish Transport and Communications Agency. The steering group of the project included Anni Hytti, Anna Schirokoff, Pekka Pussinen, Jussi Aholainen and Kristiina Jaatinen from the Finnish Transport and Communications Agency, Olli Rossi from Fintraffic Oy, Mika Kulmala from the City of Tampere and Antti Paasilehto from the Ministry of Transport and Communications. Timo Majala and Niko Kynsijärvi from Nodeon Finland Oy, as well as Johan Scholliers, Kimmo Kauvo and Sami Lehtonen from VTT Technical Research Centre of Finland were responsible for the study. The work was part of the joint Nordic NordicWay 3 project, which received financial support from the Connecting Europe Facility (CEF) in the years 2019–2023.

Helsinki, 29 May 2024

Anni Hytti
Chief Adviser
Finnish Transport and Communications Agency Traficom

ALKUSANAT

Tieliikenteen viranomaiset ovat jo useiden vuosien ajan kehittäneet ja kokeilleet viestien välittämistä ajoneuvojen sekä ajoneuvojen ja infran välillä niin kansallisesti kuin muidenkin maiden kanssa yhteistyössä. Suomessa on erityisesti kehitetty viestien vaihtoa matkaviestinverkkoa hyödyntäen yhteistyössä muiden Pohjoismaiden kesken niin kutsutussa NordicWay-yhteistyössä. Vuosien saatossa on ymmärretty, että tällaiset palvelut, ns. C-ITS eli Co-operative Intelligent Transport System -palvelut ovat olennainen ja perustavaa laatua oleva pohja automaattiajamisen mahdollistamiseksi.

Tämän työn tavoitteena oli osoittaa EU:n C-ITS-järjestelmien turvatunnusten hallintajärjestelmän yhteensopivuus 5,9 GHz - matkaviestinteknologioiden ja pitkän kantaman, joko kaupallisten tai yksityisten, matkaviestinverkkojen kanssa sekä edellä mainittujen yhteentoimivuus C-Roadsissa määriteltyjen C-ITS-palveluiden kanssa. Lisäksi Hankkeen tavoitteena oli tukea ja edistää ITS-direktiivin mukaisten palveluiden käyttöönottoa Suomessa. Hankkeessa toteutettiin pilotti todellisessa tieliikenneympäristössä Suomessa.

Työn toimeksiantajana ja tilaajana toimi Liikenne- ja viestintävirasto. Työn ohjausryhmään kuuluivat Anni Hytti, Anna Schirokoff, Pekka Pussinen, Jussi Aholainen ja Kristiina Jaatinen Liikenne- ja viestintävirastosta, Olli Rossi Fintraffic Oy:stä, Mika Kulmala Tampereen kaupungilta ja Antti Paasilehto liikenne- ja viestintäministeriöstä. Työstä vastasivat Nodeon Finland Oy:sta Timo Majala ja Niko Kynsijärkvi, sekä Teknologian tutkimuskeskus VTT Oy:sta Johan Scholliers, Kimmo Kauvo ja Sami Lehtonen. Työ oli osa yhteispohjoismaista NordicWay 3 -hanketta, joka sai Verkkojen Eurooppa -ohjelman (CEF, Connecting Europe Facility) rahoitustukea vuosina 2019– 2023.

Helsinki, 29. toukokuuta 2024

Anni Hytti
Johtava asiantuntija
Liikenne- ja viestintävirasto Traficom

FÖRORD

Vägtrafikmyndigheterna har redan i flera år utvecklat och prövat på att förmedla meddelanden mellan fordon samt mellan fordon och infrastruktur, både nationellt och i samarbete med andra länder. I Finland har man i synnerhet utvecklat utbytet av meddelanden genom att utnyttja mobilnätet i samarbete med de övriga nordiska länderna i det så kallade NordicWay-samarbetet. Under årens lopp har man förstått att sådana här tjänster, så kallade C-ITS eller Co-operative Intelligent Transport System-tjänster, är väsentliga och grundläggande för att möjliggöra automatisk körning.

Syftet med detta arbete var att visa att EU:s system för hantering av C-ITS-systemens säkerhetskoder är kompatibelt med mobilnätstekniken på 5,9 GHz och med lång räckvidd, antingen kommersiella eller privata, samt interoperabiliteten för ovan nämnda med de C-ITS-tjänster som definieras i C-Roads. Dessutom var målet med Projektet att stödja och främja ibruktagandet av tjänster i Finland enligt ITS-direktivet. I projektet genomfördes ett pilotprojekt i en verklig vägtrafikmiljö i Finland.

Transport- och kommunikationsverket var uppdragsgivare och beställare av arbetet. Till styrgruppen hörde Anni Hytti, Anna Schirokoff, Pekka Pussinen, Jussi Aholainen och Kristiina Jaatinen från Transport- och kommunikationsverket, Olli Rossi från Fintraffic Ab, Mika Kulmala från Tammerfors stad och Antti Paasilehto från kommunikationsministeriet. För arbetet ansvarade Timo Majala och Niko Kynsijärvi från Nodeon Finland Oy samt Johan Scholliers, Kimmo Kauvo och Sami Lehtonen från Teknologiska forskningscentralen VTT Ab. Arbetet var en del av det samnordiska projektet NordicWay 3 som under 2019–2023 fick finansiering från Fonden för ett sammanlänkat Europa (CEF, Connecting Europe Facility).

Helsingfors, den 29 Maj 2024

Anni Hytti
Ledande sakkunnig
Transport- och kommunikationsverket Traficom

Contents

Figures

Tables

1 Introduction

1.1 Background

Cooperative Intelligent Transport Systems (C-ITS) represent a subset of Intelligent Transport Systems (ITS), facilitating the exchange of information among various stakeholders, including road users, roadside infrastructure and other ITS systems. Over the past several years, there has been extensive testing and experimentation of C-ITS services at a national level. In Finland, particular emphasis has been placed on advancing data exchange through mobile networks. This work has often been done in collaboration with other Nordic countries, where the long-term co-Nordic NordicWay projects have provided a suitable platform for joint Nordic research, development and demonstrations for these technologies.

The testing and development work conducted within both co-Nordic and national Research and Development (R&D) projects has demonstrated that mobile network technologies possess the capability to serve as the foundational infrastructure for current informative C-ITS systems.

Finland has actively participated in the C-Roads Platform, a collaborative initiative among European Member States and road operators. The primary objective of this initiative is to test and implement C-ITS deployment across Europe, with a specific emphasis on achieving cross-border harmonisation and interoperability.

The definition and development efforts of C-Roads as well as other European C-ITS activities using short-range communication have largely relied on the ITS-G5 standard defined by the European Telecommunication Standards Institute (ETSI). Concurrently, the 3rd Generation Partnership Project (3GPP), a consortium of seven telecommunications standard development organisations, has been active in developing an alternative C-V2X Direct standard based on mobile network technologies. C-V2X Direct has garnered an enthusiastic reception in the market and has rapidly established itself as a clear competitor in the device manufacturing sector, providing a distinct alternative to the ITS-G5 standard.

There have been uncertainties regarding which of these two technologies will emerge as the primary V2X direct communication technology. This situation is further complicated as both technologies operate within the same communication frequency band and lack interoperability and compatibility. In Europe, some car manufacturers have already integrated ITS-G5 technology into their vehicles, but most recently a group of major automotive manufacturers have shifted commitment towards new generation 5G-V2X for V2X technology in Europe [16].

In accordance with the EU's C-ITS strategy, as outlined in COM (2016) 766 and COM (2018) 283, the European Commission has undertaken extensive collaboration to enhance the information and cybersecurity of C-ITS systems. This effort has involved the development of common European information security policies and a common cybersecurity platform solution (EU CCMS, EU C-ITS Credential Management System). The primary focus of EU CCMS is to guarantee the integrity, confidentiality and availability of exchanged C-ITS messages by employing a European-level Public Key Infrastructure (PKI).

The security requirements in accordance with EU CCMS primarily serve as specifications for securing communication in C-ITS short-range applications between roadside units (RSU) and onboard units (OBU).

1.2 Purpose and scope of the study

The objectives of the study can be divided into three different sections:

1. to deploy and demonstrate an EU-wide EU CCMS system, which ensures the safety of C-ITS systems by providing trust.
2. to test and demonstrate the operation of C-V2X (LTE-V2X) technologies defined by 3GPP.
3. to investigate the applicability and compatibility of C-Roads platform specifications together with C-V2X technologies.

This project aimed to achieve these objectives by deploying a C-ITS I2V (Infrastructure to Vehicle) service at a traffic light controlled intersection defined by C-Roads platform specifications (SI, Signalised Intersections). The intersection was equipped simultaneously with short-range communication capability using LTE-V2X Direct and long-range communication capability utilising commercial mobile networks. LTE-V2X Direct communication was secured with PKI (Public Key Infrastructure) certificates following EU CCMS guidelines.

2 Methods

2.1 Project structure

The project consisted of the following phases:

1. Design phase: development of the system architecture, and the specification of the tests to be performed. In this phase the test site was selected and the system components were specified. The system is further discussed in Section 7.1.
2. Development and deployment: in this phase the interfaces between different components, if not yet available, were developed. The components were installed on site and tested. Deployment-related issues are described in Section 7.2.
3. Functional testing: during this phase the tests were performed. The main target of the testing was the communication performance, as well as issues related to the use of the C-ITS trust model. Physical tests are described in Section 8.2 and the results of these tests in Section 8.3.
4. Reporting and recommendations: the conclusions and recommendations based on the results from the tests are presented in Section 9.

2.2 Research questions

The main research questions for this study were:

- Can the C-ITS trust model (EU CCMS) Level 0 be used for both short-range and long-range communications?
- How suitable are C-V2X (long-range and short-range) technologies for implementing C-ITS services, and how do they perform?
- Is LTE-V2X Direct a feasible solution for transmitting C-ITS messages, and can it be used to implement C-Roads-specified C-ITS services?

For the definition of the test cases, the C-Roads test specifications for cross-border tests were used as much as possible. The tests were adapted towards the solutions used in this project (replacing ITS-G5 with LTE-V2X), and without the cross-border context. The tests are specified in more detail in Table 5 in Section 8.1.

3 Cooperative Intelligent Transport Systems (C-ITS)

3.1 Definition

Intelligent Transport Systems (ITS) encompass advanced technologies and services that use information and communications technology to enhance safety and address transportation challenges, such as reducing emissions, minimising traffic congestion and preventing accidents.

Cooperative Intelligent Transport Systems (C-ITS) refer to intelligent transport systems that enable ITS users to interact and cooperate by exchanging secured and trusted messages, without any prior knowledge of each other and in a non-discriminatory manner [10]. C-ITS encompasses a group of ITS technologies and applications that allow data exchange through wireless communication technologies between components and actors of the transport system either between vehicles (vehicle to vehicle, V2V) or between vehicle and infrastructure (vehicle to infrastructure, V2I) [1]. The general term for all communication types is vehicle-to-everything (V2X). These communication types enable offering road users different types of C-ITS services. Road users can get information in advance of roadworks in their route, warnings of potential hazardous locations, information of road or lane closings or even real-time information from the traffic lights ahead. These types of services help road users make better decisions. From the road operators' perspective these services can help reduce travel times, lower emissions, provide real-time insights to the situation on the road and improve safety.

Both ITS and C-ITS have similar features, e.g. enhancing safety by means of information and communication technology at the roadside or on vehicles. However, as ITS focuses more on providing intelligence to roadside systems and vehicles, C-ITS focuses on enabling communication between these systems. In C-ITS, communication can occur on an ad hoc basis and should be trusted and secured.

The EU C-ITS Credential Management System (EU CCMS) is the PKI (Public Key Infrastructure) set up for the European C-ITS trust model, as defined in the Certificate Policy [9], which ensures that C-ITS messages are exchanged in a secured and trusted way.

C-ITS service refers to a cluster of use cases based on a common denominator. This can be e.g. a signalised intersection or roadworks. Another term often referring to C-ITS service is "C-ITS application." In Directive (EU) 2023/2661, C-ITS service is defined as a category of ITS services based on an open architecture that enables a many-to-many or peer-to-peer relationship between C-ITS stations. This means ITS services that are provided using C-ITS.

Use case describes the function of the system and its desired behaviour. The desired behaviour can also be of the actors interacting with the system. Example use cases are Signal Phase and Timing Information and GLOSA (Green Light Optimal Speed Advisory) under the Signalised Intersections service.

3.2 Technologies and standards

Cooperative Intelligent Transport Systems (C-ITS) operate based on exchanging trusted and secured C-ITS messages. Messages are exchanged using C-ITS communication technologies; direct wireless communication for short-range and IP-based communication for long-range. Figure 1 shows the communication chain for short-range and long-range communication.

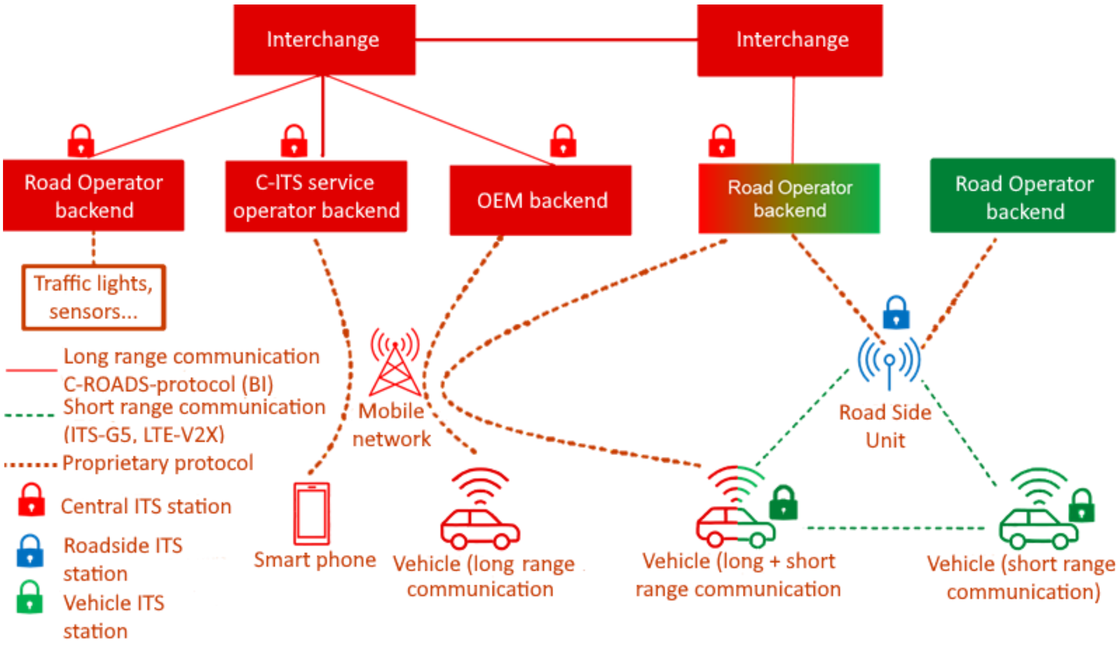
Interchange
Interchange
Road Operator backend
C-ITS service operator backend
OEM backend
Road Operator backend
Road Operator backend
Traffic lights, sensors...
Long range communication C-ROADS-protocol (BI)
Short range communication (ITS-G5, LTE-V2X)
Proprietary protocol
Central ITS station
Roadside ITS station
Vehicle ITS station
Mobile network
Road Side Unit
Smart phone
Vehicle (long range communication
Vehicle (long + short range communication
Vehicle (short range communication)

Figure 1. C-ITS communication chain

For short-range communications, the prevalent technologies in use are ITS-G5 and C-V2X Direct, both of which operate in the 5.9 GHz band and facilitate direct communication between road users. C-Roads only addresses ITS-G5. ETSI also includes C-V2X in the standards. ITS-G5 is based on physical and MAC layers of IEEE 802.11p, which itself is based on the wireless LAN standard IEEE 802.11. [3]

For long-range communications, IP-based communications and mobile networks are utilised to exchange C-ITS messages. In C-Roads, only the communication between the backends of C-ITS operators is specified. Communication to C-ITS operators' backend is proprietary and is to be decided by the C-ITS service operator or the OEM. Figure 1 depicts these communication channels and protocols.

There are multiple technologies, standards and standardisation bodies active in C-ITS. Table 1 presents these standards grouped by the technology they are related to and the organisation responsible for them.

Table 1. Categorisation of standards and their related organisations [15]

Technology	Standards	Organisation
WLAN-VANET	IEEE 802.11p	IEEE
	IEEE 1609	
	WAVE	
	SAE J2735	SAE (North America)
	WSMP	
	GeoNetworking	ETSI (Europe)
	ITS-G5	
Cellular	4G LTE (LTE-V2X)	3GPP & ETSI
	5G New Radio (5G-V2X)	

GeoNetworking protocol is a network-level protocol standardised by ETSI in EN 302 636. It supports packet routing in ad hoc networks and communication among individual ITS stations as well as distribution of packets in geographical areas. GeoNetworking protocol is also specified in the C-Roads ITS-G5 system profile as the network-level protocol to be used.

C-ITS messages are data packets that are formed using Facilities Layer Protocol Data Units (PDUs). These PDUs contain a payload, generated by the application layer, which is merged with the ItsPduHeader. This merging process results in the creation of complete messages. These messages, incorporating both header and payload, are then transmitted within the C-ITS environment. This approach ensures that information from the application layer is organised and communicated effectively across the system.

C-ITS messages are standardised by ISO and ETSI and are signed according to ETSI TS 103 097. Harmonised profiles for the standards have been developed by the Car2Car consortium for V2V services and by C-Roads for infrastructure-based services (including special vehicle services such as emergency vehicle, roadwork and public transport vehicles). Table 2 introduces C-ITS messages profiled by C-Roads, their logic of transmission and the function of the message.

Table 2. C-Roads profiled messages

C-Roads profiled messages	Logic of transmission	Function
IVIM (In-Vehicle Information Message)	I2V	Provides information of physical road signs that could be static or variable, virtual signs, or roadworks.
CAM (Cooperative Awareness Message)	V2I, V2V	Status information of vehicles. Holds information like location and state of the vehicle.
DENM (Decentralised Environmental Notification Message)	I2V	Provides information related to an event that has potential impact on road safety or traffic condition.
SREM (Signal Request Extended Message)	V2I	A message for requesting priority at the intersection (public transport) or pre-emption (public safety).
SSEM (Signal request Status Extended Message)	I2V	Acknowledgment to SREM message telling if the request has been approved, cancelled or changed in priority.
SPATEM (Signal Phase and Timing Extended Message)	I2V	Provides information about the current signal state of the traffic light controller, the time before changing to the next state, the allowed maneuvers and aid for crossing the intersection.
MAPEM (MAP topology Extended Message)	I2V	Provides information about the lane topology at the intersection and allowed maneuvers within intersection or road segment.

The messages above are standardised in ETSI Release 1 standards. ETSI is currently working on Release 2, which also includes services for support of automated driving, such as the Collaborative Perception Service (CPS). These services are more demanding and require more bandwidth resources. Release 2 also aims to remove interdependencies between different protocol layers. Some

Release 2 standards have already been published, such as the DENM Release 2 specification. Release 2 is expected to be ready by the end of 2024.

3.3 C-Roads Platform

The C-Roads platform is a collaborative initiative involving European Member States and road operators. Its aim is to test and implement C-ITS services with a focus on cross-border harmonisation and interoperability. C-Roads unites authorities and road operators to harmonise the deployment activities of C-ITS across Europe. C-Roads focuses on mature technologies, meaning ITS-G5 for short-range communication and IP-based communications for long-range. In ITS-G5, the focus is on the communication from the roadside unit to the vehicle, while in long-range communication the emphasis is on communication between backends.

