Faculty of Fundamental Problems of Technology
Wrocław University of Science and Technology

ISMS
Policy

Team 3
Borek Mateusz
Budnik Michał
Chrząszcz Jakub
Czyszczonik Jakub
Drzazga Bartosz
Jachniak Mateusz
Tański Gabriel

Politechnika
Wrocławska
Wrocław 2020

Contents

1 Company Policy **1**
- 1.1 Corporate ISMS Policy . . . 1
  - 1.1.1 Purpose . . . 1
  - 1.1.2 Relevance . . . 1
  - 1.1.3 Goals . . . 1
  - 1.1.4 Objectives . . . 2
  - 1.1.5 Policies . . . 2
  - 1.1.6 Secure executive support . . . 2

2 Context establishment **3**
- 2.1 Study of the organization . . . 3
  - 2.1.1 Preamble . . . 3
  - 2.1.2 The organization's main purpose . . . 3
  - 2.1.3 The organization's business . . . 3
  - 2.1.4 The organization's mission . . . 3
  - 2.1.5 The organization's values . . . 3
  - 2.1.6 Structure of the organization . . . 4
  - 2.1.7 Service level agreements . . . 4
    - 2.1.7.1 Electronic dimension of the road . . . 4
    - 2.1.7.2 Commercial nodes . . . 5
    - 2.1.7.3 Emergency Vehicles . . . 5
    - 2.1.7.4 Electric Grid . . . 5
    - 2.1.7.5 Network Relays . . . 6
    - 2.1.7.6 Dynamic Road Signs . . . 6
    - 2.1.7.7 Road Weather Station . . . 6
  - 2.1.8 Organization chart . . . 7
  - 2.1.9 List of the constraints affecting the organization . . . 7
- 2.2 Basic criteria . . . 8
  - 2.2.1 Preamble . . . 8
  - 2.2.2 Risk evaluation criteria . . . 8
  - 2.2.3 Impact criteria . . . 8
  - 2.2.4 Risk acceptance criteria . . . 9

3 Risk Assessment **11**
- 3.1 Identification of assets . . . 11
  - 3.1.1 Critical infrastructure . . . 11
  - 3.1.2 Primary assets . . . 11
  - 3.1.3 Supporting assets . . . 11
- 3.2 Identification of threats . . . 11
  - 3.2.1 Availability . . . 11
    - 3.2.1.1 Blackhole and Greyhole attacks . . . 11
    - 3.2.1.2 Flooding attack . . . 12
    - 3.2.1.3 Jamming attack . . . 12
    - 3.2.1.4 Coalition and platooning attacks . . . 12
  - 3.2.2 Integrity . . . 12
    - 3.2.2.1 False messages attack . . . 13
    - 3.2.2.2 Replay attack . . . 13
    - 3.2.2.3 GPS spoofing attack . . . 13

3.2.3 Confidentiality and privacy . . . 13
3.2.3.1 Eavesdropping attack . . . 13
3.2.3.2 Location tracking . . . 14
3.2.4 Authenticity . . . 14
3.2.4.1 Certificate replication attack . . . 14
3.2.4.2 Sybil attack . . . 14
3.2.4.3 Masquerading attack or impersonation attack . . . 14
3.2.5 Non-repudiation . . . 14
3.3 Identification of vulnerabilities . . . 15
3.3.1 Vulnerabilities . . . 15
3.4 Identification of Existing Controls . . . 15
3.4.1 Preamble . . . 15
3.4.2 Availability . . . 15
3.4.2.1 Prevention . . . 15
3.4.2.2 Mitigation . . . 16
3.4.2.3 Recovery . . . 16
3.4.3 Integrity . . . 16
3.4.3.1 Prevention . . . 16
3.4.3.2 Mitigation . . . 17
3.4.3.3 Recovery . . . 17
3.4.4 Confidentiality and privacy . . . 17
3.4.4.1 Prevention . . . 17
3.4.4.2 Mitigation . . . 17
3.4.4.3 Recovery . . . 18
3.4.5 Authenticity . . . 18
3.4.5.1 Prevention . . . 18
3.4.5.2 Mitigation . . . 18
3.4.5.3 Recovery . . . 18
3.4.6 Non-repudiation . . . 18

4 Possible attack scenarios **19**
4.1 Analyzed scenarios . . . 19
4.2 Description of *Spike in communication latency* . . . 19
4.2.1 Introduction . . . 19
4.2.2 Identification of consequences . . . 19
4.2.3 Probability of incident . . . 19
4.2.4 Risk estimation and evaluation . . . 20
4.2.5 Risk treatment . . . 20
4.3 Description of *Message broadcast failure / event information not registered* . . . 21
4.3.1 Introduction . . . 21
4.3.2 Identification of consequences . . . 21
4.3.3 Probability of incident . . . 21
4.3.4 Risk estimation and evaluation . . . 21
4.3.5 Risk treatment . . . 21
4.4 Description of *Spoofing, false information injection, manipulation* . . . 22
4.4.1 Introduction . . . 22
4.4.2 Identification of consequences . . . 22
4.4.3 Probability of incident . . . 23
4.4.4 Risk estimation and evaluation . . . 23
4.4.5 Risk treatment . . . 23

5 Conclusion **25**

Literature **27**

A System Documentation **29**
A.1 Preamble . . . 29
A.2 V2X infrastructure . . . 29
A.2.1 Independent of the Company . . . 29

A.2.1.1 Vehicles . . . 29
A.2.1.2 Electronic dimension of the road . . . 29
A.2.1.3 Commercial nodes . . . 30
A.2.1.4 Electric grid . . . 30
A.2.1.5 Network Relays . . . 30
A.2.1.6 Dynamic road signs . . . 30
A.2.1.7 Emergency vehicles . . . 31
A.2.1.8 Road Weather Station (RWS) . . . 31
A.2.2 Dependent on the Company . . . 31
A.2.2.1 Central server . . . 31
A.2.2.2 Central authority . . . 33
A.3 Functionality provided by the infrastructure of V2X . . . 34
A.3.1 Collision/accident warning . . . 34
A.3.2 Roadworks warning . . . 34
A.3.3 Lane departure warning . . . 34
A.3.4 Approaching emergency vehicle warning/management . . . 34
A.3.5 Platooning . . . 35
A.3.6 Traffic rerouting . . . 35
A.3.7 User authentication . . . 35
A.4 Communication . . . 35
A.4.1 Classification of Intelligent Transportation Systems . . . 36
A.4.2 List of specific protocols and documents that specify the type of messages . . . 37
A.5 Network topology . . . 37
A.5.1 Management layer . . . 38

1 Company Policy

1.1 Corporate ISMS Policy

1.1.1 Purpose

The purpose of this policy is to protect from all threats the information assets of:

- The Company
- Its Customers

The objective of this policy is to ensure:

- Protection against unauthorized access to information
- Integrity of information, protection against unauthorized modifications
- Availability of information for authorized parties
- Business continuity
- Meeting regulatory requirements
- Evidence of due diligence
- Information security training for all employees
- Proper handling of all breaches and incidents
- Reporting, investigating, and patching suspected weaknesses

1.1.2 Relevance

All employees involved with any assets of information covered by the scope of the Information Security Management System are responsible for implementing this policy. Every action taken for this purpose shall have the support of Management, who have approved this document.

1.1.3 Goals

To identify the threats and vulnerabilities of information assets through risk assessment. To define risk acceptance levels and risk treatment plan through the establishment of policies and procedures, design, implementation and maintenance of an Information Security Management System, updating it continuously and verifying it every 2 years. To comply with standards, regulations and legislation, including:

- General Data Protection Regulation (2018)
- EU Cybersecurity Act
- ISO 27001-2005
- ETSI EN 302 637 (2014)

1.1.4 Objectives

To meet the requirements of the above standards, the ISMS focuses on the following components (described in the following chapters) divided into three categories:

1. Know-how
    - Policies
    - Processes
    - Procedures
    - Instructions
    - Inputs/outputs (document and information templates)
2. Education
    - Training
    - Guides
    - Tools
3. Organization
    - Roles
    - Contexts
    - Normative sources

1.1.5 Policies

Policies regarding Employees and HQ:

- Site access control policy
- Computer and password usage policy
- Data retention and backup policy
- Incident management policy

Policies relating to products and services:

- Network security policy
- Terminal security policy
- Security breach and incident management policy

1.1.6 Secure executive support

To secure the above aspects, it is necessary to define an ISMS and train employees in accordance therewith. To create such a secure system, full support from the management is required - that includes resources (like people, software and access to infrastructure) and budget for defining and maintaining the management system. Cooperation with government institutions should be established in case of lost personal data, in order to provide full security of all users.

2 Context establishment

2.1 Study of the organization

2.1.1 Preamble

This document was created for the purpose of outlining the responsibilities of the company, listing and describing the functional elements of the Vehicle-to-Everything (V2X) infrastructure, and analyzing possible threats and discussing threat mitigation. A relevant and valid security model is critical for providing service availability and safeguarding the privacy of the users, as well as preventing malicious parties from gaining unauthorized access to any protected information or manipulating the service. Furthermore, such a document serves as proof of due diligence and compliance with any relevant regulations, helping the Company avoid litigation in an event of a breach.

2.1.2 The organization's main purpose

- Prototyping, testing, and implementing infrastructure for V2X solutions based on 802.11p communication protocol.
- Evaluating the internals of the infrastructure against supplied documentation and real-life challenges.
- Evaluating documentation of the infrastructure against Security Targets.

2.1.3 The organization's business

- Development of solutions necessary for establishing a communication network between V2X participants - the infrastructure, network, grid, vehicles, pedestrians, and any supported devices.
- Providing necessary information and warnings, as well as directing the resources based on the current condition of the system.
- Maintaining and upgrading the infrastructure to meet the newest industry standards and ensure full data security.
- Ongoing upgrades to the system by utilizing collected data for the use of machine learning models.

