Information Security Management System - V2X

Aleksander Lasecki, 236371
Grzegorz Zaborowski, 236447
Paulina Jałosińska, 232892
Przemek Borszowski, 234869
Mikołaj Grzegrzółka, 241073

1 Introduction

The following document is an Information Security Management System (ISMS) report for an abstract company responsible for infrastructure that supports V2X systems. It was based on and made in accordance with the ISO 27001 standard. Firstly, an analysis of the company in question is presented. Then an overview of security risk is given, followed by an in depth risk identification and analysis. Lastly possible risk treatments are provided.

2 Context establishment

2.1 Study of the organisation

2.1.1 The organisation's main purpose

- Deployment (through contractors) and testing of V2X related solutions
- Upkeep and maintenance of V2X infrastructure
- Ensuring high availability and reliability of deployed products

2.1.2 Its business

- Finding and analysing cutting edge V2X solutions
- Carrying out of software tests
- Carrying out of laboratory controlled and in field hardware tests
- Hiring of contractors to deploy V2X server stations
- Periodic control of the hired contractors
- Collecting and analysing statistical data regarding the safety, security and availability of the companies services

2.1.3 Its mission

The organisations mission can be expressed by their motto: "Don't bother and drive". More specifically the company does the following for its clients:

- Driving confidence and comfort
- Better awareness of road amenities availability
- Car accidents reduction

2.1.4 Its values

- Deployment and maintenance of fast and reliable V2X infrastructure
- High availability of the companies services
- Gaining and maintaining trust of the drivers in the companies services
- Increasing safety on the roads where the infrastructure is deployed

2.1.5 Technical processes

Vehicle-to-network communication (V2N) - Low and medium criticality: V2N enables vehicles to send and receive a variety of messages to and from the local V2X-AS (Application server) via an LTE and/or 5G cellular connection. Among those of low criticality are:

- Car status reporting - Each car connected to the network periodically sends a message consisting mainly of the car's GPS position, speed and heading. Path predictions may also be sent (especially if the car is following GPS directions). This process is of low criticality since its effects are mainly to do with drivers comfort (traffic jam warnings, smart GPS directions, etc) and statistical analysis (e.g. data regarding the frequency of cars on specific roads at specific times of the day can help the city's public transport with designing better bus timetables)
- Traffic status - V2N connected vehicles can request information about traffic jams, average speed on various roads, speed limits, traffic light patterns and timings, etc. This process is of low criticality for the same reasons as the previous one
- Road works information - A local V2X-AS might host information about road works that are planned or currently happening. The server can then provide each car approaching the area about the situation which might help the driver with planning a good route

Among those of medium criticality are:

- Emergency vehicle warnings - An emergency vehicle can use the server to broadcast information about the vehicle's current position and route to cars outside of V2V range allowing drivers to prepare (e.g. ensure that the emergency vehicle will be able to pass them) a lot earlier. Since this process has a more direct impact on the flow and safety of traffic it was categorised as a process of medium criticality
- Accident and car malfunction warnings - Whenever an accident happens or a car malfunctions, the cars involved in the event can inform the server about the situation (either automatically, through sensor or manually). The server can then broadcast this information to all cars in the area to warn them about potential difficulties (e.g. the message might say that a detour is required because the road is blocked)

Since 5G infrastructure allows for high speed data transfer between connected devices, certain high criticality processes, which were previously handled only by V2V (Vehicle-To-Vehicle) due to its low latency, can now be progressed by V2N. Offloading such processes to the network makes standardisation a lot easier, because vehicles do not need to be able to talk directly to each other. This also enables vehicles without full functionality to receive important messages from a local V2X-AS. Here are some examples of such high criticality processes:

- Near by accident and car malfunction warnings - Standard warnings of this kind have been given medium priority, however when a car receiving a warning is relatively close to its source, the message is considered as one of high criticality. This is because of the fact that a warning being late or not arriving at all might cause further damage (for instance, when a car crash occurs, it is vital that every car in the vicinity of the event receives a warning as soon as possible, as that will make the drivers aware of the situation and allow them to e.g. slow down or avoid a collision in time)

- Collision avoidance - This process takes place in several situation where there is a potential for a collision of two or more vehicles. Cars can send messages through the network that warn other users of the road about behaviour that might be dangerous, such as changing lanes on height speed roads, leaving and/or entering a highway. This king of communication can enable a smoother and safer environment for all vehicles but in might also prevent potentially tragic accidents (especially on highways), which is why it is considered as a process of high criticality