The structure of C-Roads consists of the Steering Committee and Working Groups. The Steering Committee is composed of Member State representatives and is responsible for steering the C-Roads Platform. The Steering Committee is supported by Working Groups that ensure proper decisions towards interoperable deployments.

Technical aspects are addressed by WG2. Figure 2 shows the workflow of the different documents [1]:

- TF2 provides the specifications for the services and the use cases.
- TF3 then provides the profiles for the messages. TF3 has also drafted a handbook for assisting in the creation of SPATEM and MAPEM messages.
- TF3 also developed a profile for ITS-G5 related roadside and mobile equipment. C-Roads has developed a profile for ITS-G5 based roadside and mobile units, which is based on the Car2Car consortium Basic System Profile. This profile specifies the minimum set of standards and the requirements needed to realise an interoperable roadside ITS station. The ITS-G5 profiles also describe the use of the different channels in the 5855-5925 MHz band for ITS services. For the Day 1 services, only the ITS-G5 control channel (10MHz – 5895-5905 MHz) is sufficient, but for Release 2 messages such as CPS more channels are needed.
- TF4 has specified the IP-based profile for communication between backends.
- Security-related documents have been specified by TF1. TF1 is also working on a protection profile for Roadside units, which is needed when proceeding to security Level 2.
- TF5 has defined a concept and tests for cross-border interoperability testing.

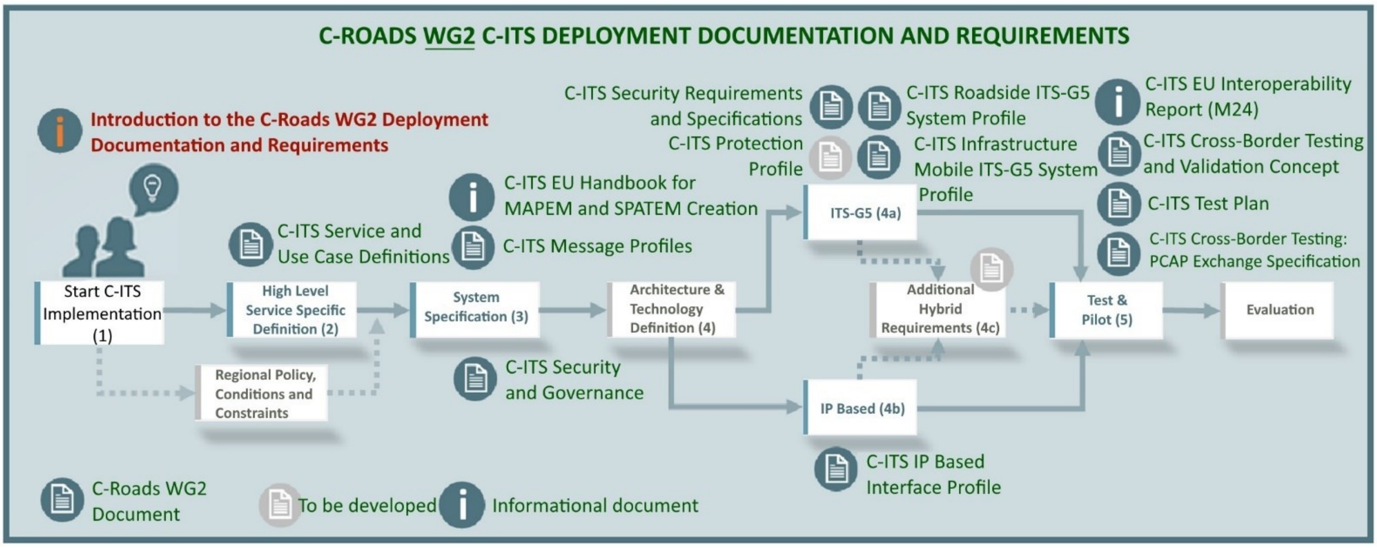
C-ROADS WG2 C-ITS DEPLOYMENT DOCUMENTATION AND REQUIREMENTS
Introduction to the C-Roads WG2 Deployment Documentation and Requirements
C-ITS Security Requirements and Specifications
C-ITS Protection Profile
C-ITS Roadside ITS-G5 System Profile
C-ITS Infrastructure Mobile ITS-G5 System Profile
C-ITS EU Interoperability Report (M24)
C-ITS Cross-Border Testing and Validation Concept
C-ITS Test Plan
C-ITS Cross-Border Testing: PCAP Exchange Specification
C-ITS EU Handbook for MAPEM and SPATEM Creation
C-ITS Service and Use Case Definitions
C-ITS Message Profiles
Start C-ITS Implementation (1)
High Level Service Specific Definition (2)
System Specification (3)
Architecture & Technology Definition (4)
ITS-G5 (4a)
Additional Hybrid Requirements (4c)
IP Based (4b)
Test & Pilot (5)
Evaluation
Regional Policy, Conditions and Constraints
C-ITS Security and Governance
C-ITS IP Based Interface Profile
C-Roads WG2 Document
To be developed
Informational document

Figure 2. C-Roads documents [1]

In C-Roads, different C-ITS services are described as a functional way and are a result of harmonisation efforts taken place within task force two. In this project, the deployment of the pilot system has been conducted following C-Roads Signalised Intersections (SI) service specifications. Table 3 presents all the current services and use cases under C-Roads.

Table 3. C-Roads Service and Use case catalogue version 2.0.8

C-Roads Service and Use case catalogue.	
Service	Use cases
In-Vehicle Signage (IVS)	IVS – Traffic Signs
	IVS – Free Text
Hazardous Locations Notifications (HLN)	HLN – Accident Zone
	HLN – Traffic Jam Ahead
	HLN – Stationary Vehicle
	HLN – Weather Condition Warning
	HLN – Temporary Slippery Road
	HLN – Animal or person on the road
	HLN – Obstacle on the road
	HLN – Emergency or Rescue/Recovery Vehicle in Intervention
	HLN – Emergency of Prioritised Vehicle Approaching
	HLN – Railway Level Crossing
	HLN – Unsecured Blockage of the Road
	HLN – Alert Wrong Way Driving
	HLN – Public Transport Vehicle Crossing
	HLN – Public Transport Vehicle at Stop
Road Works Warning (RWW)	RWW – Lane Closure
	RWW – Road Closure
	RWW – Road Works Mobile
	RWW – Winter Maintenance
Signalised Intersections (SI)	SI – Signal Phase and Timing Information
	SI – Green Light Optimal Speed Advisory
	SI – Imminent Signal Violation Warning
	SI – Traffic Light Prioritisation
	SI – Emergency Vehicle Priority
Automated Vehicle Guidance (AVG)	AVG – SAE Level Guidance
	AVG – Platoon Support Information
Probe Vehicle Data (PVD)	PVD – Vehicle Data Collection
	PVD – Event Data Collection

4 Cellular Vehicle to Everything (C-V2X)

Cellular Vehicle-to-Everything is a communication technology established by 3GPP in 2016, fostering connectivity between vehicles, pedestrians and roadside systems. It operates in two modes: direct device-to-device communication ("C-V2X Direct") without the need to rely on a network infrastructure in the 5.9GHz band, and network-based communication that links to mobile network base stations and core networks. The latter mode uses a licensed cellular spectrum and is operated using network LTE interface [2].

For C-V2X Direct, two different non-compatible versions have been standardised: LTE-V2X Direct and NR-V2X Direct. LTE-V2X Direct was standardised in 2016 by 3GPP under Release 14, while NR-V2X Direct was standardised by 3GPP in Release 16. Table 4 compares LTE-V2X Direct and NR-V2X Direct. During this project, NR-V2X chipsets were only beginning to come to the market [24] and were not yet integrated in commercial products.

Table 4. Comparison between LTE-V2X Direct and NR-V2X Direct [33]

	LTE-V2X Direct	NR-V2X Direct
Specification	3GPP Rel 14/ Rel 15	3GPP Rel 16 / Rel 17
Latency	low latency: 10-100 ms	ultra-low latency: 1 ms
PC5 message type	broadcast	broadcast, unicast and groupcast
Application Scenarios	Rel. 14: Day 1 services Rel, 15: platooning, advanced driving, extended sensors, remote driving	Rel. 16: complex interactions (e.g. cooperative lane merge)

When operating in direct device-to-device communication mode, LTE-V2X Direct does not depend on any public mobile network infrastructure. However, when supporting vehicle-to-network (V2N) applications, the applications would be delivered using a public mobile communications network over the very same commercially licensed cellular spectrum where other voice and data communications occur. [4]

When communicating over the network interface, the user equipment sends its V2X messages to the relevant V2X server and the server delivers the messages to user equipments in the target area. Both IP-based and non-IP based communication are supported. In case of the non-IP based V2X messages, the messages should be encapsulated in IP packets by the user equipment. [5]

Major European carmakers, representing jointly 70% of the European market, informed their commitment to go forward with 5G-V2X, including both NR-V2X Direct and 5G mobile network communications, for the provision of C-ITS services. [16]

The European frequency regulator CEPT (European Conference of Postal and Telecommunications Administrations) has designated a total of 40 MHz in the frequency range 5875-5915 MHz for safety-related ITS prioritised for road ITS [36]. In addition, 10 MHz in the range 5915-5925 MHz, which is prioritised for urban rail ITS, could be used after ETSI has developed polite protocols and/or proper co-channel sharing mechanisms between road and rail ITS. The frequency range 5855-5925 MHz is technology-neutral and used by both ITS-G5 and C-V2X (LTE-V2X Direct, NR-V2X Direct) [34].

Without mitigation actions both technologies may interfere with each other, resulting in reduced performance. ETSI has studied several co-channel coexistence mitigation methods in ETSI TR 103766 [14]. However, these methods require modifications to standards. Nevertheless, discussions between the involved stakeholders are ongoing. Several solutions have been proposed, e.g. assigning specific frequency ranges for each of the technologies (5GAA [19]) or defining politeness rules for technologies operating in the same frequency band (ASECAP [20]), such as listen-before-talk (which is not supported by LTE-V2X Direct) or time-splitting [13]. So far, no decisions have been taken. To deploy interoperable systems, system profiles, like the ones developed by Car2Car Consortium and C-Roads for ITS-G5 ITS stations, are needed. The access layer for LTE-V2X Direct is specified in ETSI EN 303 613. ETSI EN 303 798, which is under preparation, is a revision of ETSI EN 303 613 and extends to include NR-V2X Direct. ETSI has published a profile for LTE-V2X Direct communications (ETSI TS 103 723) and is working on a profile for 5G NR-V2X Direct communications (ETSI TS 103 939). The documents refer to the Car2Car and C-Roads profiles as baseline and indicate deviations from these specifications. The GeoNet header has media-specific fields, but for LTE-V2X the content is the same as for ITS-G5.

To avoid unstable network behaviour and channel congestion, and hence maintain a sufficient QoS, C-ITS short-range communication systems implement congestion control: for ITS-G5 Decentralised Congestion Control is specified in ETSI TS 102 687, for LTE-V2X Direct in ETSI TS 103 574, and for NR-V2X it will be included in ETSI EN 303 798, which is underway.

5 European Union C-ITS Security Credential Management System (EU CCMS)

5.1 Introduction

C-ITS messages can be exchanged between actors without knowledge of each other. To ensure that the messages can be trusted, a common C-ITS trust model has been created by the European Commission. The C-ITS trust model is implemented by means of a policy on the use of PKI (Public Key Infrastructure) called the EU CCMS (European Union C-ITS Security Credential Management System).

When communicating using C-ITS short-range technologies, the communication is based on radio broadcasts. This means that all devices nearby can receive them, and the original sender of the message has no control over who receives the message. On the other hand, anyone can also send messages and the station cannot control from whom it receives messages. This means that the different C-ITS stations have no prior knowledge of each other.

To verify the authenticity, integrity and authorisation of the exchanged C-ITS messages, digital certificates are used. The method to sign and verify these certificates involves the public and private keys associated to them. [6]

As some C-ITS messages (CAM) are based on inputs from road users' movement, they can be regarded as holding privacy-sensitive information. For this reason, short-range certificates used to sign messages are changed regularly and have restrictions on repetition of use. This reduces the potential for tracking or following road users. Potential privacy issues are considered more in depth in chapter 9.3.4.

To ensure the interoperability of C-ITS services in the EU area, it has been widely accepted that there is one trust model for C-ITS in Europe. This trust model is governed by one common Certificate Policy and includes all C-ITS stations, from vehicles to road infrastructure. [6]

5.2 Actors and architecture

The Public Key Infrastructure used in the European C-ITS Security Credential Management System at its highest level is composed of a set of Root Certificate Authorities (RCAs) that have their certificates registered to the European Certificate Trust List (ECTL) and published by the Trust List Manager (TLM). [7]

The C-ITS trust model architecture consists of multiple Root Certificate Authorities, which can be operated by a private or a governmental organisation. For entities who participate in the C-ITS trust model and do not want to organise their own Root Certificate Authority, the EU RCA (Root Certificate Authority provided by the European Commission) is offered for use. [7]

The Trust List Manager (TLM) is nominated by the C-ITS Certificate Policy Authority (CPA) and is responsible for managing the European Certificate Trust List (ECTL). In addition, the Trust List Manager regularly reports to the Certificate Policy Authority for the overall secure operation of the C-ITS trust model. The inclusion and possible exclusion of Root Certificate Authorities to the European Certificate Trust List is also the responsibility of the Trust List Manager, and it acts upon notification by the Certificate Policy Authority. The Trust List Manager also has a role in signing the European Certificate Trust List and transmitting it to the C-ITS Point of Contact (CPOC). [7]

The European Certificate Trust List (ECTL) is the element in the C-ITS trust model that ensures the trust to approved Root Certificate Authorities (RCAs) to all participants. This is because the trustworthiness of the messages can be checked by following the chain of trust all the way to the issuing RCA and checking the current valid ECTL [6]. The C-ITS trust model is visualised below in Figure 3.

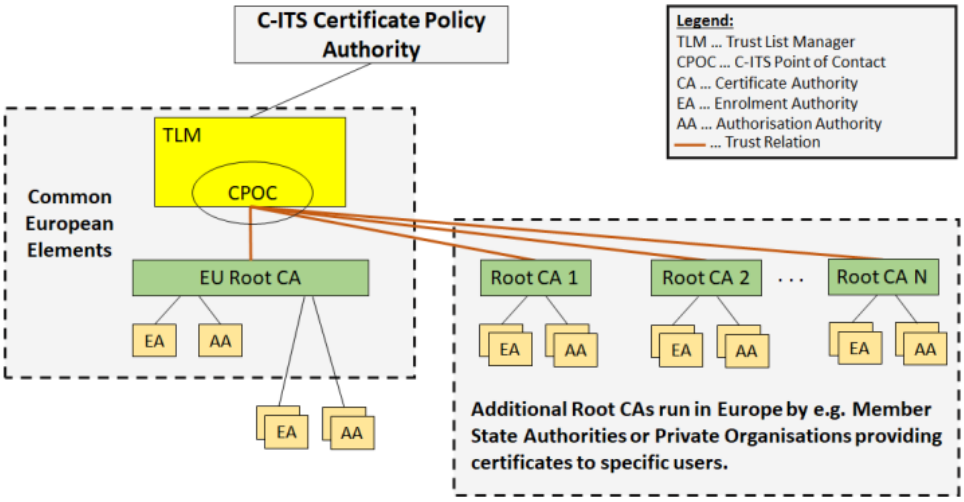
C-ITS Certificate Policy Authority
Legend:
TLM ... Trust List Manager
CPOC ... C-ITS Point of Contact
CA ... Certificate Authority
EA ... Enrolment Authority
AA ... Authorisation Authority
... Trust Relation
TLM
CPOC
Common European Elements
EU Root CA
EA
AA
EA
AA
Root CA 1
Root CA 2
...
Root CA N
EA
AA
EA
AA
EA
AA
Additional Root CAs run in Europe by e.g. Member State Authorities or Private Organisations providing certificates to specific users.

Figure 3. C-ITS trust model architecture [10]

The different roles, especially from the different authorities, are described in more detail in [11]. Figure 4. Interaction between C-ITS operators, C-ITS stations and PKI [11]

shows the interaction between the manufacturer, C-ITS operator and C-ITS station and the PKI. Dependent on the contractual setup, the manufacturer or the C-ITS operator is responsible for the initial setup of the C-ITS station, including the installation of key and certificate material.

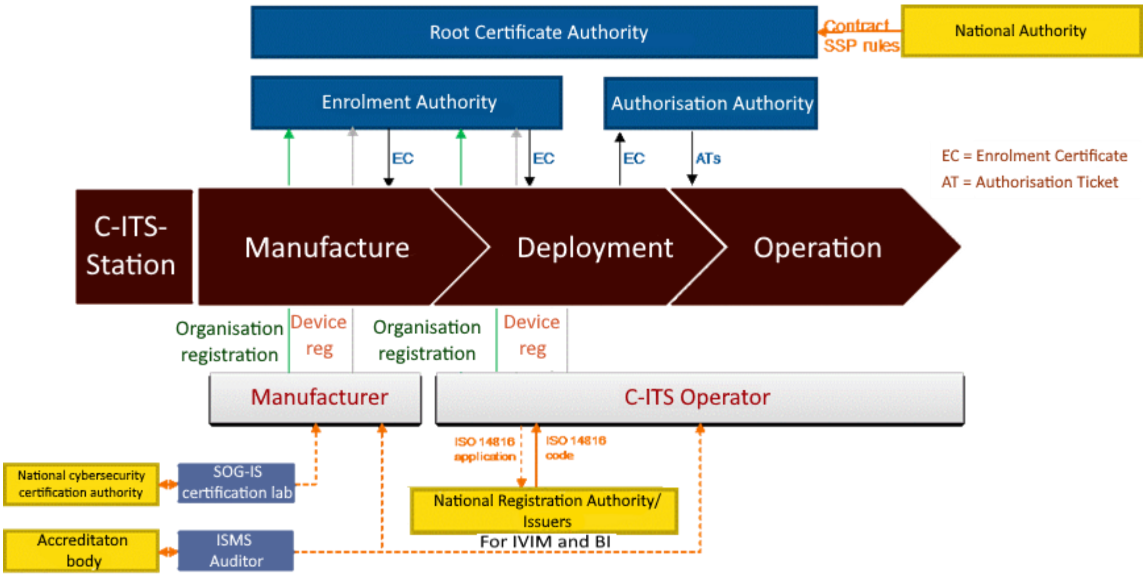

Figure 4. Interaction between C-ITS operators, C-ITS stations and PKI [11]

5.3 Operation levels

The guidelines for participating in the C-ITS trust domain are outlined in the C-ITS Point of Contact (CPOC) Protocol [7], the Security Profile (SP) [8] and the Certificate Policy [9]. Since the deployment of C-ITS is not yet mature enough for full production operations, three levels of trust have been defined to support C-ITS deployment in Europe. These levels serve different purposes and provide a means to test C-ITS stations without immediately needing to comply with full production rules.