2.1.4 The organization's mission

The mission is to ensure all users' safety and comfort by any security means possible in a V2X system. The users (clients) of this system are fully protected while using the service. The Company tries to analyze and find any insecurities before updates to the infrastructure are made. The Company also stays on top of the technological developments and advancements in order to continuously provide top-notch protection of its customers.

2.1.5 The organization's values

Providing full confidentiality of user data. Enabling the participants of the system to be notified of any noteworthy events, as well as optimize their travel times. Protecting the integrity of communication within the system.

2.1.6 Structure of the organization

The company is divided into 8 separate sections:

1. Research and development team - researches security solutions and develops the company's software.
2. Penetration testing team - attempts to gain unauthorized access to the V2X network and exposes security vulnerabilities within the solutions.
3. Software testing team - tests software, making sure that everything works as needed.
4. Customer and PR section - handles the procurement of new customers, takes care of the good image of the company.
5. HR and accounting section - handles accounting, human resources, recruitment.
6. Information Security and Infrastructure section - creates ISMS policies for the company and ensures compliance; overviews the company's IT systems.
7. Legal section - ensures compliance with the existing regulations, as well as handles the company's legal matters.
8. Guards and cleaning section.

2.1.7 Service level agreements

Services with our company are not directly responded to. The following services are outsourced for creating and maintaining these services with other companies with specific secure SLA. More detailed description you can find in chapter 3. The following service level agreement was written with the principles provided in Muhammad Raza's guide [3].

Agreement list:

- Electronic dimension of the road
- Commercial nodes
- Emergency vehicles
- Electric grid
- Network Relays
- Dynamic road signs
- Road Weather Station

2.1.7.1 Electronic dimension of the road

Responsibility:
Local Road authorities
Objectives:

- Maintain and service of the road and weather sensors.
- Monitoring and health checking services.
- Replacing and repairing broken sensors.
- Collecting data from data loggers to the V2X cloud server.
- Providing data from sensors to V2X users.
- Propagation data from V2X Cloud servers to V2X users.

Service:
Repair and replace broken sensors will be done in 1 working day.
Fixing data flow within 12h.
Availability agreements:
20 days in a year of inaccessibility of sensors.
6 days in a year of inaccessibility of data flow.

2.1.7.2 Commercial nodes

Responsibility:
Commercial nodes' owners (private property).
Objectives:

- Propagation data from V2X Cloud servers to V2X users.
- Providing commercial services for V2X users.
- Collecting data from V2X users to the V2X cloud server.

Service: Commercial services at least 10h per day.
Fixing data flow within 12h.
Availability agreements:
12 days in a year of inaccessibility of services during service time.
6 days in a year of inaccessibility of data flow.
Threat level: Low

2.1.7.3 Emergency Vehicles

Responsibility:
Owners of emergency vehicles
Objectives:

- Register new vehicles or renew a free licence for being a V2X user.
- Remove licence before transferring ownership or selling vehicles.

Service:
None
Availability agreements:
None
Threat level: Medium

2.1.7.4 Electric Grid

Responsibility:
Infrastructure maintainer in cooperation with energy suppliers.
Objectives:

- Charging stations for electric cars.
- Propagation data from V2X Cloud servers to V2X users.
- Collecting data from V2X users to the V2X cloud server.

Service:
Charging car services at least 12h per working day.
Charging car services at least 8h per holiday day
Fixing data flow within 12h.
Availability agreements:
15 days in a year of inaccessibility of services during service time.
6 days in a year of inaccessibility of data flow.
Threat level: Low

2.1.7.5 Network Relays

Responsibility:
Telecommunication companies.
Objectives:

- Propagation data from V2X Cloud servers to V2X users.
- Propagation V2X network in specified areas.

Service: Fixing data flow within 4h.
Fixing network propagation within 15 min.
Availability agreements:
2 days in a year of inaccessibility of data flow.
6 hours in a year of inaccessibility of the network in specified areas.
Threat level: High

2.1.7.6 Dynamic Road Signs

Responsibility:
Local road authority and their subcontractors.
Objectives:

- Informing clients about speed limits, road works, car accidents, future weather changes
- Road detours information
- Propagation data from V2X Cloud servers to V2X users.
- Providing commercial services for V2X users.
- Collecting data from V2X users to the V2X cloud server.

Service:
Information service 24h/7
Proposing road detour within 15 min after traffic jam detection or car accident detection.
Fixing data flow within 12h.
Availability agreements:
7 days in a year of inaccessibility of services during service time.
10 days in a year of inaccessibility of data flow.
Threat level: Medium

2.1.7.7 Road Weather Station

Responsibility:
Local road authority or institute of meteorology and water management.
Objectives:

- Localized notifying clients of current and expected future weather situation
- Mapping the current weather situation.
- Providing commercial services for V2X users.
- Collecting data from V2X users to the V2X cloud server.

Service:
Weather services 24h/7.
Fixing weather stations within 1 day.
Fixing data flow within 12h.
Availability agreements:

12 days in a year of inaccessibility of weather services during service time.
18 days in a year of inaccessibility of data flow.
Threat level: Low

2.1.8 Organization chart

The Company has one Chief Executive Officer, who together with team leaders create the organization management team. The whole organization is overlooked by the management team, and all the proposals have to be approved by it.
Some teams have a leader; leaders are responsible for different aspects of the company life:

- Chief Research and Development Officer - leader of the Research and Development team,
- Chief Security Officer - leader of Penetration testing and Software testing teams,
- Chief Information Technology Officer - leader of Information security and Infrastructure team,
- Chief Operating Officer - tends to the non-IT part of the company, for everything to run smoothly.

2.1.9 List of the constraints affecting the organization

The main constraint is the relatively small number of users at the moment, as V2X solutions based on the newest standards are still a developing field. That does not render the services useless, nor does it mean that no development in the infrastructure is done, but it limits the real-environment testing and leaves potential scalability issues unchecked. Furthermore, as this is a relatively uncharted field, it is difficult to lay out an exact road map and find the best people for the teams that handle V2X research and implementation.

List of the legislative and regulatory references applicable to the organization

- The General Data Protection Regulation (EU) 2016/679 (GDPR)
- The EU Cybersecurity Act
- ISO 27001-27005
- ETSI EN 302 637 (2014)

List of constraints affecting the scope

- Time constraints
- Budget constraints
- Regulatory constraints
- Contractual obligations

List of clients and cooperation parties

- Users of V2X, which has restricted access and law
- Local road authorities (for all countries)
- Owners of commercial nodes (e.g. gas stations)
- Telecommunication companies
- Local road authority or institute of meteorology and water management.
- Commercial authorities and fuel stations.

2.2 Basic criteria

2.2.1 Preamble

The following chapter concerns establishment of a methodology appropriate to assessing risks, their impact on the Company and accepted risk levels. A relevant and valid model of criteria is needed in order to enable systematical estimation of all risks and construction of treatment plans.

2.2.2 Risk evaluation criteria

Since this is a first iteration of company's ISMS and no historical incident data are available, the developed estimation methodology is qualitative. In order to comply with the ISO/IEC 27005 standard, the more general scale of qualifying attributes to describe the magnitude of potential consequences and the likelihood of occurrence is used. Quantitative estimation not based on historical data would create an illusion of accuracy of the risk assessment.

Both probability of risk emerging, and risk impact on the Company can be described with five categories. The categories with corresponding numerical values are as follows:

- Negligible (0)
- Low (1)
- Medium (2)
- High (3)
- Very High (4)

The summarized risk assessment is expressed as a sum of numerical values estimated for risk's impact and probability. The final risk evaluation criteria is assigned a qualitative category based on thresholds resulting from numerical values of calculated risk according to the table:

Total value (impact + probability)	Category
0	Negligible
1-2	Low
3-4	Medium
5-6	High
7-8	Very High

2.2.3 Impact criteria

Impact criteria are evaluated based on degree and costs of damage to the Company. If several of the following cases are applicable, then the risk impact is decided as a maximum.

- Impact of all risk is generally qualified based on fine/compensation amount relative to company's annual income:
  - below 0.5% as Negligible
  - between 0.5% and 1% as Low
  - between 1% and 3% as Medium
  - between 3% and 5% as High
  - above 5% as Very High
- Any risk resulting in fatal casualties shall be qualified as Very High.
- Impact of risk resulting in impaired operations, like:
  - loss of license/concession
  - detention of an employee

  but not only, are categorized as Very High.

- Breaches of contractual obligations are categorized at least as High as those are associated not only with financial losses to fines but also undermine the trust of partners.
- Failure to comply with whichever regulations qualifies at least as High.
- Damage of properties due to data corruption or unavailability is categorized at least as High as it causes not only financial loss but also undermines trust of partners and clients.
- Loss of clients' data or clients' data confidentiality shall be categorized at least as High considering it causes not only direct financial losses to fines but also seriously threatens the reputation of the Company.
- Disruption of plans and deadlines shall be assessed at least as Medium.
- Other, not listed cases shall be categorized accordingly, and to the best of knowledge. Less severe risk impacts can be qualified as Negligible, and Low.

Every effort has been made to ensure that evaluation is in accordance with all accepted standards.

2.2.4 Risk acceptance criteria

Generally no risk is preferred, should that prove to be infeasible then risk at the level Negligible is accepted. Risk at the level Low is also accepted if its impact is associated solely with financial loses.

In special cases, risk at the level of Medium can be accepted if there are plans set in place to minimize the risk to lower level that would become effective in under 6 months, and risk's impact does not threaten the reputation of the company.

3 Risk Assessment

3.1 Identification of assets

3.1.1 Critical infrastructure

The central server is a single point of failure within the entire infrastructure, and therefore it has to be adequately protected. The failure of other elements of the infrastructure may impede the functionality of the system locally or globally, but only the failure of the central server can disable all services provided by the infrastructure. In such a case, the top priority is to restore the availability of services. Fail-safe procedures allow for a swift restoration of service availability in case of a failure.