Vehicle-to-infrastructure communication (V2I) - Medium criticality: V2I enables communication between vehicles and network enabled road infrastructure (this includes traffic lights, road signs and even road markings). This allows drivers to receive useful information about the situation on the road (such as speed limits and red light warnings) directly from devices that are producing this information through a device-to-device 5G connection, without the need of a cellular connection or a server. This also allows network enabled road infrastructure to collect information from vehicles about the current situation on the road. Because these processes are more directly connected with the immediate situation on the road and will also become highly useful for autonomous vehicles, they are categorised as medium criticality. Here are some example communication processes:

- Smart traffic control - Traffic lights can use information about the number of vehicles in their vicinity as well as their position to switch lights between red and green at more appropriate times
- Red light warnings - Vehicles approaching a red light (or one that will soon turn to red) can receive a warning from the traffic light itself
- Stop sign warnings - Network enabled stop signs can send an warning message to vehicles that are closing in to ensure that the sign is not missed

2.1.6 Organisational processes

Here is a list of brief descriptions of some of the main processes taking place in the organisation:

- Hiring and controlling contractors - The finance department and the legal department will be responsible for hiring appropriate contractors (ones that are trusted to perform reliably) and making sure that contracts are carried out in accordance with the documentation and deadlines supplied by the hiring company
- Establishing contract with 5G service providers - 5G communication necessary for V2X is done through base stations that are not owned by the company. For this reason contract with service providers are established. Additionally, the company requires that the service providers up keeps their services for at least 99.9% of the time in a year.
- On site maintenance and infrastructure/software testing - Periodic on site maintenance of the infrastructure will be carried out by the IT testing and security department as well as the Infrastructure engineering team to ensure that the system has not been damaged and that it is running within given parameters
- Gathering statistical data - Company servers will constantly collect data regarding traffic density, number of accidents, etc from V2X-AS
- Analysis of statistical data - The data analysis department will be analysing the data gathered by the company servers to ensure that the infrastructure is performing with accordance to expectations (e.g. that the number of accidents is going down or that the frequency and severity of traffic jams is decreasing)
- Presenting statistical data - Results of data analysis will be given to the marketing team that will ensure that people (i.e. potential users of the system) are informed about the positive effects of using V2X systems in order to grow trust towards this new technology

2.1.7 Structure of the organisation

- Divisional structure: each division is placed under the authority of a division manager responsible for the strategic, administrative and operational decisions concerning his unit
- Functional structure: functional authority is exercised on the procedures, the nature of the work and sometimes the decisions or planning (e.g., production, IT, human resources, marketing, etc.)

The organisation is divided into nine departments. Each department must cooperete and provide support and documentation. Some of the chiefs manage more then one department.

- Research and Development department - main task is to plan, implement and develop new services and improve existing product or services. The second important task is to understand customers expectations on to-be manufactured services. Chief Research and Development Officer is responsible for overseeing the entire process.
- IT testing and security department - main tasks are monitoring all operations, detecting and tracking software defects and inconsistencies, executing all levels of testing, analysing users stories and use cases, monitoring all security tools and technology, ensuring cybersecurity stays on the organisational radar. Chief Technology Officer is responsible for overseeing the entire process.
- Infrastructure engineering team - main tasks are maintenance of V2X-AS hardware, periodic on site testing of the infrastructure, ensuring security and privacy of network and computer systems, troubleshooting to identify and resolve problems in a timely manner, maintaining hardware and software inventory. On-site tests are performed using company owned cars that are equipped with all necessary V2X devices. Chief Technology Officer is responsible for overseeing the entire process.
- Data analysis department - main tasks are collecting, interpreting and analysing results using statistical techniques and provide ongoing reports, developing and implementing databases, data collection systems and data analysis. Chief Data Officer is responsible for overseeing the entire process.
- Legal and HR department - main tasks are recruiting and administrating personnel, keeping positive work climate, supporting transactions, helping the organisation understand legislative and regulatory change that may impact its business model and operations, helping the organisation understand the legislative and regulatory implications of its new projects, products, services and expansion plans, managing down the legal consequences of business failures. Chief Legal and Human Resources Officer is responsible for overseeing the entire process.
- Finance department - main tasks are finance planning, providing insights into upcoming issues or potential profit, capital budgeting, treasury and finance control. Chief Finance Officer is responsible for overseeing the entire process.
- Customer service department - main tasks are managing large amounts of incoming phone calls, building sustainable relationships and trust with customer accounts through open and interactive communication, providing accurate, valid and complete information by using the right methods, handling customer complaints, providing appropriate solutions. Chief Marketing Officer is responsible for overseeing the entire process.
- Marketing team - main tasks are defining and managing the brand, producing marketing and promotional materials, monitoring and managing social media. Chief Marketing Officer is responsible for overseeing the entire process.
- Market relations team - main tasks are finding now possible contractors and maintain good relationships with them as well as researching their past work. This is done to help with hiring new contractors when needed. Chief Market Relations Officer is responsible for overseeing the entire process.