Level 0 (L0) is the lowest of the three levels and is meant for limited time testing. It offers a way to build competence towards standard and technical requirements conformity. This pilot project was conducted following the L0 requirements. In this level no compliance to the C-ITS trust domain policies is required, but the correct format of Root Certificate shall be checked. [7]

Level 1 (L1) serves as a transitional level between L0 and L2 and shall be used to align C-ITS implementation to the C-ITS trust domain processes and approach full compliance. It is intended for production environments and requires a full compliance to C-ITS trust domain policies, but with a defined set of exceptions compared to Level 2 [6]. L1, intended to support C-ITS Day 1 services, is designed for a transition phase of two years [7]. The central elements (CPOC, TLM, ECTL) for L1 are expected to become available in the beginning of 2024, and the transition period is expected to last until the end of 2025 [7].

Level 2 (L2) is the highest of the levels and shall be used for certified production operation of C-ITS station and PKI implementations. It is intended for large and distributed C-ITS networks and mandates full compliance to C-ITS trust domain policies. [7]

C-ITS stations at Level 2 (and partially in Level 1) undergo certification according to the protection profile before being introduced to the market. The protection profile includes the cybersecurity requirements for the operation of the C-ITS stations. The equirements include e.g. physical protection of the devices, the communication with the PKI, road authority and Traffic Control Centre, and the continuous operation of the C-ITS station. Road maintenance operators are not expected to access the interfaces to the C-ITS station.

5.4 Experiences

5.4.1 Getting certificates from the EU RCA

This project involved a cybersecurity-related task of obtaining L0 certificates from the EU RCA. The EU CCMS consists of multiple RCAs that are listed in the ECTL. The EU RCA is offered for use and operated by Atos on behalf of the European Commission.

The process of obtaining L0 certificates is a multistep process consisting of three steps.

The first step of the process was to contact the EU RCA L0 service operator and indicate the request for service registration. This request includes necessary information such as project needs, expected duration and quantities of devices to be registered.

The second step was to fill in the C-ITS EU ROOT CA & SUB-Cas SAAS AGREEMENT upon receiving it. In addition to completing the agreement, the organisation must name two trusted persons responsible for PKI-related interactions. When returning the signed agreement, the organisation must include a legal registration proof of the organisation and return both documents to the EU RCA L0 service operator.

Following the two previous steps, the organisation should receive confirmation of authorisation to use the service. The final step consists of enrolling devices to the L0 PKI, generating keys and specifying permissions.

5.4.2 Using RCA preferred by manufacturer

As the EU CCMS architecture consists of multiple RCAs, an entity participating in the trust model is free to use another PKI provider that has their RCA registered in the ECTL. In this project another commercial PKI provider, Microsec, was used in addition to the EU RCA. Microsec has their RCA registered to Level 0 ECTL and operates the L0 service for tests and pilots.

Using this method saves time compared to getting certificates from the EU RCA. This requires cooperation between the C-ITS station manufacturer and PKI provider to assure compatibility.

However, there are manual steps in the enrolment that cannot be automated. SSPs, i.e. Service Specific Permissions, that indicate which messages the C-ITS station can transmit must be inserted manually since they depend on different factors. These SSPs must match the C-ITS messages in use, and they depend on the service and use cases to be implemented.

Additionally, the type of C-ITS station to be registered must also be defined. This is because not all stations are supposed to send all the specified messages.

Vehicles are not supposed to be able to send messages, that should come from roadside infrastructure and vice versa. This is why the type of the stations must be defined when registering it to a PKI provider.

The C-V2X device manufacturer, Commsignia, offers APIs for installation of the Microsec certificates.

6 Information and Cyber Security in C-ITS

6.1 Introduction

The purpose of this chapter is to examine the interconnections between Information Security Management Systems (ISMS), Cyber Security Management Systems (CSMS), the NIS2 EU-wide legislation on cybersecurity (Network and Information Systems Directive), the ISO 27001 information security standard [21], and the C-ITS technological domain relating the information and cybersecurity requirements directed at organisations and technological systems involved in the C-ITS domain.

The cybersecurity requirements for the transportation sector, especially in ITS and C-ITS business areas, come from various places and levels.

At the smallest level, these requirements may originate from national de facto standards or principles typically established by local public authorities and consistently applied in ITS business segment tendering processes. These requirements are typically based on broader standards, but they often include many country-specific requirements (primarily because wider standards or regulations might not exist).

Moving up a level, requirements may derive from multinational cooperative initiatives focused on creating cross-border principles and de facto standards to promote interoperability in ITS products and services across Member States and industrial organisations (e.g. C-Roads).

At the broadest level, requirements are shaped by international standardisation or regulations and laws established by public authorities, such as those at the EU or US level (e.g. NIS2).

While all the levels establish a set of requirements for ITS domain organisations, covering both private and public sectors, they necessitate the establishment of "proof" to demonstrate compliance with these requirements. This “proof” could take various forms, such as a certified quality or information security management system, a set of required certificates at the employee level, or type approval for a certain product.

6.2 Information Security Management System

ISO 27001 is a widely recognised and mature standard aimed at enhancing information security, cybersecurity and privacy protection within organisations. As it is part of a very popular ISO (International Standards Organization) standard collection, it has become the most utilised information security standard across various organisations.

The standard outlines the requirements for establishing, implementing, maintaining and continually improving an ISMS system within an organisation. The ISMS framework specifies the methods how organisations meet numerous information security requirements outlined in the standard, considering e.g. an organisation's operating environment, leadership, planning, support functions and operation processes, all of which must be implemented according to the standard.

Enforcing the use of an ISMS system and meeting the requirements of the ISO 27001 standard is an effective approach to cover information security requirements in a holistic manner within an organisation. The adoption of this globally acknowledged standard improves trust among customers and collaboration partners regarding the organisation's commitment to information security.

The European DIGITAL SME Alliance has drafted a set of guidelines for SMEs on security controls [22] and on implementing the information security management system (ISMS) in accordance with ISO 27001 [23].

In summary, an ISO 27001 certified ISMS system provides organisations operating in the C-ITS domain with a comprehensive framework for addressing unique cybersecurity and information security challenges inherent in the design, development, deployment, maintenance and operation of C-ITS systems.

6.3 Cyber Security Management System

A Cyber Security Management System (CSMS) is often viewed as a subset of ISMS (Information Security Management System). While these systems share many similarities, CSMS specifically concentrates on managing cybersecurity risks related to systems and networks, whereas an ISMS has a broader focus on organisation information safety, including the management of sensitive company information and the implementation of policies and processes to safeguard information assets from various threats.

An ISMS offers a broader framework for managing all aspects of information security, especially at the organisational level, while a CSMS is more narrowly tailored to address cybersecurity risks related to digital assets, technical systems/devices and networks (the "cyber domain"), as well as controls for managing those risks. Such risks might include cyberattacks, hacking, malware and phishing threats.

There are numerous cybersecurity management systems and frameworks available, many of which are tailored to specific industry needs. For instance, the IEC 62443 standard focuses on enhancing the cybersecurity of industrial automation systems, while PCI DSS (Payment Card Industry Data Security Standard) provides a set of security standards for the payment card industry.

In the automotive industry, UN Regulation 155 requires that vehicle manufacturers establish and implement a CSMS. The requirements in UN regulation 155 must be met for obtaining type approval for vehicle safety systems and therefore gaining market access. The same CSMS required by vehicle manufacturers in UN Regulation 155 may also cover vehicle C-ITS stations inside type-approved vehicles.

In EU Regulation 2022/1398, the European Union acceded to the previously mentioned UN Regulation 155 and applies it on a compulsory basis.

6.4 NIS2

The NIS2 Directive is a regulation of the European Union, which means that an increasing number of organisations will soon need to systematically prepare for cyber threats, as NIS version 2 comes into force in October 2024. The main objective of the NIS2 Directive is to ensure a common high level of cybersecurity throughout the European Union, both in the private and public sectors.

Although NIS2 sets limits on the size of organisations required to comply (those with over 250 employees), its impact extends far beyond. Given that the whole transportation sector, defined as part of the critical infrastructure, is included within NIS2, this implies that all suppliers and supply chains serving the public sector must, in practise, fulfil the requirements of NIS2 to ensure compliance when providing systems and services within the transportation sector.

More specifically, operators of Intelligent Transport Systems (ITS), as defined in Article 4, point (1), of Directive 2010/40/EU of the European Parliament and of the Council, fall under the NIS2 scope. [35]

6.5 Organisational Requirements

In the C-ITS context, both ISMS and CSMS systems are involved in setting requirements for the organisations and use technical systems as part of the C-ITS ecosystems.

As the previous chapter on NIS2 demonstrated, this European Union cybersecurity framework will have a significant impact on the cybersecurity requirement for the entire transportation sector. While there are numerous alternatives for organisations to fulfil NIS2 requirements, it has been observed that obtaining certification for the ISO 27001 information safety management system provides organisations with a solid foundation for addressing these requirements.

The ISO 27001 has also been recognised as a requirement in more specific C-ITS activities.

The EU CCMS (C-ITS Security Credential Management System) has been discussed in Chapter 5. As has been discussed in section 5.3, there are three security levels for C-ITS systems, with Level 2 (L2) being the fully operational security level, for which all C-ITS stations and C-ITS station operators have to go through the certification processes.

At security Level 2 of the EU CCMS, organisations operating C-ITS stations need to operate an Information Security Management System (ISMS) in place, according to the Security Policy [8]. The ISMS must be according to ISO 27001 and ensure the security of all the C-ITS stations and processed data.

The C-ITS station operator must maintain valid certification for compliance with Security Policy following the guidelines for the ISO 27001 audit. Vehicular C-ITS stations may be covered by a CSMS that is certified in accordance with UN Regulation 155 and EU Regulation 2022/1398. [8]

C-ITS station operators that operate an essential road transport service according to the NIS2 Directive may apply the security measures and security requirements defined by the national transposition of the NIS2 Directive instead [8].

C-ITS stations shall also implement proper countermeasures to mitigate risk, and such countermeasures should implement controls as defined in ISO 27001 and ISO 27002 or Annex 5 of UN Regulation 155 for vehicle C-ITS stations. [8]C-ITS station operators must maintain valid certification for compliance with Security

Policy following the guidelines for the ISO 27001 audit, or the certification process of a CSMS according to UN Regulation 155 for vehicle C-ITS stations, or a valid evaluation for compliance for the road operators subject to the NIS and NIS 2 Directives. [8]

7 Pilot system

7.1 Pilot architecture

The architecture in the pilot was designed to implement the Signalised Intersection (SI) C-ITS service specified by the C-Roads platform. The method of communication in this C-ITS service was I2V (infrastructure to vehicle) and it was carried out using short-range communication technology together with long-range communication technology. In both communication channels the C-ITS messages transmitted originated from the traffic light controller. The messages used in the pilot were of the types SPATEM and MAPEM.

The architecture consisted of two parallel communication methods and the systems and actors for each of them. In both communication methods the C-ITS messages were coming from the traffic light controller as unsigned messages. Figure 5 presents an overview of the architecture and systems involved in it.

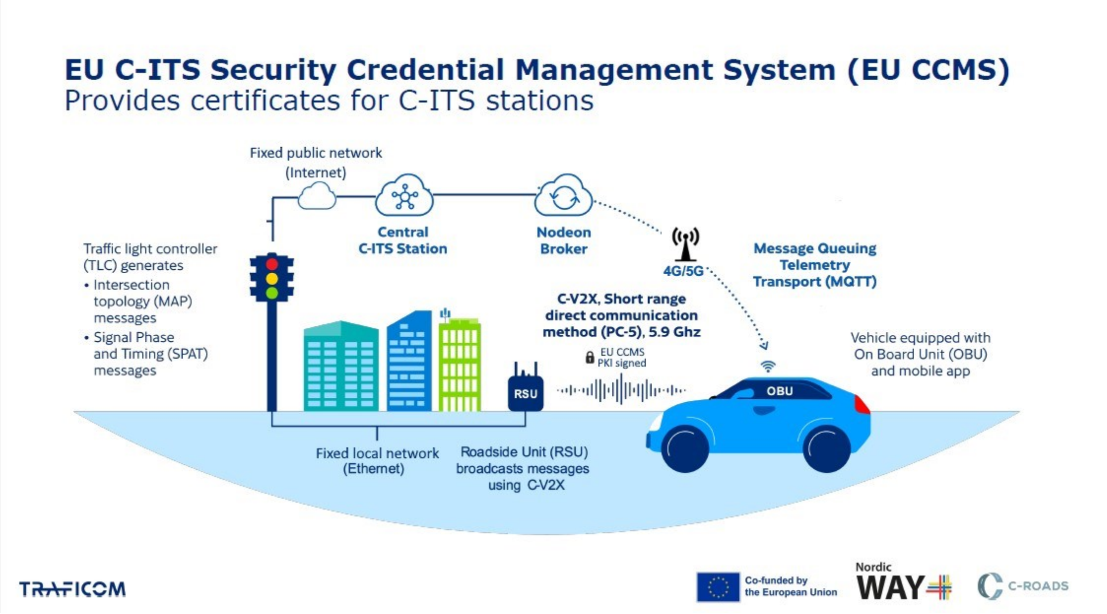
EU C-ITS Security Credential Management System (EU CCMS)
Provides certificates for C-ITS stations
Fixed public network (Internet)
Central C-ITS Station
Nodeon Broker
Traffic light controller (TLC) generates
• Intersection topology (MAP) messages
• Signal Phase and Timing (SPAT) messages
4G/5G
Message Queuing Telemetry Transport (MQTT)
C-V2X, Short range direct communication method (PC-5), 5.9 Ghz
EU CCMS PKI signed
RSU
OBU
Vehicle equipped with On Board Unit (OBU) and mobile app
Fixed local network (Ethernet)
Roadside Unit (RSU) broadcasts messages using C-V2X
TRAFICOM
Co-funded by the European Union
Nordic WAY
C-ROADS

Figure 5. Pilot architecture

In the short-range communication the traffic light controller forwarded the C-ITS messages it had generated directly to the RSU connected to it. The RSU had been enrolled to EU CCMS and had received L0 certificates for its operation. Using these certificates, it was able to sign the incoming messages before broadcasting them to nearby systems using LTE-V2X Direct short-range direct communication.

Long-range communications involved two systems for transmitting C-ITS messages originating from the traffic light controller. The first system, the Tampere C-ITS Node (TLEX), was in direct connection with the traffic light controller over the fixed public network. The Nodeon C-ITS Service Provider subscribed to these messages from the Tampere C-ITS Node and relayed them to the vehicle over the mobile network.

The vehicle was equipped with an OBU and mobile phones with apps for receiving data through both communication methods. The OBU received data packets over LTE-V2X Direct and processed them for the short-range mobile app. Meanwhile, the long-range mobile app received C-ITS messages over the mobile network and processed them directly within the app.

In the pilot architecture, the EU C-ITS Security Credential Management System operated as the trust provider for the enrolled C-ITS stations. It provided certificates for the stations to sign and validate incoming and outgoing C-ITS messages.

C-ITS messages utilised in the pilot were encoded using the ASN.1 UPER schema, following ETSI standards. This was done to keep the packet sizes minimal and to mitigate network payloads. In this pilot, the Traffic Light Controller (TLC) served as the system responsible for encoding messages before forwarding them.

In terms of architecture, there is a distinction in where the messages are decoded from ASN.1 UPER. On the long-range channel, the decoding of messages happened in the Nodeon Broker service. This centralised point in the communication chain allowed the message to be decoded only once, after which they could be forwarded to multiple end-user devices in a decoded format.

In short-range communication the communication is decentralised, thus every receiving station must decode incoming packets.

Figure 6 depicts the architecture used in the pilot.

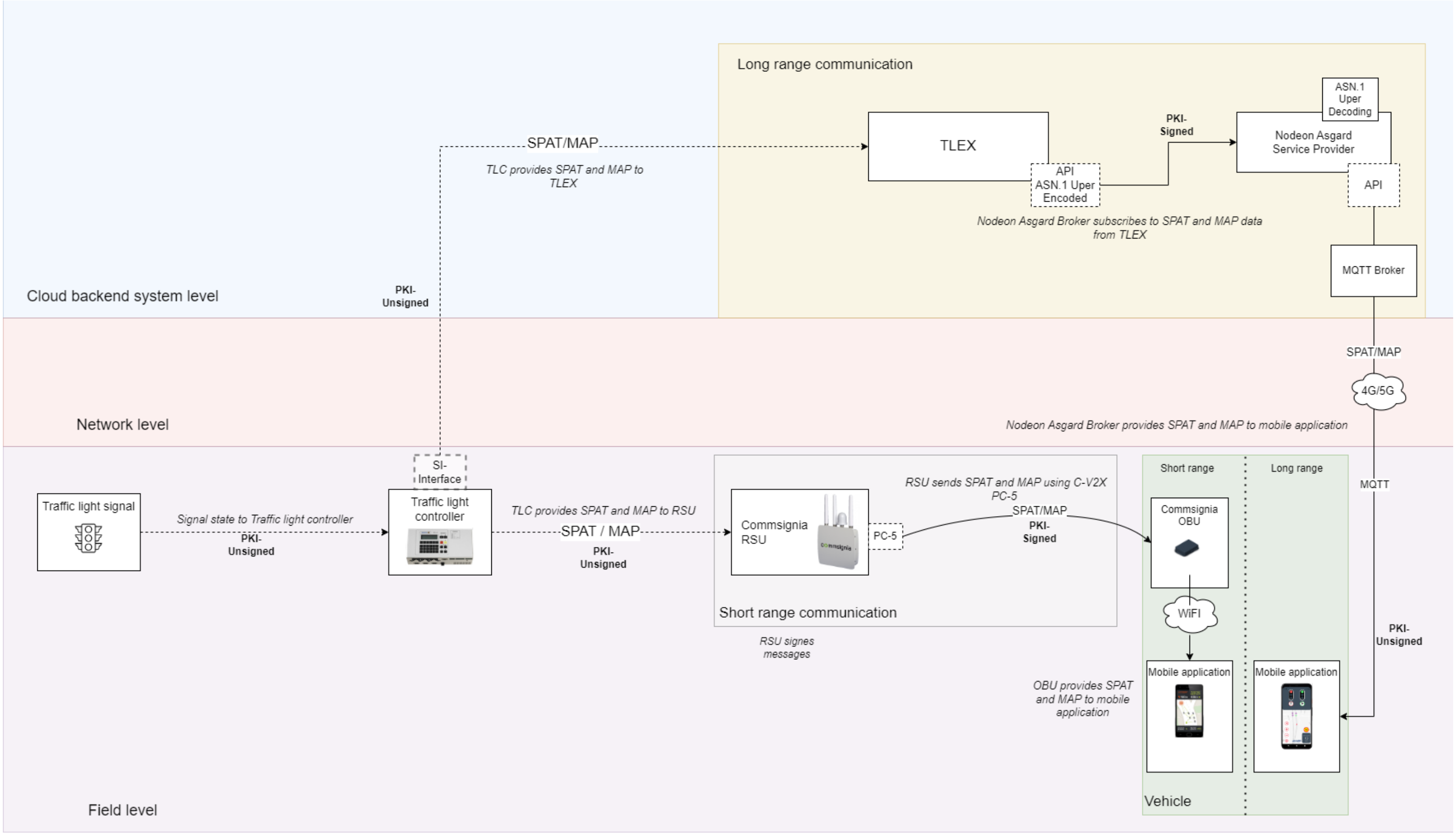
Long range communication
SPAT/MAP
TLC provides SPAT and MAP to TLEX
TLEX
API
ASN.1 Uper Encoded
PKI-Signed
ASN.1 Uper Decoding
Nodeon Asgard Service Provider
API
Nodeon Asgard Broker subscribes to SPAT and MAP data from TLEX
MQTT Broker
Cloud backend system level
PKI-Unsigned
SPAT/MAP
4G/5G
Network level
Nodeon Asgard Broker provides SPAT and MAP to mobile application
SI-Interface
Traffic light signal
Signal state to Traffic light controller
PKI-Unsigned
Traffic light controller
TLC provides SPAT and MAP to RSU
SPAT / MAP
PKI-Unsigned
Commsignia RSU
PC-5
RSU sends SPAT and MAP using C-V2X PC-5
SPAT/MAP
PKI-Signed
Short range communication
RSU signes messages
Short range
Long range
MQTT
Commsignia OBU
WiFI
Mobile application
Mobile application
OBU provides SPAT and MAP to mobile application
PKI-Unsigned
Vehicle
Field level

Figure 6. Detailed pilot architecture

7.2 Pilot deployment

The pilot system was deployed at the intersection of Hervannan valtaväylä and Jäähallinkaari/Peltikatu (TRE 533) in the city of Tampere. The intersection had six signal groups controlling the movement of vehicles through it.