3.1.2 Primary assets

Asset analysis has yielded insight into the elements that are considered to be crucial to the Company and smooth operation of the infrastructure. One of the most important assets is the reputation of the Company, to ensure fruitful cooperation with partners and local authorities, as well as trust from customers. Another primary asset is the privacy of the users, which needs be protected by restricting access to sensitive information within the Company's possession. Trade secrets and future plans of the Company can be considered to be primary assets as well.

3.1.3 Supporting assets

Supporting assets are assets that enable the company to deliver the promised functionality. That includes hardware, which hosts and extends the network, the software responsible for appropriate operation, the personnel responsible for maintenance, and the partners that take care of various elements of the infrastructure.

3.2 Identification of threats

As a commonly available system, V2X contains a lot of threats and security concerns as [5], [16] and [9] mention. The following chapter contains a list of possible attacks, shortly described with a brief security recommendation and possible impact on the system. A detailed prevention strategy and a security specification policy are described in the subsection 3.4.

3.2.1 Availability

One can say that the system meets the criteria of availability when it is possible for an entity to send and receive messages in appropriate latency. For example, a forward collision warning message should be transmitted to an incoming vehicle before the vehicle arrives at the accident point. When the usability rate drops below some acceptable level the system becomes useless and dangerous for its participating entities.

3.2.1.1 Blackhole and Greyhole attacks

Description:
The compromised node stops relaying packets to the neighbouring nodes. Thus, it blocks up the spreading of information over the network. The attacker drops all packets that are received in blackhole attack, while drops some packets in the greyhole attack.

Possible attack scenario:
a compromised node drops the received packets and blocks the targeted edge node
General recommendation for prevention:
routing nodes authentication, warning packet broadcasting, eliminating single point of failure nodes
Threat origin:
decentralized characteristic of the V2X network
Impact: MEDIUM - the attacker can impact on the overall system availability, but it could be easily prevented

3.2.1.2 Flooding attack

Description:
The attacker sends a huge volume of packets to make a victim node unavailable.
Possible attack scenario:
To initiate the attack, the attacker may exploit the binary exponential back-off scheme. Among the competing nodes, the winning node captures the channel by sending data constantly. Thus, it causes a delay in transmitting data by forcing loaded neighbours to back off for a long time.
General recommendation for prevention:
an automated tool that removes authorization of compromised node
Threat origin:
P2P characteristic of the V2X network
Impact: HIGH - the attacker can impact on the overall system availability

3.2.1.3 Jamming attack

Description:
Jammers create direct interference to transmitted signals to impede their proper demodulation. Different types of jammers exist and can cause system degradation at different levels
Possible attack scenario:
the attacker broadcasts signals to corrupt the data or jam the channel
General recommendation for prevention:
directed signal
Threat origin:
P2P characteristic of the V2X network
Impact: HIGH - the attacker can impact on the overall system availability

3.2.1.4 Coalition and platooning attacks

Description:
A group of compromised nodes collaborate to initiate malicious activities such as blocking information or isolate legitimate vehicles
Possible attack scenario:
several internal attackers collaborate and initiate blackhole attack, that could affect the information delivery even with broadcast nature that it is supported by the IEEE802.11
General recommendation for prevention:
existence of independent and trusted nodes that are available everywhere
Threat origin:
P2P characteristic of the V2X network
Impact: MEDIUM - the attack scenario requires a high number of participants, but is hard to be prevented and mainly target a single entity

3.2.2 Integrity

The integrity in the context of the V2X system means that the data exchanged between participants is delivered intact and unchanged. Messages sent to or from an entity should be protected against unauthorized modification and deletion.

3.2.2.1 False messages attack

Description:
The compromised node spreads bogus messages in the network, by generating a new message or modifying the received one. In both cases, it misleads the vehicles by giving them wrong information and putting them in a dangerous situation.
Possible attack scenario:
in IEEE802.11p, it is possible that an internal attacker may try to broadcast false safety messages through the network
General recommendation for prevention:
automated attackers detection, certificate revocation lists, digital message signature
Threat origin:
V2X network scale
Impact: MEDIUM - the possible impact on the system correctness is high, but it is easily prevented

3.2.2.2 Replay attack

Description:
UEs that receive and decode messages from other UEs can replay them. This can cause congestion, (reactive) jamming, or confusion about inconsistent message content. One can imagine a network of distributed UEs that replay messages and cause congestion, confusion, or both in different areas.
Possible attack scenario:
a compromised node could capture the signal of an emergency vehicle and use it
General recommendation for prevention:
timestamp and a nonce in each message, short message lifetime in the network
Threat origin:
the amount of information processed by V2X nodes
Impact: LOW - easily prevented in modern cryptographic schemes

3.2.2.3 GPS spoofing attack

Description:
The compromised node sends messages with fake location or after a period of time. In general, GPS is responsible for delivering both location and time to the surrounding nodes.
Possible attack scenario:
the attackers can send fake location by generating a strong signal from a GPS satellite simulator
General recommendation for prevention:
plausibility checks to detect fake location and time
Threat origin:
geological location requirement for proper system working
Impact: MEDIUM - the attack scenario is not easy to perform, but is hard to be prevented

3.2.3 Confidentiality and privacy

One of the main concerns of systems that are commonly available is providing confidentiality and privacy of handled data. An entity that is willing to be a part of the V2X system wants to be assured that its personal data is secured and unavailable for unauthorized access. It means that it should not be possible for an unauthorized entity to reveal the messages between vehicles and vehicles and between vehicles and infrastructure. It should not be possible for an unauthorized entity to analyze the identification of a person through personally identifiable information such as location or driving route of a particular person within communication messages.

3.2.3.1 Eavesdropping attack

Description:
It aims to capture packet's information and acquire sensitive and confidential information
Possible attack scenario:
the internal attacker can collect information without permission from other users
General recommendation for prevention:
encryption of confidential messages

Threat origin:
ubiquity of the signals from interacting nodes
Impact: LOW - encryption is cheap and common

3.2.3.2 Location tracking

Description:
Sharing the location with neighbouring nodes is very important for various vehicular applications. As a result, attackers can collect and use this information for tracking users.
Possible attack scenario:
the attacker can safely follow a targeted entity
General recommendation for prevention:
short-term identifiers
Threat origin:
geological location requirement for proper system working
Impact: MEDIUM - the attack scenario requires targeting and affects a single entity

3.2.4 Authenticity

Ensuring authenticity includes the process of giving nodes access to the network based on their identity using certificates and digital signatures. It works like a wall that protects the network from external attacks.

3.2.4.1 Certificate replication attack

Description:
The compromised node uses replicated certificates to conceal itself by deleting the certificates that were added to the blacklist
General recommendation for prevention:
PKI usage
Threat origin:
node identification requirement
Impact: LOW - certification is easy to be controlled

3.2.4.2 Sybil attack

Description:
A single compromised node pretends many fake identities
General recommendation for prevention:
PKI usage
Threat origin:
node identification requirement
Impact: LOW - certification is easy to be controlled

3.2.4.3 Masquerading attack or impersonation attack

Description:
The attacker exploits a legitimate identity to obtain access to the network and confidential information.
Possible attack scenario:
phishing attack
General recommendation for prevention:
certificate revocation system
Threat origin:
human nature
Impact: MEDIUM - the human error could be exploited and the privileged entity could be impersonated

3.2.5 Non-repudiation

Description:
An entity is able to deny that it has already sent a message.

Possible attack scenario:
using a stolen identity
General recommendation for prevention:
digital signatures
Impact: MEDIUM - provides prevention from an authorized entity becoming a malicious node.

3.3 Identification of vulnerabilities

Preamble

In this section we will identify vulnerabilities in the Company, based on primary assets.

3.3.1 Vulnerabilities

- Unauthorized access to production environment by unauthorized employees. Failure to perform security screening of candidates who have been qualified for working with sensitive information. Reputation is among the most important assets of the Company, and so the employees are to be held to a high standard. Protecting the customers and their privacy is the Company's priority.
- Receiving fake information from another services, because in some cases the false data cannot be easily verified. Mutual trust with our partners very important for correctness and safety of services provided by the Company.
- Improper maintenance protocols for servers and databases. Restricting physical access to server rooms is crucial for providing security and privacy of sensitive data and uninterrupted availability of critical services.
- Unauthorized access to V2X network.
- Forgery of V2X network certificates.

3.4 Identification of Existing Controls

3.4.1 Preamble

This chapter details the means taken by the company aimed at reducing the likelihood of scenarios described in the chapter **Possible Threats**, as well as mitigating their negative effects, should prevention prove infeasible or impossible.

3.4.2 Availability

Proper control over the system availability is key for clients' satisfaction and trust in the whole infrastructure.

3.4.2.1 Prevention

Preventing attacks on the system's availability means making sure all the clients stay connected and informed throughout the use of the architecture. An especially disrupting scenario may happen when the network does not spread the information as desired due to infrastructural greyholes. If the system's information propagation relies, in any place, on a single node, it opens a threat for the whole network. To fight this potential weakness a few seemingly excessive solutions will be implemented:

1. Additional relays that overlap at least two other ones. This solution not only helps in mitigating a possible focused attack but also ensures the stability of the infrastructure in case of another relay failure. They also work like load balancers, helping with the prevention of flooding type attacks.

2. Authenticating of the nodes. Each relay has to be identified and authenticated in the network in order to make sure there are no rouge nodes in the system.
3. Trusted nodes put throughout the whole infrastructure. They work as backup relays in case of their loss. These nodes are additionally authorized and connected via Ethernet and are designed not only to propagate but also locally analyze all the incoming signals.
4. Secondary power sources put alongside the main electric grid.

All those solutions should make the probability of the loss of availability next to zero.