2.1.8 Organisation chart

The organisation consists of the following teams:

1. Supervisors team
    - CEO (Chief Executive Officer)
    - CTO (Chief Technology Officer)
    - CRDO (Chief Research and Development Officer)
    - CDO (Chief Data Officer)
    - CLHRO (Chief Legal and Human Resources Officer)
    - CFO (Chief Finance Officer)
    - CMO (Chief Marketing Officer)
2. Research and Development
    - R&D executive
    - Innovation specialists
3. IT testing and security department
    - Information Technology manager
    - Software tester
    - Security specialist
    - Telecommunications specialists
4. Infrastructure engineering team
    - Information Technology manager
    - Computer service technician
    - IT security technician
5. Data analysis department
    - Data administrator
    - Data gatherers
    - Data analysts
6. Legal and HR department
    - Legal manager
    - HR manager
    - Legal writers
    - Legals
    - Paralegal
    - Employee relation specialist
    - HR support
7. Finance department

- Financial executive
- Budget specialists
- Accountants

8. Customer service
    - Customer manager
    - Customer support
    - Receptionist
9. Marketing team
    - Marketing director
    - Social media specialist
    - Advertisement specialists
    - Sales representative
10. Market relations team
    - Market research team
    - Market specialist
    - Legal team

2.1.9 The organisation's strategy

The companies strategy comprises of two main goals:

- Ensuring high availability and reliability of the companies V2X infrastructure through rigorous testing prior to deployment, periodic technical audits as well as contractor control
- Constant search for new solutions available for deployment

2.2 List of the constraints affecting the organisation

The foremost constraints affecting the organisation have to do with hiring contractors for installation of V2X server stations since the companies that can be chosen need to be highly reliable when it comes to the quality of the devices installed as well as their ability to maintain a high availability over the course of time.

More over, the laws regarding 5G communication can vary in different countries and can change over time (mainly due to the fact that 5G technology is relatively new). This requires a flexible solution that can be fitted to diverse requirements.

Another aspect that requires mentioning is the budget. Since the costs of potential security breaches can be high (such breaches can cause traffic jams and even car accidents), the budget for implementing security systems can be relatively high but should be kept at a feasible level.

2.3 List of the legislative and regulatory references applicable to the organisation

- 3GPP Release 14 TR 21.914 - Technical specification for radio technology and access regulations for V2X (to vehicle, to interface, to network, to person)
- 3GPP Release 15 TR 21.915 - Frequency band specification for the PC5 interface (used for V2V communication)

- 3GPP TS 22.185 - Latency requirements: 20 ms for collision avoidance and no more then 1000 ms for non critical communication
- 3GPP Release 16 TR 21.916 and 3GPP TS 38.101 - 5G specification
- The General Data Protection Regulation 2016/679

2.4 List of constraints affecting the scope

As stated earlier, the V2X technology will profit from 5G technology, which is not commonly used yet. In only 30% of the countries, 5G network is available. However estimations suggest that by 2026 over 1/3 of the population will become 5G subscribers. This information gives hope for V2X to be commonly used with implemented 5G network despite its environmental constraints.

Stages of development are also very important during the process. V2X uses and creates cutting edge technology in order to work properly. This means that smaller details of strategy and methods might differ over time, however the main goal is constant.

Time for developing technology might play some part however at this point no projects seems to be close to successfully implement any important parts of the technology.

3 Risk analysis

Due to the documentation that defines the basic information security activities for management systems during the implementation of V2X systems. A risk analysis should be presented for the subsequent stages of implementation and operation of the technical infrastructure, additionally basic guidelines necessary for the operation of stakeholders directly involved in the functioning of the system are presented. It is about specific minimisation of potential losses based on the prepared potential threats resulting from the analysis of weak points of the implemented infrastructure and their methodical elimination.