The roadside unit was installed on the corner of Jäähallinkaari and Hervannan valtaväylä, near the traffic light controller. The installation involved mounting an RSU to a pole attached to the traffic light controller cabinet. Figure 7 illustrates the mounting position of the RSU at the intersection.

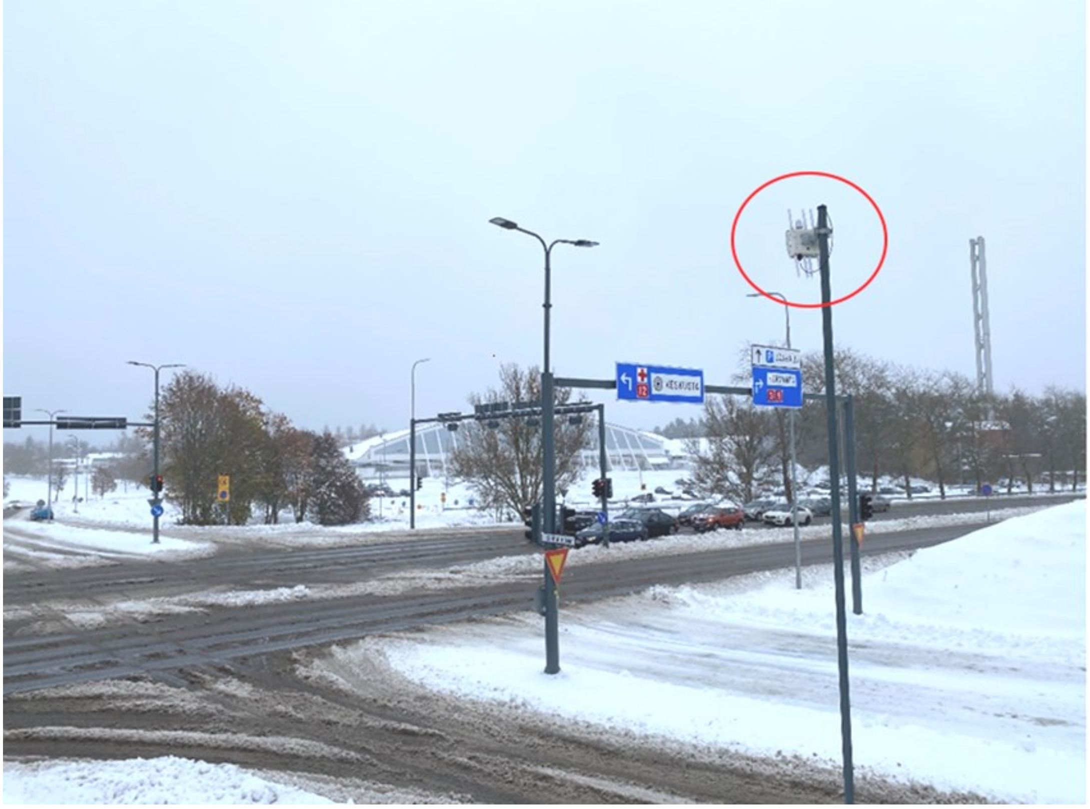

Figure 7. RSU installation at the intersection

The mounting position for the RSU was chosen to provide the best available radio communication. This is achieved when there is a direct line of sight between the antennas of the sender and recipient (i.e. vehicles). Any terrain, trees or other obstacles between the transmitter and receiver could potentially have a serious negative impact on radio transmissions. As depicted in Figure 8, the measurement setup conducted in this pilot had a clear line of sight between the RSU and OBU.

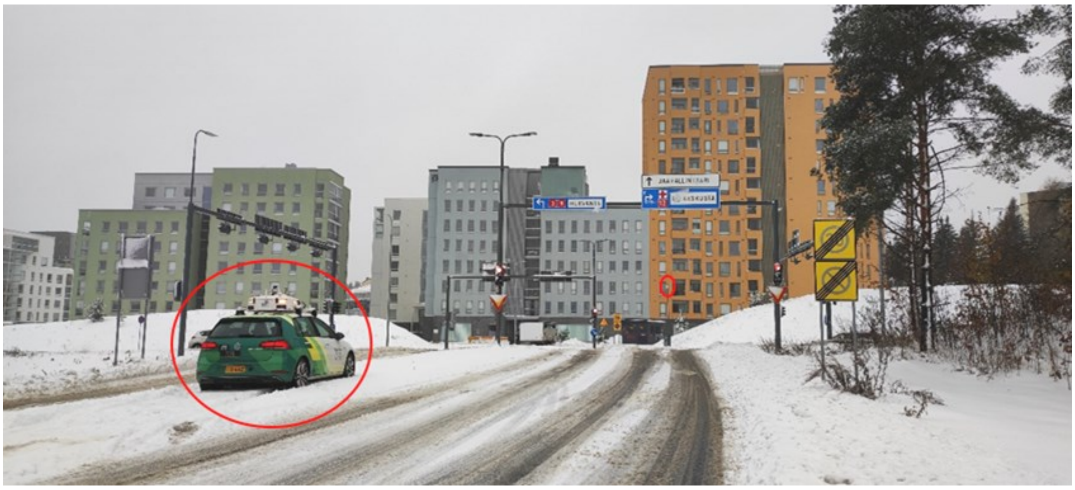

Figure 8. Measurement setup at the intersection on Pelikatu, facing west

The deployment of the long-range system was accomplished by utilising the existing TLEX system, which links multiple signalised intersections to a centralised system. As this system was already operational at the start of the pilot, no additional systems were needed to be deployed to connect the traffic lights.

8 Results

8.1 Test setup

The tests for short-range communication between RSU and OBU were conducted using two different methods. The first one was to capture incoming and outgoing packets from both devices and thus be able to inspect the content and headers of these packets. The second was shooting a video of the short-range mobile app together with the traffic light signal displaying the same signal group as the application.

Packet captures taken from OBU and RSU included arrival time, enabling latency calculations for the radio communication between devices. This was achieved by determining the latency between OBU and RSU by calculating the time difference between when the packets were sent out by the RSU and when they were received by the OBU. To ensure that both laptops were synchronised with each other, ntp (network time protocol) was used, assuring synchronisation within 5 ms.

Latency = time received^{OBU} – time sent^{RSU}

Video shooting allowed for the simultaneous capture of video material from the mobile apps and the actual traffic light signal at the intersection. For this, Racelogic VBOX Video equipment was used. This equipment enabled precise timestamps that can be compared to the actions on the video. Through these recordings and timestamps, the real end-to-end latency of application can be analysed compared to the real traffic light signal. Figure 9 shows the video recording user interface layout for mobile apps compared to the real traffic light signal.

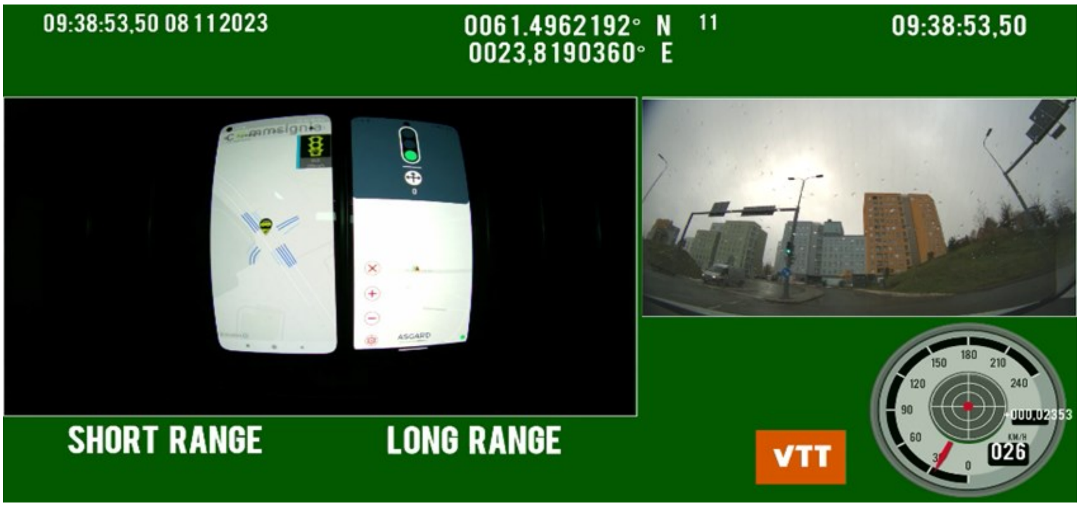

Figure 9. VBOX Video user interface layout for mobile UIs and environmental recordings

The two mobile apps used ran on two separate Android smart devices to keep the applications from interfering with each other. The short-range application was made by Commsignia, and it was running on a Xiaomi 11 Lite 5G NE phone. The long-range application was developed by Nodeon Finland and was running on a Nokia X30 5G. Both of them are the same 5G NR generation devices and have similar performance based on Snapdragon architecture (Snapdragon 778G vs. Snapdragon 695).

Tests for long-range communication were conducted in a similar manner to short-range tests. Packets flowing through the MQTT server were recorded by subscribing to the same topic as the mobile app. This enabled the recording of the same packets that the mobile app received with a precise timestamp. Together with video recording of the long-range mobile app, packet recording enabled the inspection of the content of the packets as well as calculating differences in timestamps.

Tests were conducted on signal group 6 of intersection TRE 533. Signal group 6 is responsible for directing traffic coming from east via Pelikatu towards the west. Figure 10 illustrates the geometry of the target intersection and lane topology, with Pelikatu on top.

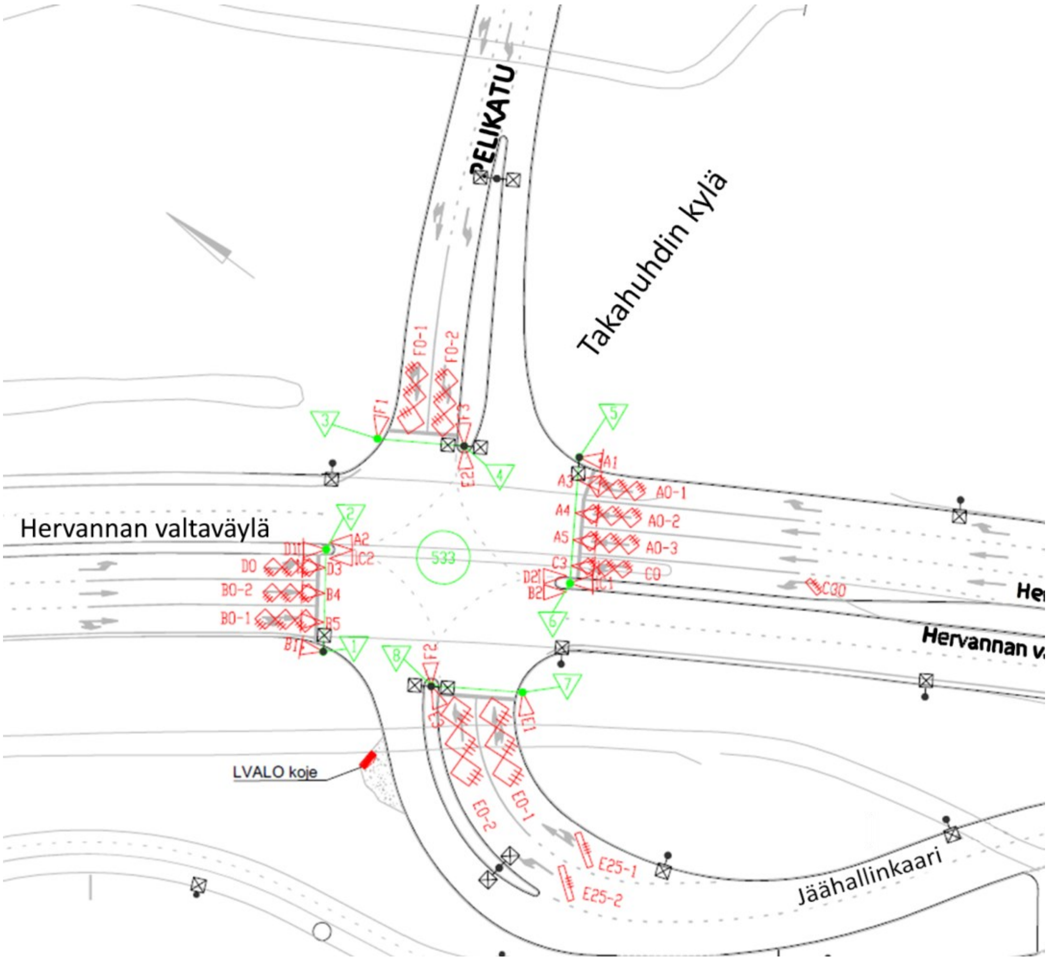

Figure 10. Intersection geometry in target area

For cyber-related tests, both the RSU and OBU were enrolled to EU CCMS. To verify that the messages were signed properly and contained all the necessary information, packet captures were utilised in conjunction with Wireshark. This allowed the security header from received messages to be dissolved and its content to be inspected.

Two test cases were executed to analyse the impact of signing messages to overall latency and to see how the system would behave if messages were not signed as expected. To test the impact of message signing, signature verifications were disabled and the measured latency was compared to a situation where verifications were enabled. In order for unsigned messages to be tested, message signing was disabled on the RSU. OBU had security features enabled, so it would expect incoming messages to be properly signed. If messages were not approved by OBU, the mobile application would not process any content of these messages.

C-Roads has also published test cases that focus on the interoperability of a C-ITS implementation. These test cases focus on three areas: ITS-G5 systems, IP-based communication (cellular), and security elements. The published test cases are divided into on-road testing and lab-based testing.

These test cases are further subdivided based on the C-ITS messages used. This project implemented the Signalised Intersections service, which uses SPATEM and MAPEM messages. For this reason, tests related to other types of messages were left out of the scope.

As the ITS-G5 was replaced with the LTE-V2X in this project, ITS-G5-specified test cases were modified to use LTE-V2X. These test cases were conducted as on-road tests at the TRE533 intersection. Table 5 lists the chosen test cases for this project.

Table 5. Selected C-Roads test cases

Test case	C-Roads test cases selected
1	TC_CROADS_SI_GENERIC_ITS-G5_SPaTEM-MAPEM_Timing_01_R2.0.4
2	TC_CROADS_SI-GENERIC_ITSG5_MAPEM_Location_03_R2.0.4
3	TC_CROADS_SI-GENERIC_ITSG5_MAPEM_SPATEM_Generic-Relation_02_R2.0.4
4	TC_CROADS_SI-SPTI_ITSG5_SPATEM_SignalPhaseAndTimingInformation_08_R2.0.4
5	TC_CROADS_SI-SPTI_ITSG5_SPATEM_speeds _08_1_R2.0.4

Test case 1 from Table 5 looked at the timing information of received SPATEM and MAPEM messages. To pass, the timing data elements “moy” (minute of year) and "timestamp" within the data field “IntersectionState of the SPATEM” should be received.

Test case 2 from Table 5 ensures that the received MAPEM has the correct ID and location of the target intersection. To pass, MAPEM needs to match the correct signalised intersection and to have matching latitude and longitude info to the target intersection.

Test case 3 from Table 5 checks that the received SPATEM relates to the newest version of MAPEM. To pass this test, SPATEM Id must match MAPEM Id and the actual target intersections Id. Also, SPATEM revision must match the MAPEM revision number.

Test case 4 from Table 5 checks that the current phase state and timing of upcoming phase changes from the signalised intersection shall be sufficiently accurate and reliable to ensure high-quality information. To pass this test, the V-ITS-S (Vehicular ITS Station) must receive timestamp and moy data elements from R-ITS-S (Roadside ITS Station) with relevant and accurate data. Data elements for current and upcoming signal phases should be received by V-ITS-S with relevant and accurate data of signalGroup, mindEndTime and maxEndTime.

Test case 5 from Table 5 checks that the current phase state and timing of upcoming phase changes from the signalised intersection shall be sufficiently accurate and reliable to ensure high-quality information. To pass this test, three verifications must be conducted. The data elements are received and the dataframe “speeds” is not concluded. Data elements for current and upcoming signal phases should be received by V-ITS-S with relevant and accurate data of signalGroup, mindEndTime and maxEndTime. V-ITS-S should receive timestamp and moy data elements with relevant and accurate data from R-ITS-S.

These same C-Roads test cases were also executed for the long-range communication system. In this scenario all the same values were inspected from the messages, but the messages were transmitted to the vehicle using the cellular network. Since the messages were originating from the same TLC in both communication options, the structure and format of the message is going to be same.

Figure 11 shows the approximate locations of the mobile cell towers near the target area; these tests used the Elisa network. This intersection is one of the busiest in the city of Tampere, and its mobile network coverage is reasonably good. Figures 12 and 13 show hourly traffic densities in the vicinity to give the reader an overview of the target area. The hourly traffic densities were around 400-600 vehicles per hour between 10:00 and 13:00. Figure 14 shows also the locations of the loop detectors on the road network for this.