3.4.2.2 Mitigation

In big part, the mitigation is based on the same infrastructural parts as prevention does. It is not possible to block completely all attacks in their various forms, thus there needs to be an established plan on how to keep the services available despite having an intruder. The system implements a few techniques used to mitigate the possible attacks on availability:

1. Signalling of malfunctioning relays. Due to the nature of the network, each relay gets a confirmation message from its neighbours. That allows, for quick and accurate signalling of broken/lost units to the central server.
2. Presence of the trusted nodes. In case of an anomaly, they are the first to inform the central server, which takes appropriate actions in order to confirm the problem and resolve it. Additionally, they are used for secondary signalling, once a certain area is left without a signal.
3. Should there be a malfunctioning relay, their authorization will be immediately removed through a specifically designed automated tool. The recognition of a malfunctioning relay is possible through looking at which communicates were sent, and whether nodes do actually propagate the same information further.

With those solutions in place, the infrastructure is easily able to identify and cut off possible threats to the whole system, making sure no further loss of nodes and coverage will happen.

3.4.2.3 Recovery

Assuming the availability of the system has been compromised, the recovery steps need to be implemented in order to bring back the immunity of the infrastructure. The recovery mode heavily depends on the type of attack that caused the infrastructural issue. The company should arrange appropriate recovery based on the source:

1. In case of node poisoning or instability (causing it to lose some or all packets) the node needs to either be completely reset and reauthenticated, or in a worse scenario, replaced by a new node. The log and CCTV image screening may be of help to the local law enforcement institutions.
2. In case of flooding or jamming the signal, the company should use all the possible means to identify and stop the source of the attack. This includes, but is not limited to, triangulation of the signal, CCTV observation of the surrounding area, log and CCTV screening, the aid of the local law enforcement institutions.

3.4.3 Integrity

Data integrity in the context of V2X systems is absolutely necessary for the proper system functioning. Any violation of this may cause the spread of false information between users and, as a result, malfunctioning the system.

3.4.3.1 Prevention

Preventing this type of attack means that a trustworthy message will arrive in an unchanged form. To achieve this, the system should control the source's confidence and ensure that the message is not changed during transport. The second task can be achieved relatively easily with message encryption. To achieve the first task the system should detect and disable as soon as possible users impersonating privileged vehicles or broadcasting false events. It should be taken into account that an attacker may behave correctly for a certain period of time before the attack starts. In order to tackle these problems, a user credibility verification system should be implemented.

3.4.3.2 Mitigation

Message rating

When A sends a message M, to B, then B calculates the credibility of M to determine the trustworthiness of the message. Messages that report similar events are recorded in the message blockchain. Therefore, for every vehicle that reports similar events, the trust of the events is calculated and stored in a trust set. Next, the probability of such events, known as P(M), occurring is calculated using the trust set. If the P(M) is greater than the existing threshold, then M will be reported as true and B will generate a positive rating on the messages received from A, otherwise, M will be reported as false and B will generate a negative rating on that message. Then, B stores M in the message blockchain which will be then uploaded periodically to a nearby RSU.

Miner election and block generation

The miner is elected periodically. Each RSU in the network registers its timestamp and calculates the hash value. When the hash value is lower than the threshold and the sum of the absolute values of its trust offset is lower than the maximum sum of absolute values than the RSU is elected as the miner. The miner publishes its block into the blockchain and spreads data in the network.

3.4.3.3 Recovery

If a vehicle is found to have more negative ratings, the cert and public key of the vehicle will be revoked by the CAM (central authority management). Firstly, when the vehicle receives negative ratings exceeding the threshold (defined by CAM), the vehicle will be temporarily blocked from sharing data with other devices. Next, the CAM investigates the behaviour of the vehicle and decides whether the device should be fixed or rather permanently banned [4].

3.4.4 Confidentiality and privacy

3.4.4.1 Prevention

Confidentiality may mean a lot for some users of the system that are aware of their data access. Additionally, even for less conscious users, their privacy is of utmost importance for the company, as the inability of preventing personal data leaks may be a way to harm all the users indirectly. Thus the company has undertaken necessary steps to not only anonymize the communication between clients and other entities but also to make sure the information sent can not be accessed by unauthorized entities. Those steps include, but are not limited to:

1. Encryption of confidential messages. Not only makes that the personal information obscured for any potential attackers, but also helps in preventing indirect attacks (like GPS readings, etc.) The company implemented a strong encryption scheme, which is less susceptible to any possible methods of attacks.

2. Short-time identifiers. This solution is an additional layer of protection, which works in two ways. Firstly, no entity using the infrastructure is to be recognized by their identification, as it is changed every time the entity connects with the system, which allows for better anonymity. Secondly, the number of packets encrypted with the same data is much smaller, which minimizes any potential chances of breaking the encryption scheme.

3.4.4.2 Mitigation

No system is fully secure, and the company acknowledges that even a random chance may enable the attackers to access the encrypted data. The company implemented methods of securing messages and communications enable the whole infrastructure to mitigate any possible attacks due to a single intercepted message.

1. The entities in the messages are identified only via their short-time identifiers. No other personal and confidential information is sent in the messages, as this information is not necessary for the system's correct functioning and data analysis.

2. The steps described in the prevention subsection work together in a way that the whole scheme of communication can not be broken from intercepting and accessing the packet information. All the messages are encrypted with a few factors, and simply possessing the temporary, short-time identification key (decrypted from the message) does not reveal any of the other encryption elements.

3.4.4.3 Recovery

This is the most difficult step in attacking the confidentiality of the system, as in many cases it may not be possible to acknowledge the existence of such an attack. Though the company has taken some steps in order to prevent the whole system from being intercepted because of breaking the encryption scheme.

1. The main server analyses the correctness and uniqueness of the incoming messages, which allows the identification of unauthorized/impersonating messages. This also allows for monitoring any suspicious behaviour (massive inflows of requests, etc.) and quick shutoff of these entities.

2. In case a suspicious behaviour persists the company is ready to quickly exchange the pseudo-random generators responsible for the identifications. In case the whole encryption scheme was broken, the company has undertaken the necessary steps that allow the scheme to be easily exchanged for the whole system.

3.4.5 Authenticity

Authorization in P2P systems that also require anonymity of users is quite complicated and critically important.

3.4.5.1 Prevention

Preventing attacks involving unauthorized users requires a reliable way of user authorization, therefore each user should have its own certificate signed by a commonly trusted certificate authority (also known as Root CA). Due to the need for anonymity of users, it is necessary to introduce a mechanism of short-time-lived pseudonyms, which are also certificates, assigned to users by the central authority server. Pseudonyms should be used in communication between vehicles

3.4.5.2 Mitigation

The central authority server makes it possible to ensure that only eligible users have access to the system and also allows linking reported events with appropriate users, which may be helpful during an analysis of false events broadcast incidents. Short-time-lived pseudonyms additionally are useful for the implementation of an anonymous user credibility verification system.

3.4.5.3 Recovery

Because of: the need for continuous exchange of significant amounts of data between vehicles 2. The use of a mechanism of short-term pseudonyms the system should eliminate as soon as possible any users who are not trustworthy. Therefore the commonly used mechanism of announcing a list of revoked certificates (CRL) cannot be used in this case (too long propagation time). Instead, the system should use an OCSP server, which allows each user to check the status of the certificate for any other participant by a simple http request.

3.4.6 Non-repudiation

The company acknowledges the chances of this kind of attacks, however, after further analysis all the security steps described for other categories of attacks provide full coverage of possible disastrous scenarios of non-repudiation. All the attack scenarios are either based on the authenticity vulnerabilities or attacking the confidentiality and privacy of the users. Therefore, the company redirects to the aforementioned chapters for the specific measures implemented for the prevention, mitigation, and recovery of the system.

4 Possible attack scenarios

Preamble

In this section we will analyse possible attack scenarios. Following analyse will be used for identification of consequences and for risk estimation, evaluation and treatment.

4.1 Analyzed scenarios

Examples of possible attack scenarios:

1. Spike in communication latency
2. Message broadcast failure / event information not registered
3. Spoofing, false information injection, manipulation

4.2 Description of *Spike in communication latency*

4.2.1 Introduction

Spike in communication latency may be caused by numerous reasons:

- infrastructure fault
- radio interference
- spike in network bandwidth consumption

All of these causes might just occur naturally or be a malicious action of an adversary.
Let's take as an example a case where communication between two nearby vehicles is delayed due to radio interference. Incoming information that is received too late is incorrect and may cause unpredictable behaviours of vehicles, e.g. two cars may collide during lane change maneuver as a result of invalid position and velocity data.

4.2.2 Identification of consequences

The main consequence of significant latency in the communication between entities is an inability of the system to work effectively. The effect is serious in itself, but it also should be noted that if there are sudden delays in communication during an overtaking manoeuvre, the effect may be an accident in which someone loses their life, which actually is a critical case. As mentioned in 2.2.3 section the risk resulting in fatal casualties shall be qualified as *Very High* and so it was qualified.

4.2.3 Probability of incident

During the tests, it was diagnosed that significant communication issues occur when the latency exceeds 420ms. During laboratory tests, such a latency occurred only 3 times, affecting 0.005% of the traffic, however, the staging environment tests betrayed the issues described below, due to which the number of unacceptable delayed packets increased to 0.1%, which is a low but not negligible value. Extensive testing in the production environment is needed to improve the estimation. System logs are

analyzed after each incident in order to facilitate quicker recovery in the future. So far, the tests have determined the average latency to be 69ms.
Prevention steps described in 3.4.2 significantly reduce the risks relating to the infrastructure failure. The use of appropriate hardware for communication between system entities significantly reduces the risk of delays caused by radio interference or other physical issues. The use of load balancer and circuit breaker (described in 3.4.2) mechanisms deal with the problem of network infrastructure overload which improves the reliability of the system. It is worth noting at this point that the network load should change periodically, the central server should be able to predict, based on, e.g. the calendar, the time and location of a significant network load increase in advance, allowing the system parameters to be adjusted. However, a significant risk is the occurrence of a malicious action of an adversary. Due to the steps described in points 3.4.3 and 3.4.4 , attacks on the infrastructure are significantly hampered, due to the extensive CCTV system, interference in communication between entities is also unlikely. In conclusion, the probability of incident is qualified as *Low*, but not *Negligible*.