3.1 Risk evaluation criteria

By default, the Common Vulnerability Scoring System, i.e. CVSS, seems to make the most sense as a risk assessment system. The use of the system comes down to improving computer security, along with the use of a standard scored risk assessment system. By default, the system is divided into two basic categories:

1. Qualitative assessment with regard to the estimation and isolation of critical risk in the functionality of the system. The division classifies all possible incidents taking into account the level of their risk, i.e .: Low - Medium - High - Critical (extreme threat)
2. Qualitative and quantitative assessment as an additional supplement related to the consideration of the hazard using a numerical scale ranging from 0 to 10. Used as an estimate of the probability of a given hazard.

The overall risk will be calculated as a product of the values given by both of the given categories, where the numerical values assigned to the quantitative assessment levels of risk are:

- Low - 1
- Medium - 2
- High - 3
- Critical - 4

Then the risk gets a finial value assigned based on the following rule:

- If the product is at most 5 the risk is evaluated as "Low"
- If the product is at most 15 the risk is evaluated as "Medium"
- If the product is at most 30 the risk is evaluated as "High"
- Otherwise, the risk is evaluated as "Critical"

3.2 Impact criteria

The criteria discussed were defined as a set of the greatest possible number of potential, exemplary events and their direct impact on the operation of the V2X system. Due to the desire to analyse the risk determination method as efficiently as possible, in order to estimate losses in general in relation to the functionality of the system as a whole.

1. Impact of loss of customer data confidentiality. Given the strong blow to the company's reputation and its ability to ensure the security of the services provided. It is definitely a very high, or potentially critical, possible risk.

2. The impact of the loss of confidentiality of company documentation should be classified very similarly to the previous one. This is a direct threat to the company's reputation for customer data documentation and the company's financial continuity. It risks significant financial losses given the income potential with the data of the R&D section.

3. Impact of the loss of confidentiality of information about the internal structure of the company. Rather, the potential risk should be characterised as medium. In case of loss of confidentiality in the internal structure of the company, there is a higher probability of successful attacks in the future, depending on the situation. Taking into account the exact characteristics of potential attack targets, also in terms of very precise attacks on the vital structures of the company's operations and attacks on personal data.

4. Impact of a potential hacker attack on the integrity of the internal system. This type of threat should be characterised as critical with regard to the structure of the V2X infrastructure operation. Depending on the effectiveness of the attack, there may be incredible losses, also related to the threat to the lives of potential system users. The impact of an attack can be characterised as a test possibility to penetrate a low-severity system or a complete change / disruption of the most important structures of the system. Moreover, such an attack clearly shows the inability to ensure the security of the infrastructure in key moments of its operation.

5. Impact of misuse of the infrastructure by a malicious user. This includes situations such as a user logging into the system multiple times in order to appear as if they had multiple vehicles on the road (e.g. to ensure a clear passage for themselves) and other potential exploits of the V2X system that do not require security breaches. Such attacks may pose a threat to the flow of traffic and even cause large traffic jams on city blockages. For this reason, these attacks should be considered as having high to critical impact on the system.

6. The impact of breach of contract should be characterised in relation to the exact factor of the contract that was actually breached. Taking into account the characteristics of the infrastructure operation and analysing the basic situations of the occurrence of such an impact, it should be defined with the potential possibility of undisturbed further functionality of the system.

    - below 1% of the annual income qualify as Low,
    - between 1% and 5% of the annual income qualify as Medium,
    - between 5% and 10% of the annual income qualify as Medium,
    - above 10% of the annual income qualify as Critical. And should be considered utmost risk of the system functionality.

7. Direct environmental impact may result in total inability to operate or destruction of the system infrastructure. Therefore, It is characterised based on the potential threat of a specific event and the impact of losses resulting from it. The possible estimation of the impact results from a general knowledge of the infrastructure operation pattern and its operating environment.

3.3 Risk acceptance criteria

In any situation, risks characterised as "Low" are acceptable, but in certain cases higher risk may also be accepted.