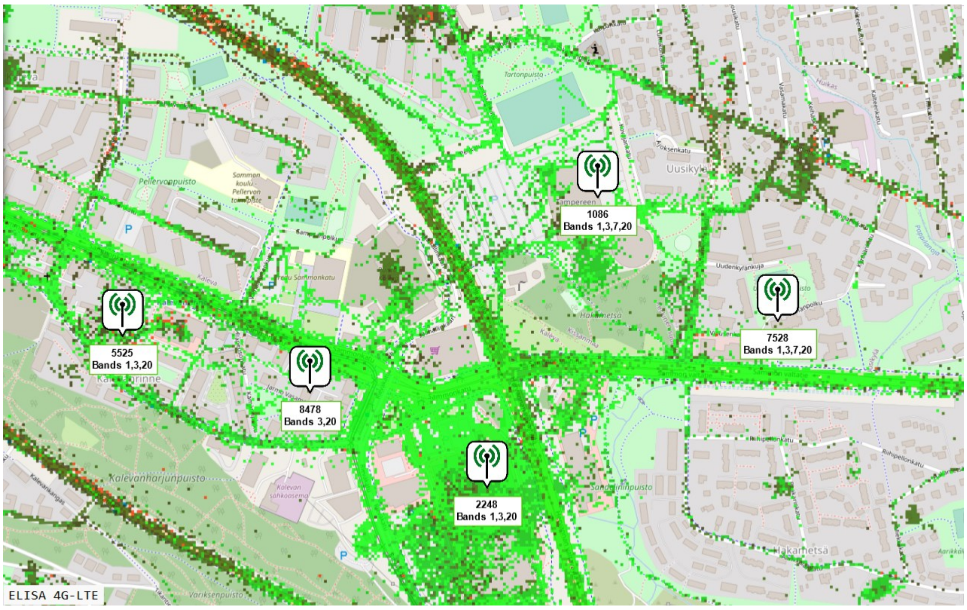

Figure 11. Approximate Elisa mobile tower locations in target area (source, Cellmapper)

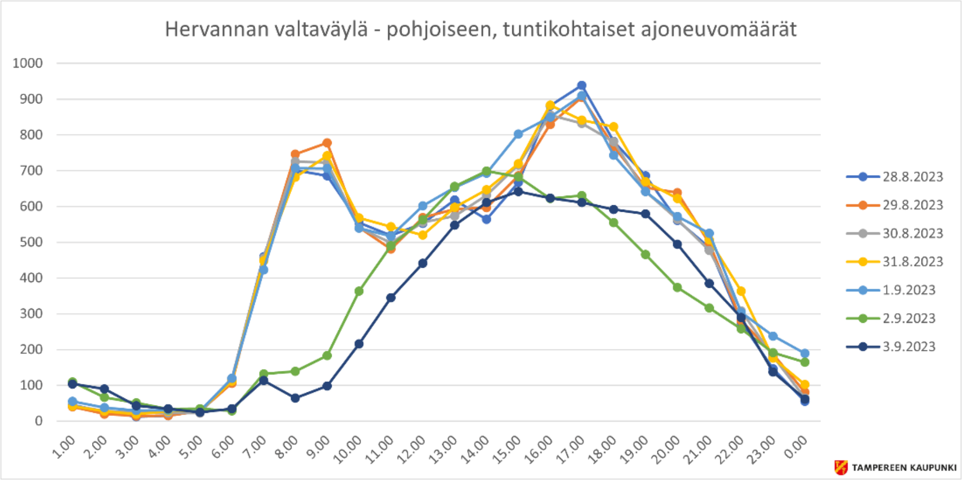

Figure 12. Hourly traffic in Hervannan valtaväylä, direction North

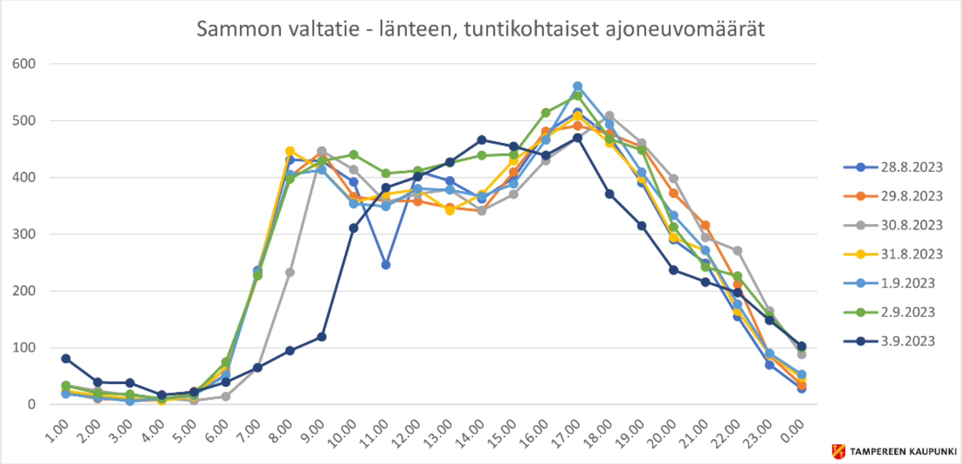

Figure 13. Hourly traffic in Sammon valtatie, direction West

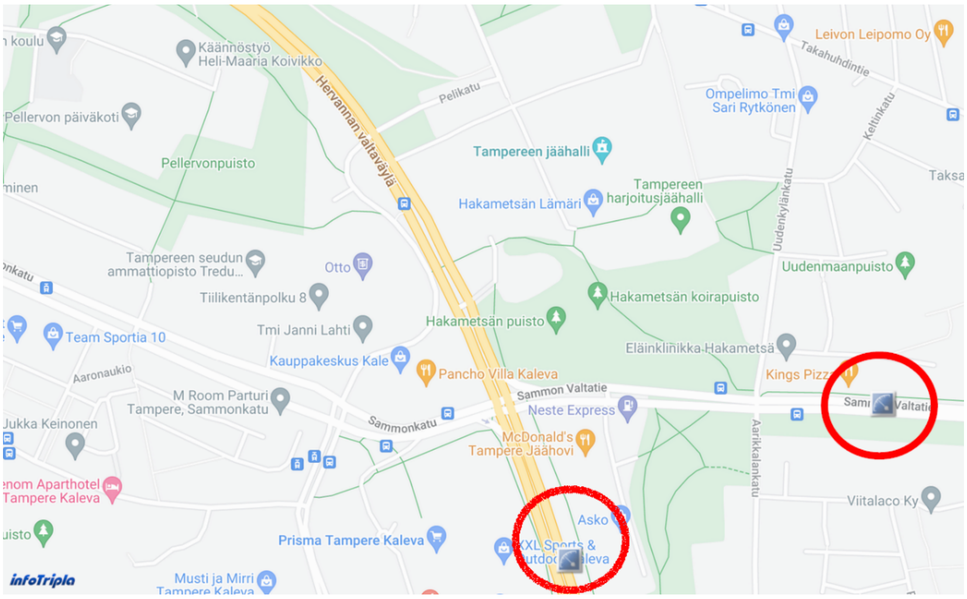

Figure 14. Loop detectors calculating hourly traffic in target area, Hervannan valtaväylä and Sammon valtatie

8.2 Physical tests in Hakametsä

Physical tests in the intersection TRE 533 were conducted in three different parts, with two of them focusing on end-to-end communication and one focusing on testing various cyber security scenarios.

The first tests were conducted on 1 November 2023 from noon until afternoon. During these tests, errors in the coordinates of MAPEM files were noticed. As a result, the short-range application could not parse the message correctly and only the long-range application could be tested. The coordinates provided were one decimal too short, which radically changed their position when parsing the values. This error did not affect packet captures, and 5,143 C-ITS messages were captured during the tests. The error on MAPEM coordinates was fixed together with the TLC manufacturer during the following day.

The second tests were conducted on 8 November 2023 around noon. The coordinate error identified in MAPEM was fixed before these tests and both the short- and long-range applications were able to be tested. In these tests, 30 traffic light cycles were recorded and 9,924 C-ITS messages were captured. No new errors were found during these tests and the pilot system operated properly. Video recordings were captured for both short-range and long-range systems.

The third tests focused on testing the pilot system on different cyber-related scenarios. These tests were carried out at noon on 19 December 2024. In these tests, the impact to short-range latencies was tested by leaving off the signing of the messages. The scenario of unsigned messages was also tested when the security features were turned on. This allowed personnel to test whether the system discards unsigned messages expectedly.

Figure 15 depicts the signal timings used in target intersection. The yellow timing is one second when going to green and three seconds when going to red.

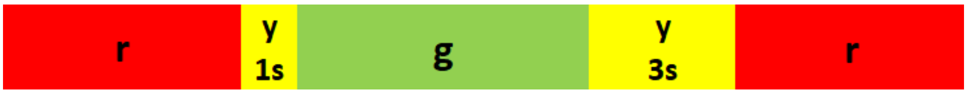

Figure 15. Signal phase timings for yellow (Pelikatu, F0-1 and F0-2, signal group 6)

8.3 Test results

Figure 16 depicts the data flow in the case of short-range measurements from the Traffic Light Signal (TLS) to the user's mobile phone User Interface (UI).

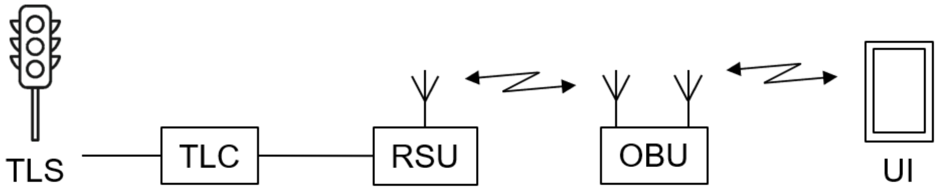

Figure 16. Data flow in short-range communication

During short-range measurements, over 15,000 C-ITS messages were captured over a span of 65 minutes, spread over two days. The average latency for communication between RSU and OBU was 13 ms. This average latency stayed the same through all captures. Table 6 outlines the detailed results from packet captures.

Table 6. Packet capture results between RSU and OBU

Packet capture results						
Date	Time	Packets	Average latency	Min latency	Max latency	Standard deviation
1.11.2023	11:54 – 12:04	2,197	13 ms	7 ms	23 ms	3 ms
1.11.2023	13:29 – 13:41	2,946	13 ms	7 ms	23 ms	3 ms
8.11.2023	10:21 – 10:34	2,993	13 ms	7 ms	25 ms	3 ms
8.11.2023	10:41 – 10:59	4,274	13 ms	7 ms	25 ms	3 ms
8.11.2023	11:06 – 11:18	2,657	13 ms	7 ms	22 ms	3 ms
Total / Average	65 min	15,067	13 ms	7 ms	24 ms	3 ms

Table 7 outlines the detailed latency results noted down from the video analysis. The results are divided into four groups complying with the signal phase cycle: from red to yellow (R_Y), from yellow to green (Y_G), from green to yellow (G_Y) and from yellow to red (Y_R). The results presented here are delay differences compared to the traffic light signal phase change seen in the video recordings.

Table 7 and Table 8 depict delays measured from mobile app user interface traffic light signal status changes compared to actual signal status at the intersection. Table 7 presents delays when messages are signed at the RSU and Table 8 shows delays when messages are flowing through the system unsigned. More detailed graphs are presented in Appendix 1.

Table 7. Delays between TLS (Traffic Light Signal) and UI, message signing enabled

Delay seen in mobile application UI compared to TLS, signing enabled (N=10)		
signal phase	delay average (s)	standard deviation (s)
R_Y	0.53	0.082

Y_G	0.48	0.079
G_Y	0.50	0.094
Y_R	0.52	0.079

Table 8. Delays between TLS (Traffic Light Signal) and UI, signing disabled

Delay seen in moble application UI compared to TLS, signing disabled (N=10)		
signal phase	delay average (s)	standard deviation (s)
R_Y	0.52	0.092
Y_G	0.53	0.134
G_Y	0.53	0.134
Y_R	0.51	0.137

The packets captured during short-range tests contained both SPATEM and MAPEM messages. Table 9 provides the results for the size of each C-ITS message type captured when signed and unsigned.

Table 9. C-ITS message types sizes captured

C-ITS message	Size signed	Size unsigned
MAPEM	977 bytes	722 bytes
SPATEM	509 bytes	255 bytes

The three generic C-Roads test cases for SPATEM and MAPEM were all passed. In these three tests, all the verification points were passed on all test runs. Table 10 presents the results of these generic MAPEM and SPATEM test cases.

Table 10. Results of generic SPATEM and MAPEM test cases for short-range

Generic SPATEM and MAPEM tests	pass / fail
TC_CROADS_SI_GENERIC_ITS-G5_SPaTEM-MAPEM_Timing_01_R2.0.4	pass
TC_CROADS_SI-GENERIC_ITSG5_MAPEM_Location_03_R2.0.4	pass
TC_CROADS_SI-GENERIC_ITSG5_MAPEM_SPATEM_Generic-Relation_02_R2.0.4	pass

Two C-Roads test cases were conducted relating to the Signal Phase and Timing Information use case. The results of these tests are presented in

Table 11.

Table 11. Results of Signal Phase and Timing test cases for short-range

Signal Phase and Timing (SI-SPTI) tests	**pass/fail**
TC_CROADS_SI-SPTI_ITSG5_SPATEM_SignalPhaseAndTimingInformation _08_R2.0.4	Inconclusive / Fail
TC_CROADS_SI-SPTI_ITSG5_SPATEM_speeds _08_1_R2.0.4	Inconclusive / Fail

On the test case TC_CROADS_SI-SPTI_ITSG5_SPATEM_SignalPhaseAndTimingInformation _08_R2.0.4, verification point 1 was passed on all three test runs. This verification point verified that the timestamp and moy value were received with accurate and relevant data. However, verification point 2, to verify that the data elements (signalGroup, minEndTime, maxEndTime) were received with relevant and accurate data of current and upcoming signal phases, had inconclusive results. All the previously mentioned data elements were present in the SPATEM message and received correctly by the receiver. Even though data elements were present, the value on maxEndTime of timing had a value of unknown (36001) in multiple messages. Also, the messages only relayed the data of the current signal phase; none of the messages had information of upcoming signal phases.

The test case TC_CROADS_SI-SPTI_ITSG5_SPATEM_speeds _08_1_R2.0.4 had three verification points that needed to be passed. The first verification point was identical to the previous test case's verification point 1, verifying timestamp and moy values. This verification point was passed during all three test runs. The second verification point was also identical to the previous test case's verification point 2, verifying signal phase and timing data elements. The results for this verification point were again like the previous test cases, resulting in inconclusive results. All the specified data elements were found in the messages, but the maxEndTiming had values of unknown (36001) in some instances. Also, none of the messages had information on upcoming signal phases; they merely relayed information of the current signal phase. Verification point 3 focused on verifying that the data elements are received, and that data frame "speed" is not concluded. None of the captured messages contained the data frame "speed".

8.3.1 Long-range measurement results

Figure 17 depicts the data flow in the case of long-range measurements. The results are divided into four groups complying with the signal phase cycle: from red to yellow (R_Y), from yellow to green (Y_G), from green to yellow (G_Y) and from yellow to red (Y_R). Table 12 depicts delays measured from mobile app user interface traffic light signal status changes compared to actual signal status at the intersection. More detailed graphs are presented in Appendix 1.

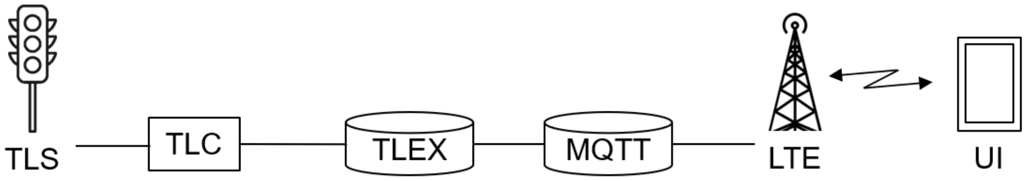

Figure 17. Data flow in long-range communication

Table 12. Delays between TLS and UI

Delay seen in mobile application UI compared to TLS (N=10)		
signal phase	delay average (s)	standard deviation (s)
R_Y	0.46	0.117
Y_G	0.47	0.048
G_Y	0.49	0.166
Y_R	0.55	0.095

The same C-Roads test cases were conducted for the long-range as were conducted for the short-range. First were the three generic test cases for SPATEM and MAPEM messages. Table 13 presents the results of the three generic SPATEM and MAPEM test cases.

Table 13. Results of generic SPATEM and MAPEM test cases for long-range

Generic SPATEM and MAPEM tests	**pass / fail**
TC_CROADS_SI_GENERIC_ITS-G5_SPaTEM-MAPEM_Timing_01_R2.0.4	pass
TC_CROADS_SI-GENERIC_ITSG5_MAPEM_Location_03_R2.0.4	pass
TC_CROADS_SI-GENERIC_ITSG5_MAPEM_SPATEM_Generic-Relation_02_R2.0.4	pass

For these C-Roads test cases the ITS-G5 communication was replaced with cellular communication. However, the test variables and expected behaviour were the same as specified for ITS-G5 test cases.

Two Signal Phase and Timing C-Roads test cases were conducted for long-range communication. Table 14 presents the results of these test cases.

Table 14. Results of Signal Phase and Timing test cases for long-range

Signal Phase and Timing (SI-SPTI) tests	pass/fail
TC_CROADS_SI-SPTI_ITSG5_SPATEM_SignalPhaseAndTimingInformation _08_R2.0.4	Inconclusive / Fail
TC_CROADS_SI-SPTI_ITSG5_SPATEM_speeds _08_1_R2.0.4	Inconclusive / Fail

As the exchanged messages are of the same format and type as in short-range, the results are the same. In both test cases the SPAT messages only held information of the current signal phase. These test cases expected SPAT to have information also from the upcoming signal phases. This led to the results' fail status.

8.3.2 Security-related results

The security-related tests focused on deploying and testing EU CCMS on the pilot system. The short-range system was enrolled to EU CCMS and signature verifications were enabled.

The results indicate a successful signing of all C-ITS messages transmitted from the RSU to the OBU. This verification was done by inspecting captured messages received by the OBU. Of the captured messages, 100% held GeoNetworking secured packet information, which contains the signature and certificate information.

However, the long-range communication system was unable to support EU CCMS during this project. This was due to the central ITS station being deployed earlier before this project, without the necessary resources for signing messages. The security of the system was handled with different elements in order to maintain the confidentiality, integrity and availability of the information and service.

The results also showed that different OEM manufacturers might have existing tools to support automatically registering and enrolling stations to EU CCMS.

In the project, one of the tested cyber security-related scenarios was testing the behaviour of the short-range system when encountering unsigned messages. In these scenarios, the system should discard any messages that do not have the required security information attached to them. Figure 18 presents a comparison of short-range user interface with signed and unsigned messages.

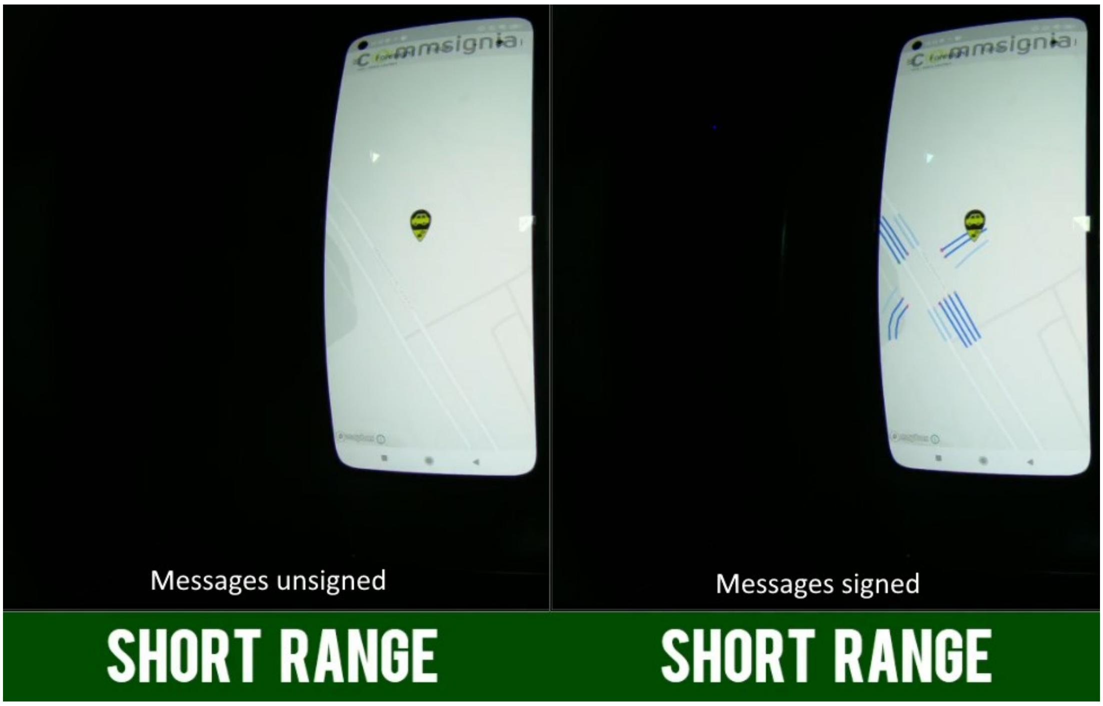

Figure 18. User interface comparison between signed and unsigned MAPEM messages

The user interface inside the vehicle functioned differently depending on if the messages were signed or unsigned. When messages are signed, the user interface renders the lane topology on top of the target intersections together with the traffic light status for each lane. When messages are unsigned, they are discarded, and the user interface won't render their contents. As seen from the figure above, the user interface did not render MAPEM and SPATEM messages when unsigned. On the left side of the figure, messages are unsigned and the user interface does not display the contents of these messages. On the right side of the figure the messages are signed, and the user interface displays MAPEM lanes and SPATEM signal states on the map. This is because the system has discarded the unsigned messages and therefore doesn't have any user interface information to display.