4.2.4 Risk estimation and evaluation

Due to the fact that the accident may have an impact on human life, risk estimation is *High*. Only cases with higher probability to occur, would be more important

4.2.5 Risk treatment

The risks related to significant latency in communication may be divided according to entities involved in the communication, namely: V2V and V2I.

V2I

A noticeable problem is slowing down or even making communication with central servers impossible. In the case of a central server, this is a non-critical issue, as only a part of the functionality will not be available to the user. It should not have a very negative impact on his opinion about the product. In the case of significant delays in communication with the central authority, the problem is much more serious as the lack of connection with the central authority makes it impossible to gain or renew access to the system, which in turn has a very negative impact on the customer satisfaction. In order to deal with these problems, the solutions described in section 3.4.2 should be applied. Such a solution seemingly increases costs through the need to create a quite complex solution and the need to maintain much more infrastructure, but can bring significant savings and benefits in the long term. Maintenance costs can be significantly reduced by initially investing more in the design of the auto-scalable infrastructure, i.e. such that adjusts the amount of resources used to the current load on the system. Such a decision will additionally benefit in a much easier development of the system at a later stage, as the system will be able to deal with the transmission of much larger volumes of data with a relatively small increase in infrastructure maintenance costs. This will additionally increase the reliability of the system due to the existence of additional server instances. Additionally, the application of the network monitoring system will allow earlier detection and troubleshoot of performance problems. The cost of such a subsystem is low due to the fact that the data is already collected on the central server, it is only necessary to process it properly and create mechanisms for responding on its basis, which is actually to development costs. The defense against malicious action of an adversary described in points 3.4.3 and 3.4.4 makes the system resistant to such attacks. Th adversary's actions could still consist of physical attacks on parts of the infrastructure, but the defence against such activities is a CCTV system.

V2V

Another possible cause of communication latency is interference caused by things around the road and vehicles. Designing devices facilitating communication between cars is a complicated task, and its solution requires the company to gain a lot of domain and technical knowledge in the field of low-level communication between entities as well as about things that are the environment surrounding the roads. The integration of this knowledge into the company would be associated with huge financial and time costs during the development and maintenance process of the resulting solutions. Additionally, it would create a significant risk of releasing critical bugs during the implementation of the subsystem. Therefore, the proposed solution is to employ a subcontractor having a ready-made solution that fits the needs of the system. His duties should be:

- delivery of system components

- maintenance of them
- guarantee of reliable communication between vehicles

The cost of purchasing the solution compared to developing it yourself is low, moreover the delivery time should also be much shorter. The risks that arise from this approach are the need to trust the subcontractor and be responsible for their mistakes. One other cause of connection latency issues are malicious actions of an adversary, who can deliberately cause communication delays at critical moments resulting in a tragic accident. The prevention of such attacks should be implementing solutions described in 3.4.5 and providing low-level keep-alive mechanisms by a subcontractor. The cost of their implementation and maintenance is significant due to the need to employ specialists, but it is a necessary investment to defend against such critical attacks. Additionally, a CCTV system may be used to identify and eliminate the adversary.

Outsourcing the low-level communication subsystem transfers the legal responsibility for critical spikes in communication latency to the subcontractor and reduces the probability of incident to negligible due to usage of well-tested solutions, but fatal accidents of system users still pose a serious risk to the reputation of the company, so the estimate can be reduced to *Medium*, which is acceptable level.

4.3 Description of *Message broadcast failure / event information not registered*

4.3.1 Introduction

It may happen that important message is not properly broadcasted to nearby devices or data about an important global event is not registered in the central database and relayed by the Central Server to other vehicles.
For example, information about roadworks or a traffic congestion is not registered properly by the Central Server and as a result the data is missing in process of calculating the fastest route for emergency vehicles, therefore a rescue vehicle may not arrive on time to the scene.

4.3.2 Identification of consequences

There may occur both *Very High* and *Medium* type of consequences. If this failure results in miscalculation of the emergency vehicles' routes the consequences may become a critical case, where people lives are at stake. For most users this failure is of *Medium* impact, as it may delay their travel or cause a non-critical gap in information impacting only the comfort of their travel. Therefore, the estimated cost of those consequences is equal to 3.

4.3.3 Probability of incident

Prevention steps described in 3.4.2 and 3.4.3 the risk of this failure to occur. However an incident is still possible and according to the adopted criteria the probability can not be set to *Negligible*. The value was calculated as *Low* instead, which gives it a score of 1.

4.3.4 Risk estimation and evaluation

Considering the consequences impact together with the probability of the incident, the risk estimation is of cost 4 which implies *Medium* impact of the incident. This failure does not result in long-term loses, and due to its low probability should not have a meaningful impact on the reputation of the company.

4.3.5 Risk treatment

First of all, it is important to understand the underlying reason for this incident. This kind of incident is most likely connected with some sort of availability or integrity issue, be it a malfunctioning relay, connectivity issues, server instability, or signal jamming. As described in sections 3.4.2 and 3.4.3, the first step in this situation is to locate the source of the problem. A few solutions were implemented for this, namely:

- signalling of malfunctioning relays (3.4.2.2),
- message rating (3.4.3.2),
- trusted nodes validating messages (3.4.2.2)
- central server log checking and security audit (performed by an external company)

Then, depending on the discovered underlying reason of the information absence, different action will be taken:

- if a node is malfunctioning, its authorisation is immediately withdrawn (3.4.2.2) and then the node is analysed and put back into use - either by resetting and re-authenticating the node, or by replacing it. (3.4.2.3)
- if the signal is being jammed, the company is to use all the possible means to identify the source of attack - by analysing the inconsistencies and location triangulation, as well as CCTV observation of potential attacks places (3.4.2.3)
- in case of central server malfunctioning, a further investigation is needed, and company's information security and infrastructure teams will become responsible for overlooking this. They may either be able to solve the problem themselves (by analysis of the data) or seek help from external organisations.

In the first two cases, additional step of informing and seeking help of local law enforcement institutions will be needed. They are required not only to deal with potential law violation, but are also able to provide further specialised investigation tools.

Moreover, if the information broadcast failure is registered at a time when the information is still valid, it is immediately re-transmitted over the affected parts of the network.

The company has reevaluated the possible scenarios of this type of incident. The risk has been changed from MEDIUM to HIGH due to a new factor and reconsideration of the existing analysis. First of all, the company has not considered possible weather and nature-related type of interference, which brings the possibility of the incident from LOW to MEDIUM, so the probability cost increases to 2. Additionally, considering the possible lose of life due to this kind of incident as a much more important factor, the consequences cost has been increased from HIGH to VERY HIGH, which brings its score to 4. Therefore, the total estimated risk of the incident is increased to HIGH at a total cost of 6. At this moment there is no possible way, to minimize a risk, but it is important to focus on it at next iteration of the scope.

4.4 Description of *Spoofing, false information injection, manipulation*

4.4.1 Introduction

Some users may try to abuse the V2X system by spoofing information and broadcasting false information, that could lead to specific behaviour of other users of the road. For example, a malicious user may try to appear as an emergency vehicle to clear the way for themselves, causing trouble for other drivers.

4.4.2 Identification of consequences

The consequences of those actions depend on the action itself, the intention of the attacker, as well as the actual execution of the attack. They vary from being low and causing minimal discomfort for other users (like manipulating weather data), through medium that may actually delay users' travel or cause minor accidents (like spoofing emergency vehicle information), to high that my put people lives at risk (for example sending misinformation about cars positions).

We can see that the consequences could be serious. However in most cases, the responsibility for an attack could be directly shifted to the attacker itself. The owner of a road is not responsible for an accident caused by some careless driver.

Considering everything the overall impact is estimated as *Medium* (3).

4.4.3 Probability of incident

The company acknowledges how impactful and broad the spectrum of vulnerabilities of this type is, but believes that steps described in sections 3.4.3, 3.4.4, and 3.4.5 altogether bring the possibility of this incident to minimum, which gives the estimation at *Low* level (1).

4.4.4 Risk estimation and evaluation

Due to the breadth of this vulnerability and possible life-threatening consequences the estimated risk is non-negligible. A singular successful attack may not have a huge impact on the company's reputation, but may lead to a chain of the infrastructure disruptions and therefore cause a domino effect over the whole system. The probability estimation along with impact evaluation yields a risk value at *Medium* level (4).

4.4.5 Risk treatment

The origin of the threat is highly related with an identity of individual entities. In order to be a part of the V2X system, a node has to be registered and authorised. For this reason a node which is a source of a transmission of a malicious message could be easily identified what makes the number of possible attackers negligible. The solutions provided in 3.4.5 provides a mechanism for node authentication.

A possible attacker could also capture a message which is correct only in particular moment and resend it to abuse the system. However adding a timestamp and a nonce in each message and assuming short message lifespan prevents the possible threat as described in 3.4.3.

Despite the fact that the probability of legitimate node to send malicious messages is negligible, there is a threat that one's identity could be stolen. The more privileged the node associated with stolen identity is the bigger the threat for the system. For that the company adapted the CRL system in order to cut-off the compromised node as fast as possible. However, it may take some time before the real owner of the identity reports the theft. For this reason, some automated malicious node detection has to be considered.

After further discussion about the identity theft problem, the company decided to buy and integrate a subsystem that automatically detects the anomaly in nodes communication, what transfers the legal responsibility for malicious activity of compromised nodes.

Adapted solutions reduced the overall risk level from *Medium* (4) to *Low* (2) (by decreasing the probability by 1 and reducing the impact by 1).