- When it comes to low criticality processes such as traffic status information broadcasting, accepted levels of risk go as far as "High" since potential threats of these protocols failing are only to do with a slightly lower level of comfort of the users

- For medium criticality processes such as emergency vehicle warnings (at a larger distance), "Medium" levels of risk can be considered as acceptable since those protocols have their high criticality counterparts (when the information is broadcasted at a short distance)

- For medium criticality processes that do not have a high criticality counterpart "Medium" levels of risk are also accepted since those protocols malfunctioning pose a higher but not critical threat, but such medium risks should be avoided as much as possible
- High criticality processes are only allowed to have low criticality risks connected with them. That is because any malfunction or glitch that has to do with them can potentially be a cause of a major car accident
- Additionally, no risk at a "Critical" level can be accepted as they may be disastrous to the entire system and render it out of order

3.4 The organisation for the information security risk management process

The Chief Information Security Officer is mainly responsible for the security of information and the system. In addition, the entire privacy structure of the company complies with the principles of the GDPR regulation, each employee is required to control the processed information as a standard due to the potential threat to the functioning of the system. Each direct section takes care of the security of the information it processes, and at the same time there are regular control procedures implemented by CISO.

3.5 Identification of assets

Essential to the potential risk analysis process is the identification of all relevant assets. Because only the risks and system flaws included in the listed assets for risk analysis are taken into account.

3.5.1 Primary assets

Those are the assets directly connected with the company's business, such as its processes and values:

- Low criticality V2N communication processes such as car status reporting as well as road and traffic status broadcasting
- Emergency vehicle warning processes (both at long and short range, the latter being of high criticality)
- Car accident reporting and warnings (similarly to the previous one, we consider communication at long and short range)
- Good relation with past and new possible contractors
- The process of establishing and executing specific requirement (e.g. legal or time based) for contractors
- The process of controlling of the contractors work and progress (i.e. checking if they are compliant with established requirements)
- Trust of the infrastructure's users
- Undisturbed services of the company and confirmation of the highest quality of the presented system
- Full compliance of the company's activities with all legal regulations

3.5.2 Supporting assets

A resource group classified as necessary to maintain primary assets is referred to as a supporting asset:

- Technical infrastructure and buildings necessary for the functionality of the company and the system
- Detailed documentation on the company's finances, implementation projects, software used, research programs and used patents

- Proven and good quality installations necessary for the functioning of V2X communication technology
- Qualified staff, neat communication processes and an individual approach to the executive process
- A modern, individual system of early detection of potential threats
- An effective system of internal security and system information processing and updating
- Detailed documentation of the company's processes

3.6 Threats

A threat has the potential to harm assets such as information, processes and systems and therefore organisations. Threats may be of natural or human origin, and could be accidental or deliberate. In presented ISMS document, the identification of the source of threats is based on notation established by ISO/IEC 27005 standard:

- deliberate (D): used for all deliberate actions aimed at information assets,
- accidental (A): used for all human actions that can accidentally damage information assets,
- environmental (E): used for all incidents that are not based on human actions.

Due to the multitude of different threats, we focus only on the most important, which can significantly affect: the proper functioning of the infrastructure, information compromise, failure to comply with the contract and company's reputation. Following threats were recognised and described as a result of research in organisation:

The proper functioning of the infrastructure:

- Fire (D, E),
- Bad weather conditions (E),
- Loss of power supply (D, A, E),
- Failure of telecommunication equipment (D, A),
- Saturation of the information system (D, A): DoS or heavy network traffic,
- Corruption of data (D, A),
- Equipment malfunction (D, A).

Information compromise:

- Revealing secret data in public documents (D, A),
- Industrial or state espionage (D),
- Retrieval of recycled or discarded media (D),
- Theft of documents or equipment (including confidential plans) (D),
- Illegal processing of data (D, A),
- Incorrect grant of privileges to workers (e.g. low-level employee has full access to system functionality) (D, A),
- Unauthorised access to specific facilities (D),

- Compromising data for evaluation by tampering with hardware or tampering with software,
- Evil maid attack (e.g. an unattended laptop in a hotel room may be infected by a malicious maid) (D),
- Specialised hacking attacks (D).

Failure to comply with the contract and company's reputation:

- Unprofessional contact with business partners (D, A),
- Failure to provide things on time (services, documentation, etc.) (D, A, E),
- Patent steal (D),
- Personnel availability (A).

3.7 Existing controls

Many controls supposed to protect company assets from potential threats have already been implemented. In this section an analysis regarding these is presented. We also mention controls that are not yet implemented, but are planned as they are necessary to obtain a full view of the companies information security situation.