9 Conclusions and recommendations

9.1 Short-range related conclusions

9.1.1 Discussion of the results

In this project, one of the key research topics was the compatibility of LTE-V2X Direct technology together with C-Roads specifications. Technologically, LTE-V2X Direct is not specified in C-Roads. The Roadside System Profile (RSP) profiled by C-Roads defines a common base for ITS-G5 communication between roadside and vehicle [17]. ETSI has provided a profile for LTE-V2X Direct roadside stations, which is based on the C-Roads profile. Additionally, C-ITS services and use cases profiled in C-Roads have ITS-G5 as the listed communication technology to be used.

However, LTE-V2X is capable of carrying the same message sets and operating with the same network protocol as ITS-G5. Although the GeoNet header contains a media-specific section, the content remains identical for both LTE-V2X Direct messages and ITS-G5 messages. In practice, using LTE-V2X would involve transitioning the radio to leverage 3GPP-specified Physical (PHY) and Medium Access Control (MAC) layers. [4]

From a functional perspective, the results indicate that LTE-V2X Direct technology is compatible with meeting the requirements specified for C-ITS services and use cases by C-Roads. The results demonstrate that replacing ITS-G5 with LTE-V2X Direct did not affect the operation of the Signalised Intersection (SI) service. The same SPATEM and MAPEM messages could be broadcasted as signed messages using LTE-V2X Direct radios. Replacing the radio protocol from ITS-G5 to LTE-V2X Direct did not create any functional differences in the operation of the SI service.

The results demonstrate that LTE V2X Direct, serving as the access layer technology, is compatible with the upper layers utilised in C-Roads.

The project highlighted the absence of a European standard in place for communication between Roadside Units and Traffic Light Controllers (TLC). According to C-Roads C-ITS roadside system profile Requirement ID: RS_RSP_007(1), roadside ITS stations should have the capability to generate and transmit infrastructure messages, such as SPATEM and MAPEM.

During the project, it became clear that the communication between RSU and TLC is currently highly based on proprietary protocols that are specific to the TLC and RSU manufacturers. SPATEM and MAPEM messages can be generated inside TLC and transmitted to RSU, or RSU can generate the messages based on the parameters and inputs it receives from TLC.

There is no technical interface defined in the ETSI standard between the Roadside ITS station and ITS application. In the Netherlands, the RIS FI interface (Roadside ITS Station Facilities Interface) has been specified as part of the Talking Traffic architecture. In this architecture, ITS applications send information via the RIS FI interface to the roadside ITS station, which then distributes it to other ITS stations. The interface description doesn’t prescribe communication media (e.g. ITS-G5) to be used; instead, it focuses on the information that needs to be communicated. [18]

However, this RIS FI interface is mostly implemented in the Talking Traffic program and in programs following its specifications. It is not detailed in C-Roads, nor is it interoperable out of the box with products that are not used in the previously mentioned programs.

The results from short-range tests indicate that most of the latency is being generated at the end-user application. Capture results demonstrate an average latency of 13 milliseconds for the radio interface between RSU and OBU. When compared to latency measured by video at the end-user device, which was consistently averaged at around 0.5 seconds, it is evident that processing and displaying the information from the incoming packet causes most of the latency.

The signing of messages at the RSU does not seem to add significant latency to the communication. The results indicate that delays are quite similar in the short-range scenario for both signed and unsigned messages. However, it's worth noting that the results are rounded to the nearest tenth of a second, which might mean that the potential additional latency from signing may be so minimal that it is not distinguishable within the rounded results.

This study and its results demonstrate that the design and implementation of an end-user application can significantly influence the overall performance of the application. The application should be optimised to minimise latency and provide the most real-time service possible. For informative services such as the Signalised Intersections Signal Phase and Timing Information, the measured latencies were sufficiently low. In informative services, there are no critical safety aspects that would require even faster message delivery.

The RSU needs to have reliable connections to the Traffic Control Centre and the PKI, either through a fixed line or mobile connection. Connection with the PKI is needed for requesting new certificates and for updates of the European Certificate Trust List (ECTL) and Certificate Revocation List. [9]

9.1.2 Future outlook

The tests conducted in this study have demonstrated that the technology works within the test configuration. However, more tests are required to assess the scalability of the solution and its performance in dynamic situations, such as how the technology operates with a large number of vehicles and at high speeds.

The LTE-V2X Direct (3GPP Release 14) technology is expected to have a short lifespan and it will likely be replaced by the newer NR-V2X Direct technology (3GPP Release 16 and newer). NR-V2X Direct is able to support more advanced V2X use cases than LTE-V2X Direct but is not backward compatible with LTE-V2X Direct. The first NR-V2X modules have appeared on the market [24] and are expected to be implemented in OBUs and RSUs. Major automotive developers have plans to deploy the technology [16]. However, additional tests are necessary to ensure that the technology meets its requirements before widespread deployment.

For the new NR-V2X Direct, technology standards are under work and some are even already published. Under the impulse of 5GAA, ETSI has published profiles for LTE-V2X Direct ITS stations and is working on profiles for newer NR-V2X

Direct ITS stations. These NR-V2X Direct stations are expected to eventually replace LTE-V2X stations. From the C-Roads perspective, currently C-Roads has only addressed ITS-G5 as short-range technology. At this juncture, C-Roads has published profiles for ITS-G5 Roadside units and mobile stations, and Car2Car Consortium for ITS-G5 vehicle ITS stations. In order to deploy C-V2X devices in the future, at a security level L2 environment, protection profiles must be generated for C-V2X Direct ITS stations. These profiles can be largely based on the protection profiles for ITS-G5 devices.

Currently for LTE-V2X Direct, the GeoNet header is the same as for ITS-G5. However, in the future the media-dependent part of the GeoNet header for NR-V2X may contain different data.

In the future, if RSUs are deployed in large numbers at signalised intersections, a standard for interfacing between RSU and TLC would be invaluable. As experienced in this project, proprietary interfacing between different manufacturers can consume additional time and resourses for the parties deploying RSUs. This is because of the necessity to develop proprietary solutions, which may differ between TLC and RSU manufacturers. A standardised interface could be required from equipment vendors in potential tenders. This would also reduce the potential vendor lock-in, as products operating with standardised interfaces could be more easily replaced.

The short-range communication utilises the 5.9 GHz frequency band. However, its range can be influenced by the presence of large objects, such as trees, which attenuate the signal. Therefore, it is crucial to maintain a clear line-of-sight between the roadside antenna and the vehicles. To ensure this, antennas should be positioned at a sufficient height to prevent signal interferences from buildings or foliage. This requirement applies to both ITS-G5 and C-V2X Direct communications.

The large-scale deployment of RSUs on the road network would generate numerous requirements for the responsible party. Physical installations would be necessary at the roadside and in intersections. The responsible party would have to acquire necessary competency to manage and install RSUs. In addition to installation, there would be a need for ongoing maintenance, monitoring and lifecycle management of the RSU network. All of these are resources that the responsible party needs to take into consideration when deploying RSUs.

9.2 Long-range related conclusions

9.2.1 Discussion of the results

The testing and demonstration of C-ITS long-range technologies was a required component of the test scenario in this study. Its main objective was to serve as a reference implementation during tests at an intersection equipped with C-ITS dual-communication capabilities, both short- and long-range communication.

For the test, both the mobile network operator and the location of the test intersection were selected randomly, without any interaction with the mobile network operator. Hence, the intersection can be considered as a randomly selected, neutral and non-optimised reference implementation.

Throughout the tests, the latency between the events, from actual signal change on the intersection and to the representation of the same event in the mobile application user interface, consistently remained close to 0.5 seconds. This can be interpreted as the total delay for the entire long-distance C-ITS system communication chain in our study.

These results could be compared e.g. to the Dutch national large-scale C-ITS deployment, Talking Traffic, where a requirement for maximum end-to-end latency for traffic light related use cases was set at one second via telecom 4G/LTE networks. The results of this study, with latencies close to 0.5 seconds, indicate similar performance to those specified in the Netherlands. [32]

According to a study done on "Classification of C-ITS services in Vehicular Environments" [28], the maximum latency required for Signalised Intersection C-ITS use cases is 500 milliseconds. This may be seen as quite a challenging target, since the transmission path in long-range solutions may be lengthy, involving numerous network and software actors. However, in our study even this target time was achieved.

When considering the functional usage of delivering informative C-ITS messages to vehicle drivers, the results can be evaluated in terms of the natural driver reaction time. It can be concluded that the latency of sending C-ITS messages could be perceived as relatively small, often being shorter than the typical driver reaction time.

Considering the randomly selected neutral test location, and when compared to other C-ITS deployments, the requirements set forth in reference literature and the functional usage of C-ITS messages, the results could be considered very positive.

When analysing the results and drawing wide-scale conclusions from the long-range demonstrations, it is also essential to understand the natural unpredictable nature of C-ITS long-range solutions.

For instance, when incorporating commercial "non-SLA" mobile networks into long-range solutions, an alteration in the selected test area can impact network coverage and quality. The natural variation in the number of mobile network users across different locations, such as a quiet suburbia, a busy business park or a lively student village within a city, can also significantly influence both the performance of the mobile network and test results accordingly.

Furthermore, in long-range test scenarios, the high-level technical architecture of the C-ITS long-range system has a strong influence on the performance of the system. For example, C-ITS backend systems might be situated on a public "non-SLA" internet network in different countries, with different cloud service providers being utilised. The communication chain may involve a varying number of actors, and the technological implementations and the performance of software interfaces between systems may vary.

All the above-mentioned factors collectively contribute to the unique technological fingerprint of C-ITS long-range deployments, making it challenging to pinpoint the actual reasons for problems or variations in performance when they arise.

Figure 19 shows the end-to-end communication chain including active nodes/systems used in this project for long-range communication.

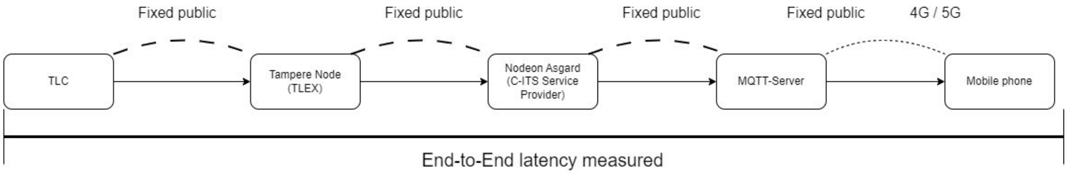

Figure 19. Long-range communication chain

Overall, the results of the long-distance study were encouraging. When the usage of C-ITS messages is focused on informative C-ITS applications, it could be assessed that under the tested circumstances, the performance of the long-distance system is adequate.

9.2.2 Future outlook

The contribution regarding the future outlook of C-ITS long-distance solutions varies from broad, high-level questions and challenges to more focused inquiries and perspectives in this chapter.

In the future, evaluating various communication and architectural methods becomes crucial in alignment with the specific purposes of C-ITS messages. C-ITS, recognised as the initial significant phase towards Cooperative, Connected and Automated Mobility (CCAM), holds particular importance. This phase plays a key role in establishing the technological foundation for seamless information exchange between intelligent traffic infrastructure and vehicles (as well as among vehicles).

This study, contextualised in its applications of using C-ITS messages for purely informative purposes, provides positive feedback on the mobile network based long-distance solution and its performance. Future assessments should involve a critical evaluation of the long-distance solution and overall technical architecture concerning the following phases of the CCAM development.

Key research questions may focus on elements such as: “If one selects long-distance solutions as a technological foundation for constructing a large-scale C-ITS digital infrastructure, how should the system and its components be organised to ensure control over all technical layers and actors, thereby offering system owners and administrators a controlled end-to-end service level to guarantee system performance?" This question includes the comprehensive technical approach to the C-ITS ecosystem, including elements such as mobile networks, fixed closed and public networks, cloud service providers, backend systems, as well as the protocols and interfaces utilised between communication chain actors.

To ensure resources for long-distance C-ITS services in the future and enhance the quality of service across the entire communication chain, several potential actions can be taken. Some are relatively straightforward, involving the redefinition of the overall technical architecture of the C-ITS ecosystem. However, others may require more extensive efforts, such as regulatory tasks carried out by the public sector and cooperation between car manufacturers and public authorities to clarify the policies in the usage of more sophisticated future ADAS features (Advanced Driver Assistance Systems) of the vehicles, which utilise information from smart infrastructure passed to the usage of vehicles. This cooperation requirement applies to all C-ITS ecosystems, not only long-distance versions.

Possible solutions may involve various elements including using closed point-to-point SLA-supportive communication channels between selective elements in the communication chain (e.g. between a closed customer network and back-end systems located on the public internet network within cloud service providers), relocating back-end systems geographically closer to the users, implementing mobile network slicing, network expansion, neutral host networks, and network monitoring.

More detailed insights into potential improvements related to the mobile networks part of the communication chain are presented in an unpublished report titled "Utilisation of commercial mobile networks in the deployment of C-ITS services" (Traficom, 2024).

It is also important to note that the inclusion of signatures in a long-distance solution can have an impact on the resources needed for transmission and the transmission latency.

According to current C-Roads specifications, each message needs to be signed, and inclusion of the GeoNet header is mandatory. Potential solutions to decrease resources include implementing signing at the facility layer (without the necessity to add the GeoNet header to each message) or utilising certificates at the transport layer according to ISO 21177.

However, signing at the transport layer is currently not yet possible due to a lack of available commercial products. These potential solutions are currently under examination in initiatives such as the C4Safety project in the Netherlands. Once all required standards are published, it may also be adopted by C-Roads.

For the long-range communication case, 5G mobile networks provide opportunities to reduce the transmission path by leveraging Multi-Access Edge Computing (MEC). MEC provides opportunities to move computing of services from a centralised cloud to the edge of the network, closer to the customer. In this scenario, C-ITS end devices and users exchange messages over a broker on the MEC that can serve customers in a certain small physical area. Brokers from different providers can exchange information with each other.

9.3 Security-related conclusions: towards L2

9.3.1 Discussion of the results

During the pilot, certificates from two RCAs were tested: certificates from the EU RCA and certificates from Microsec. Due to the tools provided by the device manufacturer, which has close collaboration with Microsec, the use of Microsec certificates was straightforward. However, when it came to the EU RCA certificate there were several challenges in the implementation of the certificate.

The results of the project show that current C-V2X units are compatible with EU CCMS L0. The units were able to be registered to both the EU RCA and Microsec RCA, which operate the L0 service. However, activating the EU RCA certificates on the units proved to be more challenging. With Microsec RCA, the process of activating certificates was quite straightforward, and both the RSU and OBU were equipped with these certificates. When activated, 100% of the messages sent by RSU were signed with these certificates.

The short-range system was proven to operate securely by testing it with unsigned messages. When the system encountered unsigned messages, while having security enabled, all the unsigned messages were dropped by the system. This indicates that the communication is valid only when the units are equipped with the needed certificates and the messages are signed properly.

For long-range IP-based communication, the signing of messages was not possible during the project. The platform deployed in Tampere before this project started did not support the signing of messages used during the project.

The deployment of both short-range and long-range systems highlighted the difference on type of communication and its relation to cyber security. In short-range, the communication is done using physical units installed in the intersection and communicating using short-range radio. This means that anyone capable of getting access to this sort of technology could send false information to other radios near it. This is why the certification of units and using PKI is essential for authentication. Long-range communication, however, is a closed system in that every actor in it can be authenticated before allowing access to the system. In long-range communication, common security protocols can be used to secure communication over the internet (Transport Layer Security, TLS). Also, when the C-ITS messages are travelling through backend systems, their behaviour and connections can be monitored constantly, allowing suspiciously behaving stations to be dropped.

9.3.2 Towards L2

During the pilot, security level L0 was tested. The central elements for Level 1 are expected to become available in the beginning of 2024, which is also when the two-year transition period towards Level 2 starts, finishing at the end of 2025.

The requirements for the deployment and operation of C-ITS systems are described in the C-ITS Security Policy [8] and the Certificate Policy [9]. The Security Policy sets requirements for the deployment and production use of the C-ITS stations, towards the C-ITS station operators, while the Certificate Policy sets requirements for the Certification Authorities. The requirements for authorities have been analysed in the Security Policy [11].

At security level L2, the C-ITS stations have to be designed, developed and assessed so that they meet the C-Roads specifications. The stations have to be assessed by a SOG-IS recognised test lab and certified using security assessment criteria against a certified protection profile, as specified in Common Criteria (ISO

15408) and approved by the CPA. So long as a certified protection profile is not available, C-ITS stations are allowed to be assessed and certified by a security target with a similar or higher evaluation assurance level. Protection profiles for ITS-G5 ITS stations are currently being developed for Road Side Units by C-Roads and for vehicles by Car2Car. The draft protection profile does not put specific requirements to the ITS-G5 radio link, only referring to the access layer standard EN 302 663, and so the replacement with another communication medium like LTE-V2X Direct or NR-V2XDirect would not require many editing changes. However, the whole process for generating and certifying the protection profile has to be redone.

At security level L1, the C-ITS stations have to be evaluated by a SOG-IS recognised test lab, to ensure that the C-ITS station is protected against attackers with basic attack potential [7].

9.3.3 Requirements for C-ITS station operators

C-ITS station operators have to set up an ISMS (Information Security Management System) according to ISO 27001, including all the operated C-ITS stations, as discussed in Chapter 6.

For L1, compliance of the ISMS according to ISO 27001 may be conducted internally by the C-ITS station operator and shall be confirmed by a self-issued statement of compliance [7].

The process for setting up the ISMS and the ISO 27001 assessment starts with making a risk assessment (identifying risks, steps for protecting information assets, action plans, identifying responsibilities) [12].

C-ITS station operators can freely choose the RCA for getting the credentials, according to the EU C-ITS trust model. The selection can be affected by the C-ITS station manufacturer’s preferences or the national or local authorities’ requirements. Potentially, the C-ITS station manufacturer could take care of C-ITS station registration in the EU CCMS.

If the C-ITS operator wants to register its C-ITS stations, it needs to first register to the EA (Enrolment Authority), a subCA of the RCA. In case the C-ITS stations are used for “special (governmental) purposes,” the C-ITS station operator must prove the authorisation of the competent public authorities of the respective Member State. Specification of “special (governmental) purposes” is up to national authorities. The CA may therefore require a document certifying that the permissions requested are compliant with the potential governmental restriction.