5 Conclusion

Together with a team of security engineers, we have developed an ISMS document to ensure the safety of users of the V2X infrastructure provided by our company to the end user. The main goals were to provide with services: availability, integrity, confidentiality, privacy and authenticity of information's. The entire document was created in accordance with the following standards: GPDR 2018, EU Cybersecurity Act, ISO 27001-2005, ETSI EN 302 637 (2014). At the beginning we establish the context of document. We specifies basic criteria such as : Risk evaluation criteria, Impact criteria and Risk evaluation criteria and risk acceptance criteria. We thoroughly analyzed the organization of company, business targets, organization flowchart and many others dependencies. We specified the service level agreements with can transfer some risks for another companies. Later we overviewed the information security risk assessment. We identified and estimate the risk and then we evaluate risk level. In next chapter we specified the risk treatment, we establish prevention and mitigation for various types of vulnerability. The threatened part was not obvious and known during the preparation of the document, so the threats discovered in the future will be analyzed in the next iterations. We create infrastructure that minimizes the effects of scenarios not provided for in the analysis. We will monitoring risk and infrastructure. We will do next iteration after 3 months of implementation the document to production. We will alarming infrastructure when risk rises over the acceptance level. The proposed solutions and implementations guarantee that at a low cost we are able to provide a safe product, without the risk of legal consequences or loss of company reputation. Next iteration is proposed to do after every 3 months. After 2 years of implementing system the inspection should be scheduled yearly.

Bibliography

[1] Magnetic tape backup best practices. https://www.nakivo.com/blog/magnetic-tape-backup-best-practices/.

[2] replication-and-sharding. https://www.awsthinkbox.com/blog/replication-and-sharding.

[3] Service Level Agreement (SLA) Examples and Template. https://www.bmc.com/blogs/sla-template-examples/.

[4] Y. J. S. T. J. A. Adnan Shahid Khan, Kuhanraj Balan. Secure trust-based blockchain architecture to prevent attacks in vanet. https://www.researchgate.net/publication/337263091_Secure_Trust-Based_Blockchain_Architecture_to_Prevent_Attacks_in_VANET, 2019.

[5] J. J. Aljawharah Alnasser, Hongjian Sunb. "cyber security challenges and solutions for v2x communications: A survey". https://doi.org/10.1016/j.comnet.2018.12.018, 2018.

[6] A. S. Dr. Gáspár Péter, Dr. Szalay Zsolt. Chapter 9. vehicle to infrastructure interaction (v2i). http://www.mogi.bme.hu/TAMOP/jarmurendszerek_iranyitasa_angol/math-ch09.html, 2016.

[7] A. S. Dr. Gáspár Péter, Dr. Szalay Zsolt. Ieee 802.11p (wave). http://www.mogi.bme.hu/TAMOP/jarmurendszerek_iranyitasa_angol/math-ch08.htmlch-8.2.1, 2016.

[8] C. C. A. M. G. S. Giovanni Nardini, Antonio Virdis. Cellular-v2x communications for platooning: Design and evaluation. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5981612/, 2018.

[9] S.-W. LEE. Tu-t sg17 work on its security –x.1373 and x.itssec-2. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201708/Documents/S2-Lee.pdf, 2017.

[10] I. K. Markus Mueck. Networking vehicles to everything: Evolving automotive solutions.

[11] I. . Z. K. . B. C. Pan, Jane Popa. Proactive vehicular traffic rerouting for lower travel time. vehicular technology. (2013). IEEE Transactions on. 62. 3551-3568. 10.1109/TVT.2013.2260422.

[12] T. Petrov. Emergency vehicles coordination using v2x communication. https://ec.europa.eu/transport/themes/research/challenge/projects/emergency-vehicles-coordination-using-v2x-communication

[13] P. C. Russ Fellows. Full-incremental-or-differential-how-to-choose-the-correct-backup-type. https://searchdatabackup.techtarget.com/feature/Full-incremental-or-differential-How-to-choose-the-correct-backup-type.

[14] T. e. a. Sukuvaara. "vehicular networking road weather information system tailored for arctic winter conditions.". IJCNIS 7 (2015).

[15] Sukuvaara-Mäenpää. v2x-weather. https://www.semanticscholar.org/paper/Vehicular-Networking-Road-Weather-Information-for-Sukuvaara-Mäenpää/8d3d3da17131592ac286cf7855a5bb1a8049a8ef.

[16] B. D. E. Vuk Marojevic Wireless@VT, V. T. B. Computer Engineering. C-v2x security requirements and procedures: Survey and research directions.

[17] F. B. Zabat, Stabile. The aerodynamic performance of platoons. ISSN 1055-1425.

A System Documentation

A.1 Preamble

This appendix provides the description of the System responsible for fulfilling the business responsibilities of the company. It lists the core components of the infrastructure, describes the functionalities provided thereby, outlines the exact method of communication used in the process, and, finally, introduces the management layer along with its responsibilities.

A.2 V2X infrastructure

A.2.1 Independent of the Company

A.2.1.1 Vehicles

Data collected:
movement metrics, road and weather condition
Goal;
safe and convenient travel/transportation of goods
Technologies:
sensors, 802.11p compatible communication devices, geolocation
Responsibility:
V2X users (private property)
Summary:
Vehicles are the most important part of a V2X network, as the name itself suggests. There are multiple kinds of vehicles that are able to participate in a V2X architecture - buses, trucks, passenger cars, motorcycles. They connect to the infrastructure using their onboard computers and send information such as their movement metrics or experienced road conditions. The infrastructure provides all the vehicles in its range with frequent reports based on data from its own sensors and the information supplied by the vehicles. Additionally, they can communicate with each other if need be, for example, to facilitate safer and quicker maneuvers. Important thing is to consider vehicles not controlled by computers.

A.2.1.2 Electronic dimension of the road

Data collected:
weight, in-road pressure, soil temperature,
Goal:
traffic prediction, load distribution
Technologies:
various sensors, LAN connectivity
Responsibility:
Local road authority.
Summary:
Weather and road traffic sensors are used within the automatic traffic control to warn the driver of adverse weather and road situations. Both sensors provide useful data that is transmitted to other components in the V2X system. Usage of those sensors in traffic control systems on motorways provides various important insights in the road situation - traffic jam prediction, load distribution, time to the end of travel

prediction and more. All the data is sent to a station data logger and then transferred to the main server.

A.2.1.3 Commercial nodes

Data collected:
vehicles data, infrastructure power consumption
Goal:
expanding infrastructure functionality
Technologies:
AC/DC conversion, monitoring, data relays
Responsibility:
Commercial nodes' owners (private Aproperty).
Summary:
Commercial nodes are devices that enable enterprises to provide various services to users of the V2X system. Other companies may offer their services, e. g.: Electronic Road Pricing (ERP) system parking lots travel guides, hotels, gas stations advertising A node of special meaning:

A.2.1.4 Electric grid

Data collected:
car states, electricity usage, infrastructure power consumption
Goal:
managing power supply, providing charging stations
Technologies:
AC/DC conversion, monitoring, data relays
Responsibility:
Infrastructure maintainer in cooperation with the energy supplier.
Summary:
Vehicle-to-Grid (V2G) technology enables electric vehicles to charge up, but also to monitor the internal car states. This is done by using a special type of charging station capable of AC/DC power conversion. The grid is the basis for providing energy to the whole system. The stations are also used to provide and monitor the internal electric situation of the infrastructure and to store and transmit information about the situation on the road.

A.2.1.5 Network Relays

Data collected:
N/A
Goal:
extending the reach of the network
Technologies:
802.11p antennas
Responsibility:
Telecommunication companies.
Summary:
Network relays extend the reach of the V2X network, covering the entire length of the road and enabling all the clients to communicate with the infrastructure. They have no other function in the architecture than propagating the communicates.

A.2.1.6 Dynamic road signs

Data collected:
None
Goal:
informing clients about speed limits, road works, car accidents, future weather changes, road detours; general propagation of infrastructure messages
Technologies:

802.11p
Responsibility:
Local road authority and their subcontractors.
Summary:
The main function of the dynamic road signs is informing and warning road users about future road conditions, temporary road signs, or other kinds of road events. Dynamic road signs support propagating infrastructure messages to the clients. The owner maintains the physical apparatus but allows us access to send relevant info.

A.2.1.7 Emergency vehicles

Data collected:
infrastructure data, other entities location, incidents info, weather data
Goal:
controlling traffic signals, dynamic decision making, partial autonomous car control, faster reaction time of non-privileged entities
Technologies:
sensors, 802.11p compatible communication devices, geolocation, authorization device
Responsibility:
Local authorities.
Summary:
Besides regular vehicles, there are special traffic participants which have additional privileges. These are called Emergency Vehicles or Privileged Vehicles, and their status directly results from the current law regulations. These mainly include vehicles related to life and property saving, security service vehicles, disaster recovery and government security. Might even be required by law The Polish law allows the driver of privileged vehicles not to comply with the traffic regulations, as well as road signs and signals, including traffic lights. This may lead to an increased risk of a road incident affecting other traffic participants.