3.7.1 Already implemented controls

- Communication related controls: These are mainly to do with handing V2N communication protocols in a secure way:
  - Use of public key infrastructure to ensure the integrity of the system - Long term and temporary certificate based protocols are implemented and are working as expected
  - Use of proven and secure signing and encryption protocols - Implemented and working as expected
  - Use of only trusted libraries and proven ready-to-use solutions - Mostly implemented, some libraries require additional research and testing
  - Communication prioritisation i.e. communication is prioritised according to the process criticality - Systems are implemented and are working as expected
  - High unit test code coverage - All parts of the code relevant to V2X communication are properly tested
- Data protection controls: These are mainly to do with protecting company files and statistical data
  - Weekly backups of statistical data - A contract with a backup storage company was established
  - Access to data is restricted to unauthorised users - Only employees working for the right department and of a high enough position are able to access and/or modify company files
- Physical controls: These are mainly to do with the physical integrity of the system
  - Physical documents are stored securely - Key drawers are used to store all documents
  - Servers and other devices that are part of the V2X infrastructure are well built - All devices have appropriate certification and are properly tested
  - High quality cables and other materials are used - All materials have appropriate certification and are properly tested
- Organisational controls: These are mainly to do with the organisation and its internal processes

- Proper care is taken when preparing requirements and contracts - All reviewed documents were written properly and in accordance to the law
- Company personnel is well paid - All personnel is given a salary appropriate to their position and level of responsibility
- Only reliable contractors are hired - The company has a department entirely responsible for ensuring the reliability of hired contractors, additionally those hired are controlled to ensure that their work is done on time and in accordance with established specifications
- Proper documentation of company processes - The legal department also makes sure that all company processes are well documented and in accordance with the law

3.7.2 Planned controls

- Frequent on site device/software tests - Enough tests will be performed to ensure high availability and reliability of the system
- Frequent usage tests - Tests using vehicles connected to the system will be performed to ensure that everything is performing as expected
- Periodic maintenance - Monthly maintenance will be carried out to prolong the life of used devices

3.8 Vulnerabilities

A thorough procedure of maintaining security and ensuring appropriate organisational procedures requires the analysis of vulnerabilities in the system security and the basic weaknesses of the general functionality of the system based on V2X communication. There will also be more prosaic forms of potential threats from these vulnerabilities, such as system misuse. Accurate summaries allow for the minimisation of errors that may cause a significant threat in the overall spectrum of the system's operation, which could consequently lead to its paralysis. A careful and thorough analysis is therefore essential.

- No control was found that would protect statistical data that is stored on company servers. Because of that a potential specialised hacking attack might be able to modify or remove such files which poses a serious thread to the system.
- The company has to rely on 5G service providers and thus has a relatively small level of authority over the communication infrastructure. Because of that failures of telecommunication equipment are not in the companies control and thus the company has to rely solely on the fact that service providers promise undisturbed communication of at least 99.9% of time (this is calculated for an entire year).
- An unexpected peak in traffic might lead to saturation of the system which could lead to denial of service or delays longer then declared in the specification.
- Insufficient testing and maintenance of the installed equipment might lead to its premature failure.
- If a key to one of the secure document drawers is given to an employee that is not authorised to use it, the documents might be accessed by someone that should not be able to see then which could lead to a leak of company secret data.
- A contractor that is not treated with appropriate respect (i.e. a correct pay, well determined deadlines etc) might performs their tasks incorrectly (by e.g. delaying the deployment of an application server) or might do their task correctly by not want to work with the company again.

3.9 Identification of consequences

With most important threats, assets and vulnerabilities explained, it is possible to analyse consequences of certain incidents. In this section we will take a look at some of the threats and consider following action and assets affected by it. These scenarios might clear out the consequences of fulfilling risks evaluated earlier.

- **Threat**: Fire
  Possible assets: All communication processes, undisturbed services, documentation of the companies processes
  Despite the effort, fires hazard is still an existing hazard among many facilities. For example, even a lightning strike might cause a significant amount of damage. With spread of fire, hardware containing user data and documentation might be destroyed, which means days or even weeks of rebuilding the infrastructure. During this this time technology will not work as intended. The proper counteraction would be to call fire brigade immediately. Technicians would also help and try to recover all possible data. This threat is evaluated to be of "critical" impact.

- **Threat**: Equipment malfunction
  Assets: Undisturbed services, technical infrastructure, documentation of the companies processes
  Most of technical devices (like hard drives or other storage equipment) are not immune to breaking and wearing down of age. This may lead to many accessibility problems until problem won't be solved by technicians. This calls for making backups of all possible data collected and always having emergency storage devices for quick recover. Every second is important when it comes to providing undisturbed services.