9.3.4 Privacy-related issues

As C-ITS is based on exchanging information between ITS stations, there is potential risk of tracking movement of these stations. In this project, only roadside units transmitted information, and thus no privacy-related issues were found in the pilot. The information exchanged consisted of information from traffic lights and intersection topology, and these SPATEM and MAPEM messages holding this information do not contain any personal information. This is the same for both short-range and long-range communication.

When using short-range communications, the ITS stations also continuously transmit CAM messages which contain identity information. To meet the privacy requirements in ETSI TS 102 940 [29], the authorisation tickets and all addresses and identifiers (such as the ITS station ID in the C-ITS messages) must change regularly.

Users must provide consent [31] to participate in the C-ITS ecosystem. Only by accepting to transmit CAM messages will the users be able to receive C-ITS messages.

In the Probe Vehicle Data service, data generated by vehicles is aggregated at the Road Side Unit and used for road traffic management. The collection of vehicle data can generate concerns about the traceability of vehicles when the service is used by road operators or service providers. Different Member States have taken different measures to assure that GDPR requirements are fulfilled, but there is no certainty or consensus in C-Roads at the moment that the approach from individual Member States can be adopted in all Member States to guarantee compliance with GDPR. [30]

The Probe Vehicle Data service is used with long-range communications in intersection applications in the Netherlands and Flanders. CAM messages are sent when vehicles approach an intersection. The main aim is to be able to replace loop detectors at intersections with vehicle-generated data. The user of the service provides consent to the service operator, e.g. the operator of the mobile phone app. To ensure that user consent is formally enforced, the road operator needs to have an agreement with the respective service operator. Data must be anonymised by the service operator prior to sharing it with the road operator, and by the road operator prior to sharing it with service operators. When sharing information, the road operator also needs an agreement with the other parties to make sure that the original agreement between the road operator and the respective service operator is respected by the other parties. [30]

Vehicle manufacturers collect data, which is mainly technical information. By linking it to e.g. the vehicle identification number, the data can be linked to the owner or driver and can become personal data that should be processed in accordance with the GDPR. In the case of mobile applications, the software manufacturer must ensure that the application collects data in a GDPR-compliant manner.

9.4 Recommendations

9.4.1 Short-range communications

LTE-V2X Direct is a technology with a short lifespan due to the advent of the newer NR-V2X Direct technology. At the same time, EU CCMS is proceeding towards security Level 2, which puts additional security requirements on C-ITS stations. Hence, investments in deployment of the technology should be delayed until commercial NR-V2X Direct ITS stations for Level 2 are on the market.

At this moment, it is not clear how ITS-G5 and LTE/NR-V2X can function together in the 5.9 GHz range. Also, the support of vehicle manufacturers for the technologies is not completely clear. Volkswagen has more than 2 million vehicles on the market supporting C-ITS through ITS-G5 technology, and Volkswagen's newest C-ITS release supports several of the C-Roads HLN (Hazardous Location Notification) and RWW (Road Works Warning) use cases. However, no other manufacturers have made public announcements of equipping vehicles with ITS-G5. Major automotive manufacturers, including Volkswagen, have expressed support for NR-V2X [16]. However, no tests with NR-V2X have been published yet. Hence, it is suggested to closely follow the status of the co-existence discussions and the V2X market prior to making decisions on the deployment of short-range communication technology.

ITS stations operating in the 5.9 GHz frequency band (ITS-G5, LTE-V2X and NR-V2X Direct) are prone to possible disturbance in radio transmissions due to buildings or terrain. This is why it is crucial to find an optimum position for potential RSU installations. Any road operator looking to install RSUs to its road network should pay attention to ensuring optimal position. This would mean ensuring line-of-sight to all possible directions of traffic and positioning RSU far from large metallic objects or walls.

9.4.2 Long-range communications

Currently, the exchange of C-ITS messages in mobile networks operates on a best-effort basis. The evaluation of mobile networks to support critical C-ITS applications and subsequent phases of CCAM development needs to be done on a broader scale, including also a larger number of devices. Since best-effort mobile networks do not provide a guarantee on service delivery, they should currently only be used for informative purposes. Technical solutions for addressing coverage and service availability issues are presented in detail in the unpublished report "Utilisation of commercial mobile networks in the deployment of C-ITS services" (Traficom, 2024).

When considering the use of mobile networks for critical information, e.g. for automated vehicles, authorities should decide on how much technical control they want to retain. Using mobile networks results in saving both money and time as investments in roadside units will not be needed and existing roadside infrastructure is already widely connected to the network [27].

However, the potential downsides include reduced control of technical elements. When using short-range RSUs, the responsible party has control of the placement, number of units, coverage and technology employed. Using commercial mobile networks shifts control over to MNOs and might create a need for governance to ensure quality of service for critical applications. When shifting control over to MNOs, the MNO is also responsible for the competence and management needed to operate the network.

The complete delivery chain consists of several legs, including transmission from the road operator backend over an interchange node to the service provider backend. Load tests of the complete data chain need to be performed to assess the impact on latency.

In current C-Roads specifications, all messages must be signed, which may require considerable resources and hence also impacts the performance of backend servers and interchange nodes and increases delivery delay. Even though signing may require considerable resources, when done in a cloud environment it is possible to allocate additional resourses for the operation. The potential alternatives for signing and their impact on both resource consumption and security should be assessed. For this purpose, the standardisation work in ETSI and research in the field should be closely followed, and in the C-Roads platform discussions to implement the optimal solution should be supported.

In C-Roads, it should be assured that solutions are technology-agnostic, both for short-range and long-range solutions. Currently, long-range communications include GeoNet header, which allows forwarding the message by hybrid OBUs (i.e. long range + ITS-G5). As the GeoNet header has a media-dependent section, which may be different for NR-V2X Direct as well as for ITS-G5, this solution is not technology-agnostic.

5G mobile networks provide opportunities to reduce the transmission path by leveraging Multi-Access Edge Computing (MEC). MEC provides opportunities to move the computing of services from a centralised cloud to the edge of the network, closer to the customer. ETSI has specified a V2X Information Service in which V2X messages are routed over brokers at the MEC to vehicles in the specified area [25]. In this case, the messages are hence not further transferred from the base station to an application server on the cloud, but to a broker on the MEC, which directly sends the message to the relevant vehicles. In this way the transmission path between vehicles is drastically shortened. 5GAA has set up demonstrations for this approach in multi-operator, multi-MNO and multi-vendor environments [26]. MEC is seen as necessary to support safety-critical V2X applications, but the deployment requires collaboration of both road authorities, MNOs and OEMs [26].

9.4.3 Security

In this project, tests were made with security level L0, which was the only one available in 2023. Security Level L1 will become available in 2024, and the transition period is expected to finish by the end of 2025, after which Level 2 will be operational.

In order to be able to participate in Level 2, C-ITS station operators must have the ISO 27001 certificate to exchange messages using the EU CCMS. As this process can take considerable time, potential C-ITS station operators are advised to start the process to get the ISO 27001 certificate.

Regarding central ITS stations, the requirements for level 2 are not completely clear yet. Specification work towards a protection profile for a central ITS station has not yet started, and it is not clear whether one will become available. Hence, central ITS stations will have to be certified on a singular basis towards a "Security Target." Tests to be validated in SOG-IS recognised test labs are described in the CPOC protocol [7]. Currently, there is no SOG-IS recognised test lab in Finland.

If the C-ITS station is used for governmental purposes, the C-ITS station operator should have the permission of the relevant Member State authority. These processes must be put in place.

10 Bibliography

[1] C-Roads, 2023, Introduction to the C-Roads WG2 Deployment Documentation and Requirements, Version 2.0.7

[2] 5GAA Automotive Association. 2017. An assessment of LTE-V2X (PC5) and 802.11p direct communications technologies for improved road safety in the EU.

[3] CAR 2 CAR Communication Consortium. 2022. White paper on Additional Investigation of ITS-G5 and Sidelink LTE-V2X Co-Channel Coexistence Methods.

[4] 5GAA Automotive Association. 2016. The Case for Cellular V2X for Safety and Cooperative Driving.

[5] ETSI TR 121 914 V14.0.0 (2018-06). "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Release description; Release 14 (3GPP TR 21.914 version 14.0.0 Release 14)."

[6] C-Roads, 2023, C-ITS Security and Governance, Version 2.0.7

[7] JRC Technical Report, C-ITS Point of Contact (CPOC) Protocol in the EU C-ITS Security Credential Management System (EU CCMS), Release 3.0, January 2024. https://cpoc.jrc.ec.europa.eu/data/documents/e01941_CPOC_Protocol_v3.0_20240206.pdf

[8] JRC Technical Report, Security Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), EU C-ITS Security Policy, Release 3.0, September 2023. https://cpoc.jrc.ec.europa.eu/data/documents/e01941_C-ITS_Security_Policy_v3.0._20230916.pdf

[9] European Commission. 2018. Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Version 1.1. https://cpoc.jrc.ec.europa.eu/data/documents/c-its_certificate_policy-v1.1.pdf

[10] European Union,_DIRECTIVE (EU) 2023/1661 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 November 2023 amending Directive 2010/40/EU on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202302661

[11] I. Kotilainen, J. Scholliers, R. Öörni, R. Kulmala, Viranomaisten roolit vuorovaikutteisten älykkäiden liikennejärjestelmien (C-ITS) palveluiden käyttöönotossa ja operatiivisessa käytössä

[12] M. Masi, F. Paoletti, L. Malfatti, Reaching the L1 EU CCMS level: the experience of Autostrade Per L'Italia, 15th European Congress, Lisbon, Portugal, 22-24 May 2023

[13] Z. Wu, S. Bartoletti, V. Martinez, V. Todisco, A. Bazzi, Analysis of Co-Channel Coexistence Mitigation Methods Applied to IEEE 802.11p and 5G NR-V2X Sidelink, Sensors (Basel). 2023 Apr 27;23(9):4337. doi: 10.3390/s23094337.

[14] ETSI TR 103 766 v1.1.1 (2021-09) Intelligent Transport Systems (ITS); Pre-standardisation study on co-channel co-existence between IEEE- and 3GPP- based ITS technologies in the 5 855 MHz - 5 925 MHz frequency band

[15] Lu, Meng. (2019). Cooperative Intelligent Transport Systems: *Towards high-level automated driving*. The Institution of Engineering and Technology.

[16] 5GAA, Press Release: Automotive Giants at 5GAA Unite around the Future of Connected Mobility, 28 Sep. 2023, https://5gaa.org/automotive-giants-at-5gaa-unite-around-the-future-of-connected-mobility/#_ftn2

[17] C-Roads, 2023, C-ITS Roadside ITS-G5 System Profile, 2.0.7

[18] CROW, 2021, iVRI Interface RIS-FI, version 1.3.1. https://www.crow.nl/downloads/pdf/verkeer-en-vervoer/verkeersmanagement/landelijke-ivri-standaarden/d3047-4.aspx

[19] 5GAA, 2023, 5.9 GHz band configuration for road-ITS deployment in Europe

[20] ASECAP, 2023, ASECAP position on ITS spectrum: listen-before-talk & no spectrum split, October 2023

[21] ISO 27001 Standard, https://www.iso.org/standard/27001 last accessed 18.1.2024

[22] SME Guide on Information Security Controls, https://www.sbs-sme.eu/sites/default/files/SBS%20SME%20Guide_Information%20Security%20Controls.pdf last accessed 18 January 2024

[23] SME Guide for the Implementation of ISO/IEC 27001 On Information Security Management https://www.sbs-sme.eu/sites/default/files/publications/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management-min%20%281%29.pdf last accessed 18 January 2024 .

[24] Quectel, 2023, Quectel launches automotive grade 5G NR Release 16 modules to support autonomous driving, 28 February 2023, https://www.quectel.com/news-and-pr/automotive-grade-5g-nr-modules-ag59x

[25] ETSI GS MEC 030 v2.2.2.1 (2022-05) Multi-access Edge Computing (MEC); V2X Information Service API

[26] 5GAA (2023), Cross Working Group Work Item gMEC4AUTO, Moving towards federated MEC demos/trials (global MEC), https://5gaa.org/content/uploads/2023/04/5gaa-moving-toward-federated-mec-demos-trials.pdf

[27] Ricardo Energy & Environment. (2016). Study on the Deployment of C-ITS in Europe: Final Report (ED 60721 | Issue Number 1). DG MOVE. https://transport.ec.europa.eu/system/files/2016-10/2016-c-its-deployment-study-final-report.pdf

[28] S. Maaloul, H. Aniss, M. Kassab, M. Berbineau (2021). Classification of C-ITS Services in Vehicular Environments. IEEE Access, 2021, 9, pp 117868-117879. ff10.1109/ACCESS.2021.3105815ff. ffhal-03330673f

[29] ETSI TS 102 940 V2.1.1 (2021) Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2

[30] C-Roads (2024), Privacy in Probe Vehicle Data Collection, Working Document

[31] Volkswagen (2023), Information on the use of data when using V2X technology, https://consent.vwgroup.io/consent/v1/texts/CarNet/gb/en/dataprivacycar2x/latest/pdf

[32] CROW, 2023, Intelligent Traffic Light Controllers In Sustainable Urban Mobility Plans: *The role of Intelligent Traffic Light Controllers (iTLC) in Sustainable Urban Mobility Plans (SUMP).*

[33] L. Miao, J.J. Virtusio, K.L. Hua (2021) PC5-Based Cellular-V2X Evolution and Deployment, Sensors, 2021, 21, 843. https://doi.org/10.3390/s21030843

[34] 5GAA, 2021, Deployment band configuration for C-V2X at 5.9 GHz in Europe

[35] Directive 2022/2555. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32022L2555&qid=1709549841413

[36] CEPT, ECC decision (08)01. The harmonised use of Safety-Related Intelligent Transport Systems (ITS) in the 5875-5935 MHz frequency band, 18 November 2022

Appendix 1

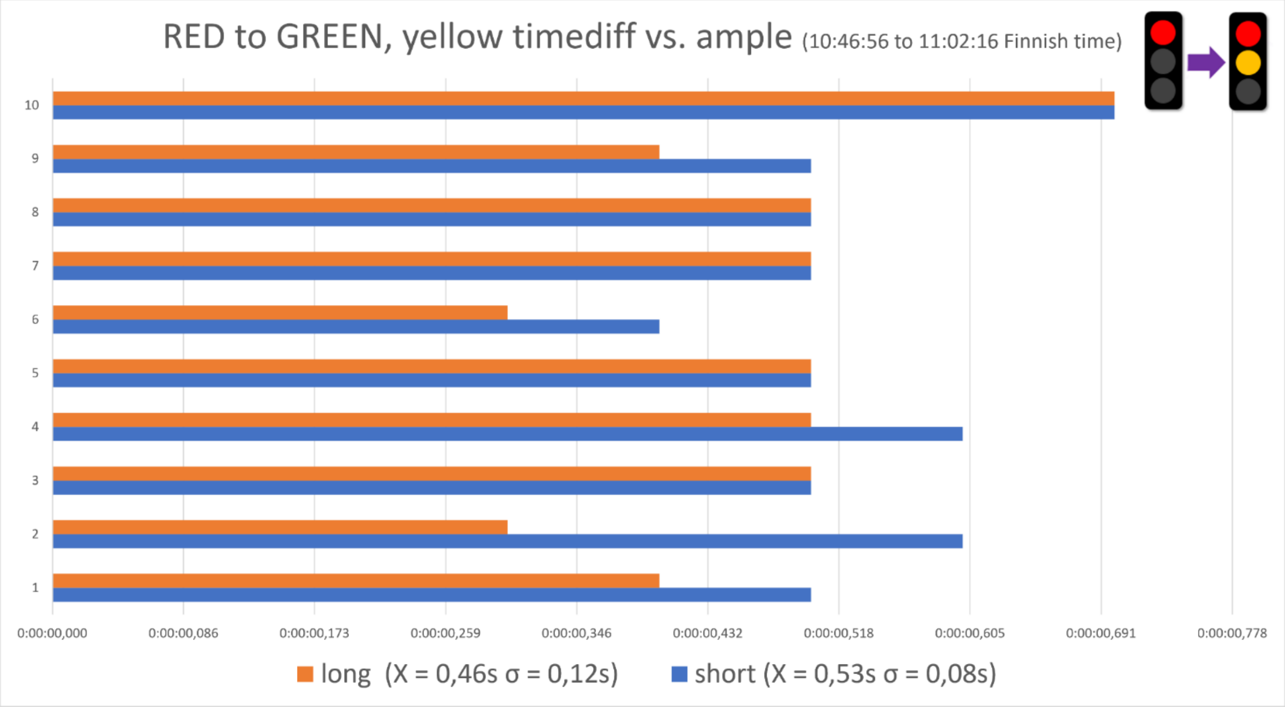

Figure 20. Long and short delays seen in UI compared to TLS, signal phase from red to yellow (R_Y), signed messages (N=10)

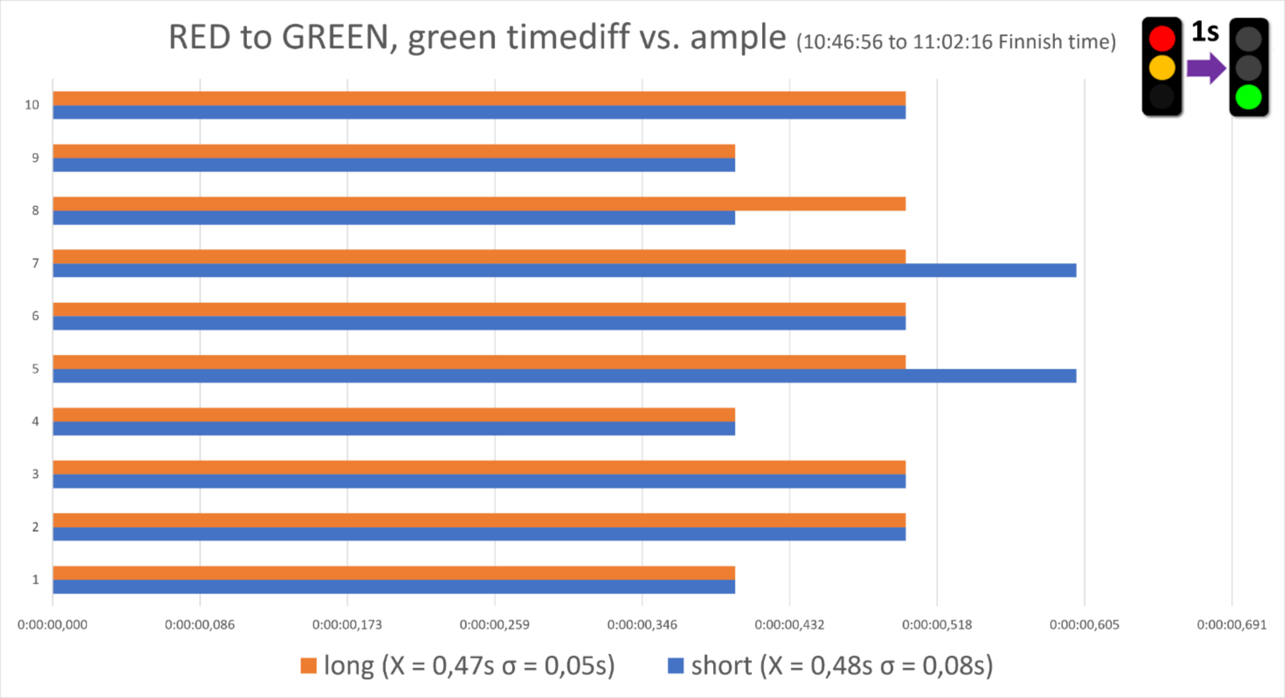

Figure 21. Long and short delays seen in UI compared to TLS, signal phase from yellow to green (Y_G), signed messages (N=10)