A.2.1.8 Road Weather Station (RWS)

Data collected:
moisture and temperature, visibility, wind, present weather, soil and underground temperature profile
Goal:
mapping current weather situation, predicting incoming weather changes, localized notifying clients of current and expected future weather situation
Technologies:
LAN connectivity, various sensors, weather station data loggers.
Responsibility:
Local road authority or institute of meteorology and water management.
Summary:
Moisture and temperature, visibility, wind, present weather, soil and underground temperature profile are being measured with various sensors by each RWS. The data is then transferred to the weather station data logger, which sends it through LAN to the main server. Based on the accumulated messages from various weather stations the mappings for the whole road are gradually calculated and updated. This allows not only for notifying clients of the current road situation but also predicts, with some approximation, incoming weather changes. [15][14]

A.2.2 Dependent on the Company

A.2.2.1 Central server

Data collected:
infrastructure and client data
Goal:
analysis of the data, localizing and predicting various events, mapping and representing the data, overseeing the infrastructure
Technologies:
LAN connectivity, machine learning based analysis systems

Summary:
The central server has a vital role in the infrastructure supporting the V2X system. Its main goal is to collect, analyze, and relay data in order to ensure cooperation and increased security of the traffic system. Central server has central control over all road entities, traffic and roads. Server stores and relays global events' messages, like:

- road construction
- traffic congestion
- emergency vehicles requests

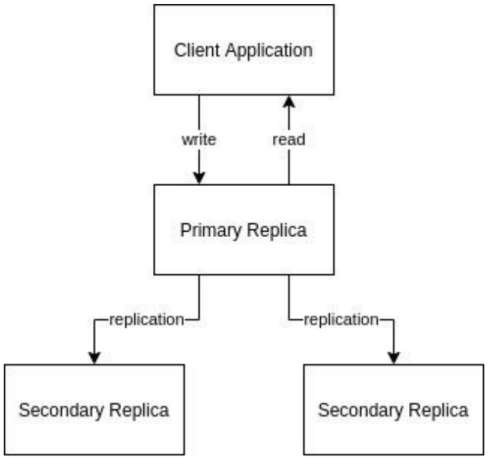
The server is responsible for collecting the traffic information from remote devices and analysis of all collected data:

- vehicles' movement data
- weather conditions
- road capacity
- traffic obstructions

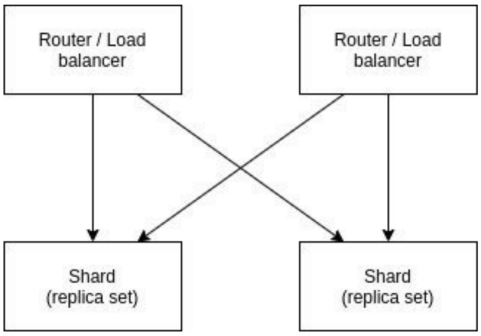
Analysis results are sent to vehicles for future use, e.g. route planning, speed adjustment in order to keep smooth traffic flow, etc. [5]

Increased security is achieved by providing a better overview and understanding of the surrounding area to the clients. Additional data from sensors located in the infrastructure and other vehicles helps to detect potential problems and obstacles that the driver or onboard sensors could overlook due to complex driving environments, distractions, or bad weather conditions.

The central server is responsible for the distribution of V2X messages to different target areas, connecting local groups of devices into the global system.
All data collected for functional, and regulatory purposes is stored in a database managed by the central server. To achieve the goals of data integrity and availability there are implemented rules of backups and database architecture resistant to failures.
Database architecture is based on replication and sharding. Replication refers to a database setup in which several copies of the same dataset are hosted on separate machines. The main reason to have replication is redundancy. If a single database host machine goes down, recovery is quick since one of the other machines hosting a replica of the same database can take over. A quick fail-over to a secondary machine minimizes downtime, and keeping an active copy of the database acts as a backup to minimize loss of data.



For a huge system scaling becomes a key performance issue and challenge in data availability. Sharding is a strategy that can mitigate this by distributing the database data across multiple machines. It is



essentially a way to perform load balancing by routing operations to different database servers.

Systems' database consists of multiple shard clusters, each built as a set of multiple replicas. This architecture allows for fast, and efficient scaling, introduces redundancy for better data availability, and integrity along with fault-tolerance, and high availability (infrastructure is operational even if some machines are down) [2].

Apart from database architecture oriented towards data availability, the Company introduced backup rules which are based on common best practices like [1] and [13]:

- Incremental backups (since last full backup) executed 4 times a day
- Full backup once a week
- Full backup on magnetic tapes once a month

The Company's database architecture and backup strategy enable continuous data protection and instant recovery, while the magnetic tape archive allows long-term data retention which is critical for ensuring the safety of passengers through enforcing the law.
The Central Server itself is using a cloud infrastructure operated solely by the Company. The V2X services are served by multiple nodes (replicas) running in numerous geographical locations. The cloud is using similar architectural solutions as the database to ensure fault-tolerance and high availability .

A.2.2.2 Central authority

Data collected
infrastructure and client certificates **Goal:**
system access control and short-time-lived pseudonyms system
Technologies:
PKI

Summary: System access control for V2X is crucial due to the relatively small amount of malicious users needed for a Sybil-like attack. Moreover, the anonymity of the cross-user communication is also important in this system, therefore users should not authenticate each other with their main certificates but should use their short-term pseudonyms. The following subsystems are required for that task:

- Certificate authority - validates the identities of vehicles or infrastructure entities and bind them to cryptographic keys through the digital certificates known as the main certificates
- Pseudonyms provider - validates the main certificate of an entity with the aid of OCSP and assigns him a short-term pseudonym (is also responsible for renewal)
- OCSP - provides a restful API, knows the lists of correct and revoked certificates. Based on these lists, it returns the status of the given certificate

A.3 Functionality provided by the infrastructure of V2X

A.3.1 Collision/accident warning

Infrastructure required:
vehicles, central server, sensors
Necessary data:
incident reports, location data (vehicles)
Description:
The central server analyses the data obtained from vehicles and cross-references it with reports from the sensors belonging to the infrastructure. If there is an obstacle ahead, the vehicles approaching said obstacle are notified in advance, so that there is no congestion at the site. The goal is to prevent pile-ups or avoidable congestions. Additionally, emergency services may be called and the path to the site can be cleared as needed.

A.3.2 Roadworks warning

Infrastructure required:
vehicles, central server, network relays, integration with public authorities and road operators
Necessary data:
vehicle movement information (speed, acceleration, position, etc.), road constructions information
Description:
By cooperating with public authorities and road operators it is possible to provide real-time warnings concerning roadworks. The data allows better route planning, more pleasant trip experience, as well as time and energy savings. Local roadworks efforts, closed roads and similar changes may occur at any time. Central server is therefore responsible for collecting vehicle movement data and its analysis data in order to detect anomalous traffic flow. Any abnormality shall be properly classified and relayed to clients [10].

A.3.3 Lane departure warning

Infrastructure required:
vehicles
Necessary data:
vehicle movement information (speed, acceleration, position), video sensors, laser sensors
Description:
The unpredictability of human behaviour and traffic dynamic characteristics are one of the main sources of dangerous road situations. Some of the incidents could be avoided by enhancing vehicles with a warning system. The proposed solution could share the position of a vehicle relative to the line with other road users or even make predictions based on actions taken by a traffic participant. The proposed solution works only for a group of nearby entities and includes the following signals exchanged by interested parties: a participant is changing a lane a participant is willing to change a lane by using a turn signal or taking any other action preceding a lane change The lane definition could be extended to include the line formed by the vehicles' position. Sources: None

A.3.4 Approaching emergency vehicle warning/management

Infrastructure required:
vehicles, central server, network relays, integration with eCall system
Necessary data:
vehicle movement information (speed, acceleration, position, etc.), road constructions, traffic congestions, weather conditions, accident details (location, time, etc.)
Description:
By providing relevant information combined from multiple databases to the vehicles, the idea has a potential to allow faster reaction time and safer transit for rescue vehicles. Emergency vehicles are enabled to broadcast emergency messages to all surrounding infrastructure (V2V, V2I) in order to clean the road. Central server's role is to use all data and resources to ensure smooth movement for emergency vehicles, including: notification for all users about approaching emergency vehicle rerouting traffic fastest route directions for emergency vehicles [5][12].

A.3.5 Platooning

Infrastructure required:
vehicles, central server (overlooking)
Necessary data:
vehicle movement information (speed, acceleration, position, etc.), road conditions/events data
Description:
Platooning enables groups of autonomic or semi-autonomous vehicles to travel together. The benefits of platooning include: Saving fuel and reducing emissions [source1] Reducing congestions Shortening commute times The reason behind reduced fuel consumption and emissions is the possibility of reducing drag for non-leading cars by up to 50 [source2]. Additionally, this method increases the safety on the roads, as the response time of a computer vastly surpasses the one of the driver. With an optional assist from the infrastructure, the entire platoon might be notified about accidents or unfavourable conditions in the blink of an eye [8][17].

A.3.6 Traffic rerouting

Infrastructure required:
vehicles, central server,
Necessary data:
vehicle movement information (speed, acceleration, position), road conditions(road works), emergency events, video cameras
Description:
Traffic flow can be blocked by road works, car accidents or another road event that can slow down the flow. The main solution for preventing traffic jams is informing cars about events on the road and proposing alternative roads that can save travelling time. The main goal of this functionality is rerouting traffic from blocked roads to alternative open roads. A big advantage of this solution is that vehicles are routed to few alternative roads for optimal traffic flow. Flow is monitored and traffic load is balanced between alternative paths [11].

A.3.7 User authentication

Infrastructure required:
vehicles, central authority,
Necessary data:
users and providers certificates
Description:
The system, on which reliability human life depends, must take care of authoristion of all components of the system. With the growth of the system, granting permissions to all new entities can be very troublesome, so it is reasonable to introduce trusted providers whose can grant and verify permissions to new devices by themselves. Due to the hierarchy in the relationship between the entities of the system, it is natural to use an central authority server responsible for controlling access to the system. Access control is based on PKI due to the need to control devices (or their suppliers) that are part of the system. Additionally, due to the need to V2V anonymous communication, a subsystem of short-term pseudonyms was introduced.

A.4 Communication

In a vehicular network, all road entities are supposed to generate and exchange messages. The messages are used to support a variety of functions, e.g. applications related to safety, traffic and infotainment. The messages are categorized into four types as [5] propose:

1. **Periodic message**: Road entities periodically broadcast status messages, which contain information such as speed, location and direction, to the neighbouring entities. These are generated at regular intervals between 100ms to 1s. As a result, each entity can perceive the local topology. Additionally, they can predict and anticipate dangerous situations or traffic congestions. This type of message is not time-critical (300ms).

2. **Local event-triggered message**: Road entities send this message when a local event is detected - such as critical warnings or intersection assist. This communication is sent to neighbouring entities as it contains useful information for neighbourhood areas only. This is a time-critical message which requires to be delivered with low latency, at around 100ms.