- **Threat**: Specialised hacking attack
  Assets: All communication processes, documentation of the companies processes, trust of the infrastructure's users, security systems
  A company, which takes responsibility to provide security might be a target for various hacker attacks as it stores big amount of appealing data. There are many assets that could be affected by this threat. Leak of users' data provided to us with biggest trust might discredit the company. On the other hand company's sensitive data might be even more damaging. This includes documentation, staff's personal data and salaries, structure and future plans. These two scenarios will certainly come with various consequences. Someone might blackmail the company in order to obtain money or other profitable goods. Someone might try to compromise the information just to create an image of untrustworthiness. In addition, attacks using software vulnerabilities or weaknesses in the communication protocol may affect the operation of the entire infrastructure and thus the safety of human life in road traffic. These attacks might come from different sources. An attacker could be performing remotely or he could make use of being inside the infrastructure (e.g by pretending to be a worker). These kind of operation will probably make devices and processes unavailable for a while or even the need to replace some hardware and software. In this scenario we should be aware of possible eavesdropping trackers that might be left inside the hardware, system manipulation or hardware damage. Technicians should make every effort to prevent such a thing. The threat's impact is considered to be "critical".

- **Threat**: Misuse of the system
  Assets: Undisturbed services, trust of the infrastructure's users, some of the communication processes
  The first case of misuse of the system may occur when accidentally logging into another user's account. This can happen when users have a similar login, for example,created by combining the first and last name and some additional character, and use simple and unsafe passwords such as first name and some number. The consequences of logging into another user's account, which may lead to data leakage, theft or manipulation, are very serious. The company may face financial penalties and, what is more, the company may lose its customer's trust.
  The second case of misuse of the system may happen by logging into the system multiple times by one user.

As a result of such action, the system may consider the road to be jammed and guide another users to the other routes. The consequence of this is the wasteful use of infrastructure. The impact of multiple logging into the system, resulting in uneconomical road use, may have serious consequences in the case of route planning for emergency vehicles such as ambulances or fire brigades. The time of arrival of these vehicles affects safety, health and human life.

- **Threat**: Loss of statistical data
  Assets: Good relation with past and new possible contractors, trust of the infrastructure's users
  A company collect big amount of statistical data to better understand the reality on the road and provide the best services to our clients. This effort might sometimes may be for nothing. Data might get lost due to various reason. It might get stolen, deleted intentionally or it might get corrupted in many ways after some kind of accident. For example a piece of hardware might get broken due to water leak or flood in the area. An important counteraction would be to have backups of data placed in different area. Also having spare data storage elements could help in quick data recovery. After any incident, technicians should try to gather most of the lost data as quickly as possible. This threat's impact is considered to be "medium".

- **Threat**: Failure of telecommunication equipment
  Assets: All communication processes, trust of the infrastructure's users
  Failure of telecommunication equipment can be caused by many issues such as loss of power supply, software/hardware problems, 5G service issues or hacker attack. Because of that it is essential to ensure that such failures are handled properly and as unlikely to happen as possible. As was mentioned earlier, the company has already implemented many controls that are supposed to lower this probability. Examples of such controls are software/hardware testing, maintenance and reliable contractors. Additionally, certain company organisational processes are designed in a way to further lower this probability, for example contracts with 5G service providers have a requirement that the communication is up undisturbed for at least 99.9% of the time each year. This is a threat that should be respected the most as, for example, a failure to comply with critical communication delay limits can lead to car accident and potentially even to human casualties.

3.10 Risk estimation

This section takes potential consequences described in the previous one and presents and assessment of them. It also provides an estimation of the risk and likelihood of each of the scenarios. The probabilities of occurrence are calculated based on statistical data taken from other, already operational, V2X systems. The impact criticality of each threat is given in accordance to the impact criteria.

- **Threat**: Fire
  Possible assets: All communication processes, undisturbed services, documentation of the companies processes
  Most company processes are relying on the V2X-AS devices installed near road infrastructure. For this reason and, additionally, because the infrastructure is built out of inflammable materials the probability of such incident is estimated as 0 out of 10 and, thus the overall impact criticality is evaluated as "Critical" due to potential damage to high criticality processes.

- **Threat**: Equipment malfunction
  Assets: Undisturbed services, technical infrastructure, documentation of the companies processes
  Taking into account the fact that the entire system functions on individual elements of the technical infrastructure. In addition to the most important devices directly responsible for the operation of the entire V2X communication protocol as well as the individual device used at work by the employees. Any major technical

failure might cause consequences that range from "Low" to "Critical" criticality. However, when the probabilities of such failures are taken into account, we observe that employee equipment (that can only cause low impact consequences) has the highest probability of failure of 6 out of 10 but for V2X infrastructure (which can cause up to critical consequences) that probability is a lot lower due to frequent tests and maintenance and is evaluated as 1 out of 10.