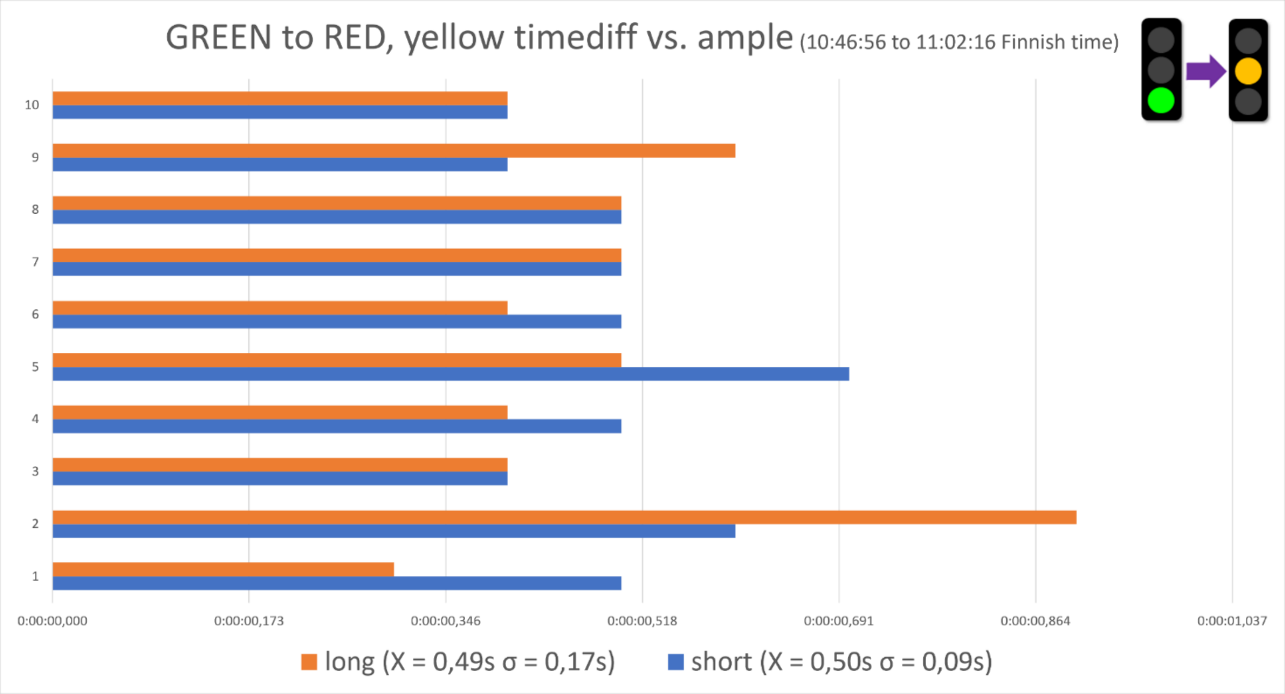

Figure 22. Long and short delays seen in UI compared to TLS, signal phase from green to yellow (G_Y), signed messages (N=10)

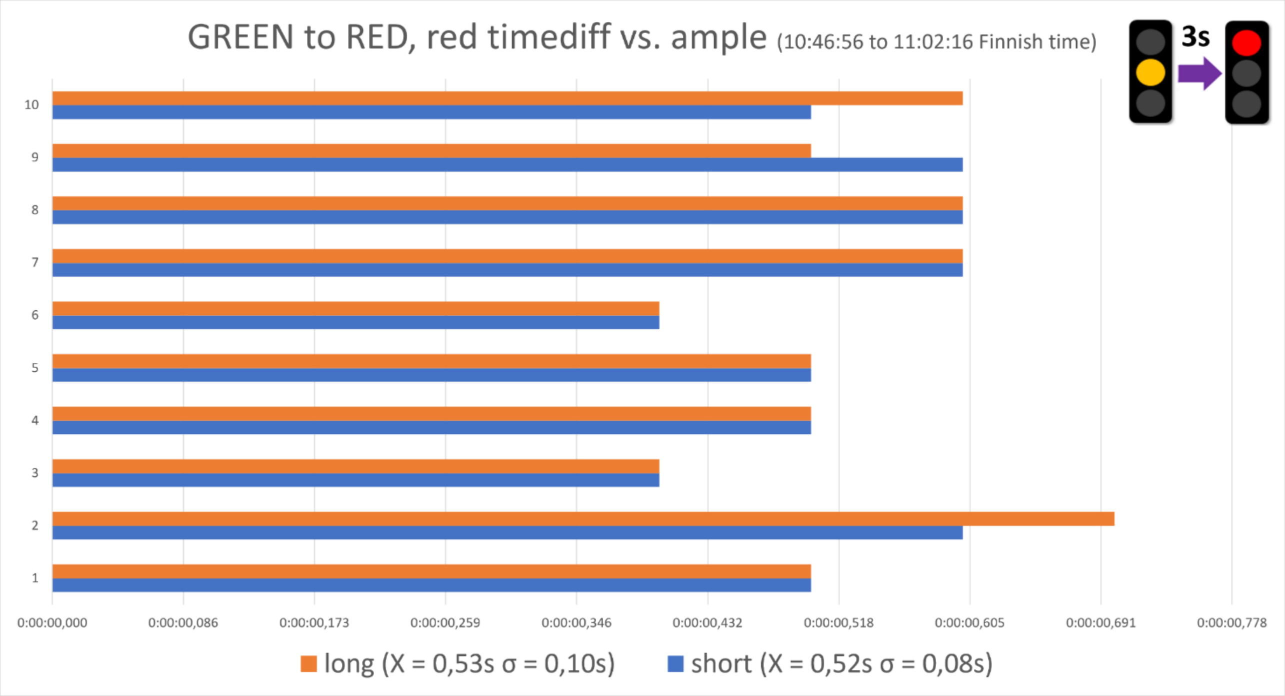

Figure 23. Long and short delays seen in UI compared to TLS, signal phase from yellow to red (Y_R), signed messages (N=10)

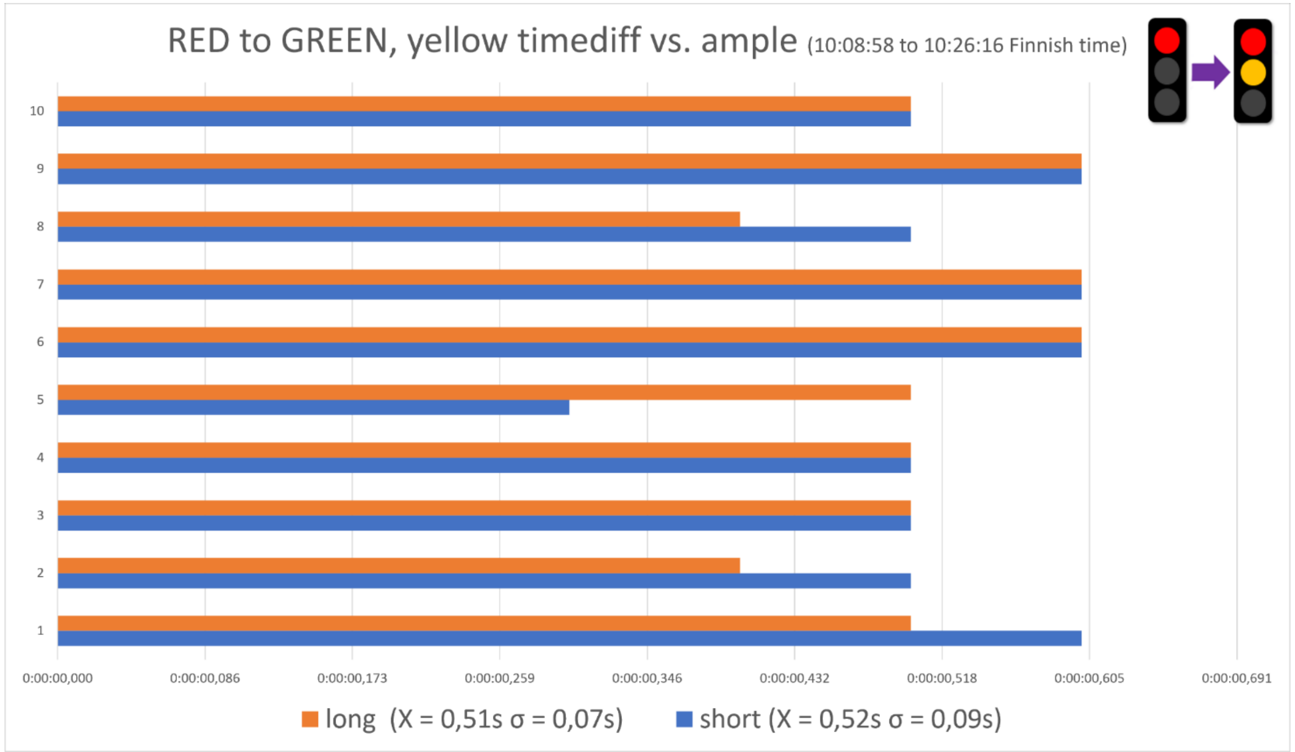

Figure 24. Long and short delays seen in UI compared to TLS, signal phase from red to yellow (R_Y), signing disabled (N=10)

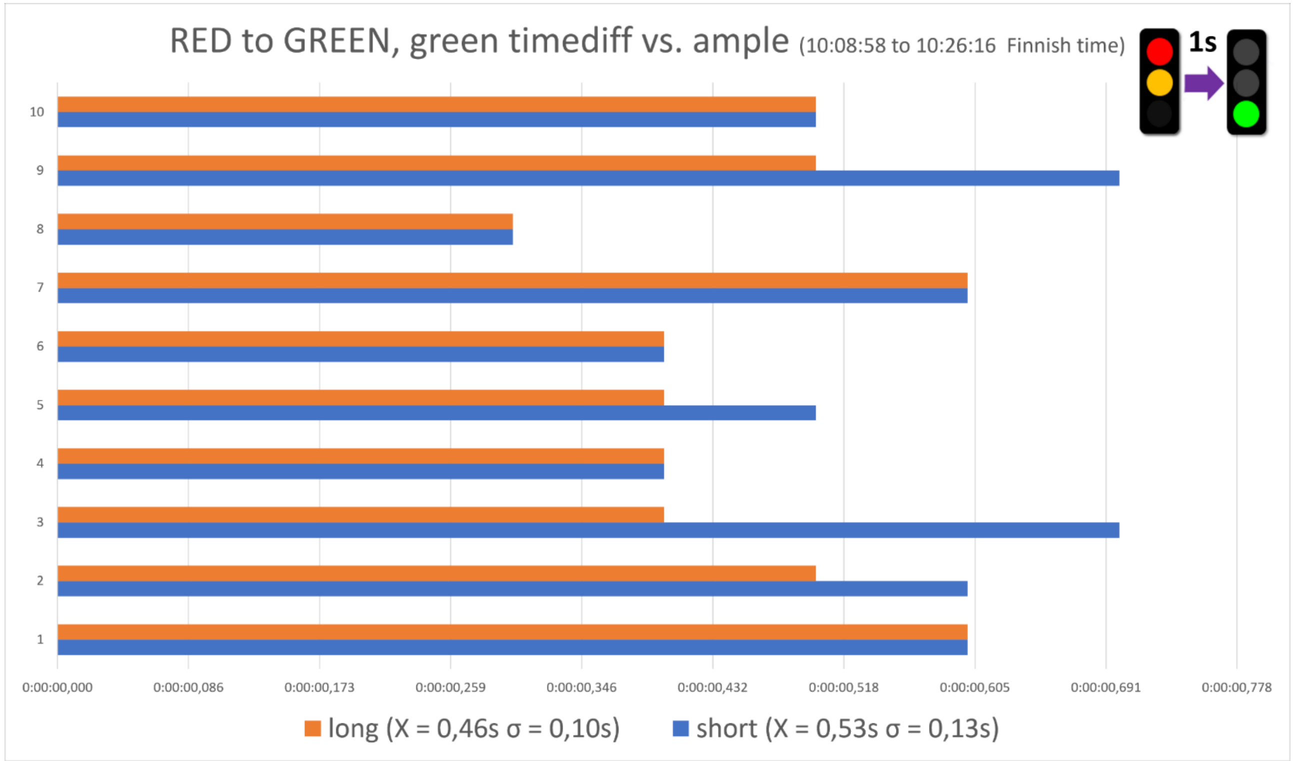

Figure 25. Long and short delays seen in UI compared to TLS, signal phase from yellow to green (Y_G), signing disabled (N=10)

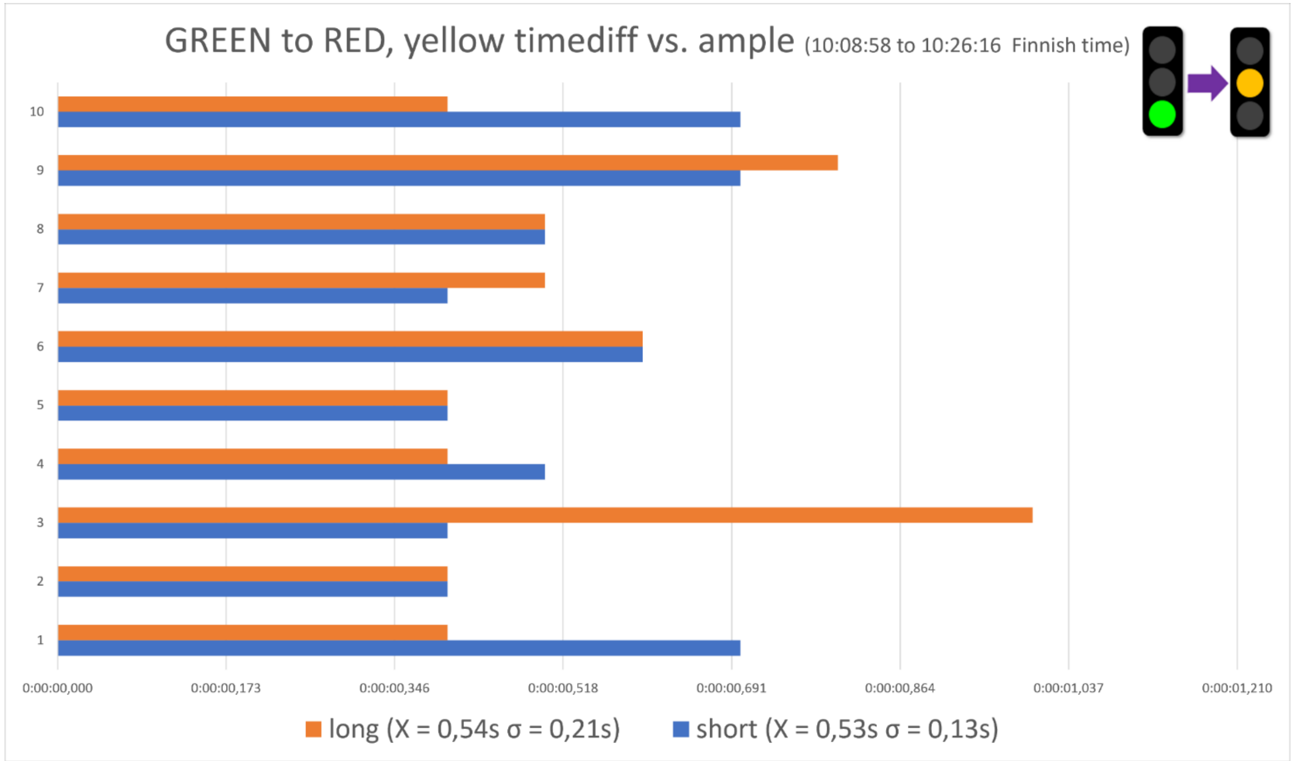

Figure 26. Long and short delays seen in UI compared to TLS, signal phase from green to yellow (G_Y), signing disabled (N=10)

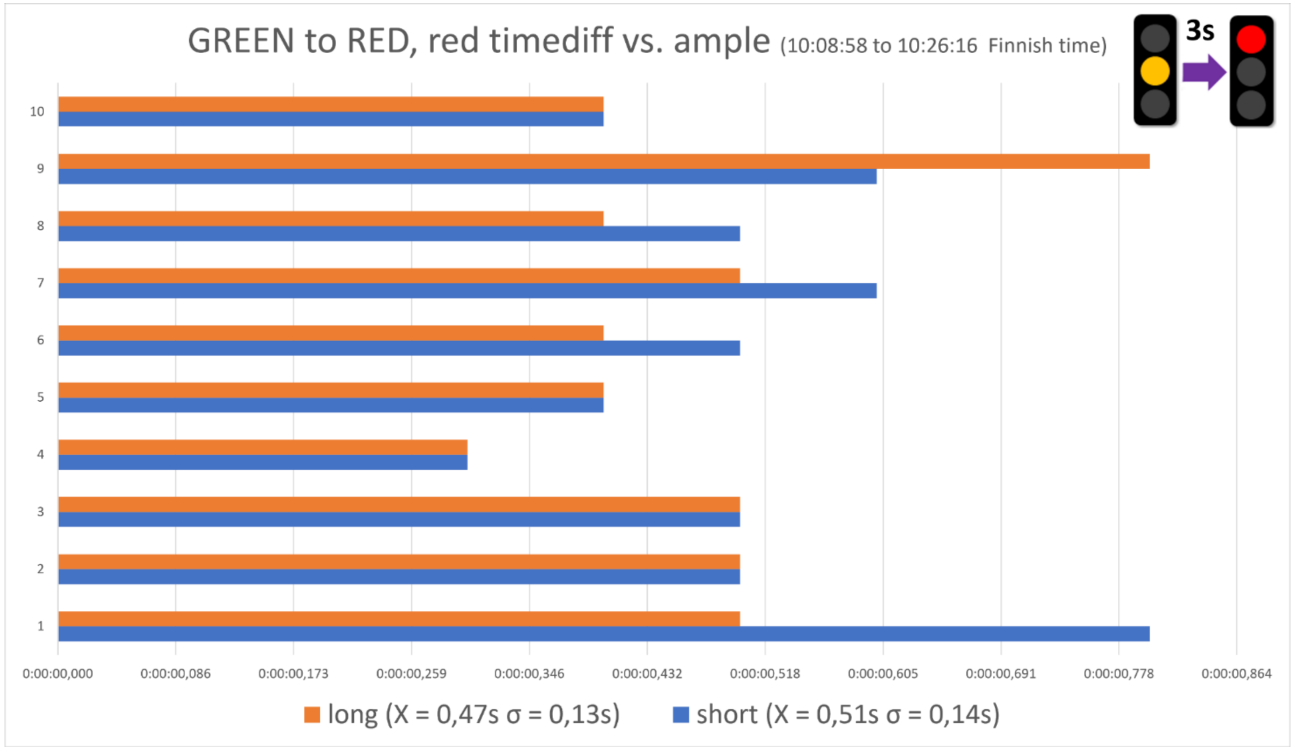

Figure 27. Long and short delays seen in UI compared to TLS, signal phase from yellow to red (Y_R), signing disabled (N=10)

Finnish Transport and Communications Agency Traficom
PO Box 320, FI-00059 TRAFICOM
Switchboard: +358 29 534 5000

traficom.fi

ISBN 000–000–000–000–0
ISSN 0000–0000 (e-publication)