3. **Global event-triggered message**: Road entities send this type of message when a global event is detected - such as road construction or road congestion. This message needs to be propagated over a wider area and is not time-critical.

4. **Emergency vehicle message**: Is used to support a smooth and clear movement for emergency vehicles. It is sent by those privileged vehicles to the surrounding clients to clear the road.

As a result of the technological improvements in the areas of sensing and wireless networking, intelligent transportation system allows various applications that are related to safety, traffic, and infotainment:

- Safety-related applications use wireless communication between surrounding entities to decrease the accident rate and protect the commuters from dangers. Each road entity periodically sends safety messages to its neighbours to report its current status. Furthermore, they may also need to transmit warning messages when a local or global event is detected.

- Traffic-related applications are deployed to manage the traffic efficiently and ensure smooth traffic flow. They should collect the traffic information and transmit them wirelessly to a remote server for analysis. After that, the analysis results are sent to vehicles for future usage.

- Infotainment-related applications aim at improving the driving experience by supporting various services such as Internet access, online gaming, video streaming, weather information, etc.

A.4.1 Classification of Intelligent Transportation Systems

Various communication security methods are desired for intelligent transportation systems. These are based on a paper [16] and can generally be classified as:

- **Identification** and **authenticity** of the user to enable authorized access to services or information, as well as authorized provisioning of services or information,

- **Integrity of messages** to ensure that the information is accurate and can be trusted,

- **Availability** of the service or information,

- **Confidentiality** and **privacy of users** and their data to prevent eavesdropping and exploitation,

- **Non-repudiation** and accountability of the source.

In V2X, users broadcast messages and have to be authorized to do so. The data and control signalling they broadcast need to be legitimate and accurate. Privacy is important to avoid tracking of users and exploits, among others.
Messages that V2X users equipment exchange are related to information about vehicle speeds, directions, and other actions, such as breaking or accelerating. Such data are transferred via basic safety messages **(BSM)**. BSMs, introduced by the Society of Automotive Engineers (SAE), support all safety-related V2X standards. These messages are regularly broadcast, usually at a rate of 10 Hz. Event-triggered messages inform about sudden or unexpected events, such as accidents. The messages that are transmitted from one vehicle will thus affect the operation of other vehicles in the area. If a user's equipment transmits false information, other users' equipment receiving it may trigger actions, which, instead of optimizing the vehicular traffic flow on roads and highways, may cause chaos. For instance, if a user's equipment warns of an accident that does not exist, the approaching vehicles may slow down creating congestion. When this happens on a recurring basis, the level of trust will decrease and future messages may be ignored, defeating the purpose of V2X as a technology to increase traffic safety, resource efficiency, and system performance. It is therefore paramount that messages can be trusted. Since they are transmitted over the air and heard by many, source and message authenticity mechanisms need to be enforced.
Availability capacity is a key metric in wireless communications for V2X. Different techniques exist to increase the capacity, but irrespective of these, adding more users increases interference and stress to the network because of the limited resources. If dummy users create service requests or participate in broadcasting dummy messages, the RF spectrum will become more congested and the V2X service

less reliable, compromising the availability of information. As shown in other communication contexts, including LTE, radiating in RF bands where V2X services are provided can make the proper decoding of messages challenging, if not impossible. Mechanisms that allow recovering corrupted or lost messages, usually by means of strong coding and retransmission, add to the RF congestion, increase latency and power consumption, among others.
Confidentiality and **privacy**. The identities, position, actions and trajectories of users' equipment need to be secured to avoid tracking of vehicles. If messages from users' equipment are replayed at different times or at different locations, the immediate effect will be RF congestion, but additionally, it will cause confusion if two messages from the same source are received with inconsistent information. Jamming the regular transmissions from a single vehicular user's equipment is also possible, even without message decoding. In dynamic vehicular environments, confusion about vehicle location, speed, etc. can be created through delayed message replay without modifying the message content.
Non-repudiation and **accountability**. Malfunctioning user's equipment can significantly compromise system performance. For example, a user's equipment is not allowed to transmit if it stops receiving the LTE time advancement commands. Similar mechanisms are needed for V2X communication schemes. In V2X user equipment rely mostly on GPS as the synchronization source but can use infrastructure nodes, where available, or even other user's equipment. If no external sources exist, depending on the type and quality of oscillators, frequency and timing drifts will occur that add up over time and can cause system malfunctioning and significant interference. Harmful nonsynchronous transmissions need to be identified and malfunctioning user's equipment has to be identified and held accountable for the messages.

A.4.2 List of specific protocols and documents that specify the type of messages

- IEEE802.11p,
- LTE-V2X,
- 3GPP, "Service requirements for V2X services - Stage 1 (Release 14)"

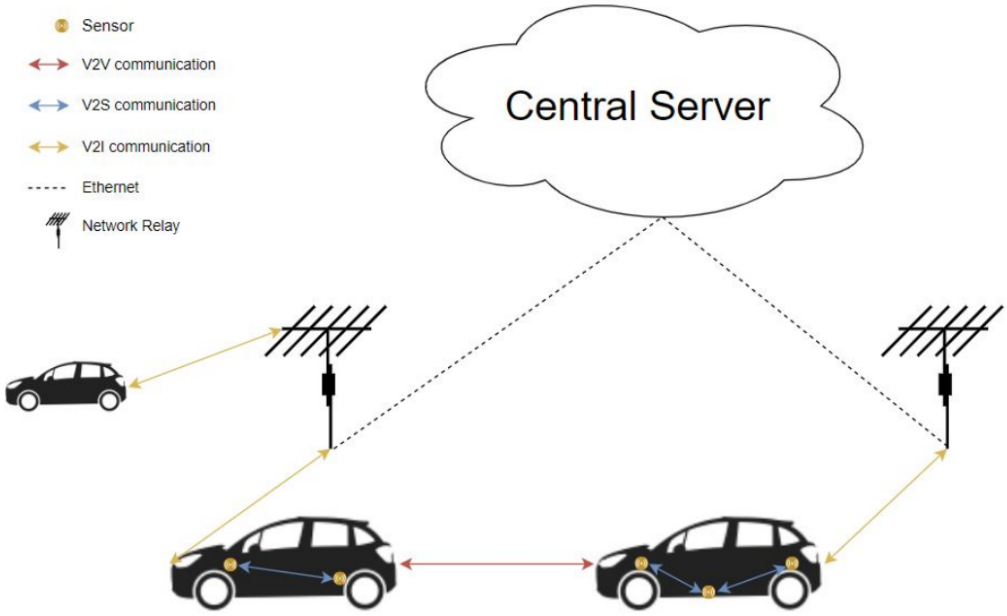
A.5 Network topology

The Intelligent Transportation System (ITS) applies data processing, communication, and sensor technologies to vehicles and infrastructure units to increase the safety and efficiency of the transportation system. To achieve this goal every element of the infrastructure is connected, forming a network of things (IoT - Internet of Things). The heterogeneous network consists of two main sub-networks:

- in-vehicle network connecting all sensors located in the vehicle with an on-board unit (OBU) that each vehicle is equipped with. Interactions between sensors and the OBU are established via Ethernet, ZigBee, or WiFi.
- intra-vehicle network responsible for connecting vehicles and all nearby devices. This sub-network connects OBUs, Network Relays, the Central Server, and all other elements of the infrastructure. OBUs use wireless connection based on the IEEE 802.11p standard to communicate with all other entities. The elements that are not in motion also use Ethernet connectivity.

The main entity in the ITS is an OBU, which connects the two sub-networks by processing and sharing the collected data of on-board sensors and by interactions with surrounding devices and vehicles (V2V, V2I).

Network Relays enable all the clients to communicate with the infrastructure, i. e. communication of vehicles with nearby devices like in-road sensors, Road Weather Station (RWS), or commercial nodes. Network Relays also propagate messages broadcasted by emergency vehicles enabling communication between devices that are out of range. Another key role of Network Relays is extending the reach of the V2X network, thus allowing connection between the Central Server and all devices in the network.
The communication type depends on the entities establishing the connection:



- Vehicle to Sensor (V2S)
- Vehicle to Vehicle (V2V)
- Vehicle to Grid (V2G)
- Vehicle to Infrastructure (V2I)

The communication type that is relevant to the services offered by the Company is V2I. The Vehicle to Infrastructure connection is accomplished entirely by the IEEE 802.11p wireless and bi-directional communication standard, which is a part of the ETSI ITS-G5 standard.
OBUs installed in vehicles use the same radio and antennas to interact both with other users of the road (V2V), and with roadside infrastructure (i. e. roads, road signs, network relays, weather stations, and commercial nodes). IEEE 802.11p WAVE is not a standalone standard, it is intended to amend the overall IEEE 802.11 standard. WAVE-conformant stations can operate in a rapidly varying environment and exchange messages without having to join a Basic Service Set (BSS), as in the traditional IEEE 802.11 use case. WAVE is an ad-hoc network that allows immediate broadcasting with a relatively small delay, which is crucial for safety in high-speed environments [6][7].

A.5.1 Management layer

Management layer consists of three planes described in [5]:

- physical plane
- data link plane
- application plane

The central server is responsible for controlling infrastructure, overseeing all entities and management of the network in those planes.
Physical plane concerns issues like:

- monitoring of all network elements (physical links, connected devices and clients)

- minimizing downtime of key infrastructure elements (maximizing online time by replicating critical components, redundant crucial hardware, emergency lines)
- ensuring low latency
- reconfiguration of physical network

Data plane is responsible for:

- ensuring data encryption (PKI, issuing certificates)
- securing data integrity (PKI, signatures)
- assuring data availability (database management, replication)

Application plane refers to:

- permissions system (certificates, signatures)
- trust system (blockchain)
- information, news, entertainment applications (infotainment systems)
- message broadcasting