- **Threat**: Specialised hacking attack
  Assets: All communication processes, documentation of the companies processes, trust of the infrastructure's users, security systems
  It is not easy to estimate the risk for specialised hacking attacks due to the multitude of known attacks and the occurrence of newer and newer attacks. In addition, attacks can exploit software vulnerabilities that we have no idea about until someone finds or exploits them.

  Algorithms are the key behind the successful operations of autonomous vehicles in C-V2X. Majority of these algorithms rely on the formation of a secure channel between the vehicles (V) and all other applications in the network (X). Vulnerability in the algorithms can lead to several types of cyber attacks on C-V2X. The threat level increases as vehicles in the network operate from full-assistance to no-assistance (fully-autonomous). The Autonomous Algorithm Safety (AAS) depends on the mode of operations and deployment scenarios of vehicles. Specifically, in C-V2X, channel security, session management, security-patches, key management, access control, and camouflage-detection are the key perspectives to look forward to for AAS. Probability of such situation is estimated as 0 out of 10 and the criticality can vary from high to critical.

  Information leakage may occur as a result of a hacking attack. In this case, the risk estimate will depend on the importance of the stolen information. In case of loss of confidentiality of any information may cause higher probability of successful attacks in the future, any such scenario should be considered as not less than "Low". Information such as the internal structure of the company, the location of servers, base stations, etc. can be accessed by lower-level employees and partners of the company, so the probability of leakage is estimated as 5 out of 10 and should be considered as the "Low" level due to its low impact. For high-level employee impact should be "Medium" due to the access to the technical side of the infrastructure and probability of such situation is estimated as 3 out of 10.

- **Threat**: Misuse of the system
  Assets: Undisturbed services, trust of the infrastructure's users, some of the communication processes
  Misuse of the system by logging into the account of another use may appear as a result of several components that must occur at the same time. The chance for this is small, but taking into account that names will often repeat themselves and people often do not care about securing the account with an appropriate password, it cannot be excluded. The probability of such incident is is estimated as 1 out of 10 and its impact is evaluated as "High".

  On the other hand, logging in multiple times by one user can be a bigger problem as it can cause traffic jams and even city blocks. Many users will surely be interested in checking if they can manipulate the system in any way. This problem is more likely to occur and is given the probability of 6 and its impact is estimated as "High".

- **Threat**: Loss of statistical data
  Assets: Good relation with past and new possible contractors, trust of the infrastructure's users
  Considering many different sources of potential data loss, the probability of data loss is estimated as 4 out of 10. This comes also with a fact, that there's a lot of equipment storing all the statistical data and some of it is not in the hands of the company (backups are handled by another entity). Taking it to account we must also acknowledge that with backups working as intended, the long term impact will be low, and with corresponding

protocols, the company might loose little to no data permanently. Despite that, the overall impact of this threat is evaluated as "Medium" due to possible temporary issues it may cause to the companies ability to gain and maintain the trust of drivers.

- **Threat**: Failure of telecommunication equipment
  Assets: All communication processes, trust of the infrastructure's users
  Potential failures of the communication equipment pose a serious threat to the system and its users. This is because they can cause delays in the communication (which is especially problematic in the case of critical communication which has to have a delay of at most 20 milliseconds) or a total lack of any communication for a short period. This can lead to traffic jams, car accident and even death and so the impact of this risk is evaluated as "Critical". Multiple countermeasures are implemented or are planned to be implemented to lower the probability of such an event to a value that is as low as possible. Among these countermeasures are frequent test and maintenance of all V2X devices as well as the fact that the company only hires reliable contractors for application server deployment and many others. Because of that the probability is evaluated as 0 out of 10.

4 Risk evaluation

The process of comparing the results determined according to the risk analysis guidelines with the risk assessment criteria performed when estimating the potential acceptability of a given risk is called a Risk evaluation. According to the analysis performed, detailed guidelines for risk evaluation criteria are classified and prioritised in terms of the level of acceptability. The following list is ordered from the threats of highest priority (those that are furthest from acceptable) to lowest priority (ones that are fully acceptable).

- Specialised hacking attack is not easy to evaluate due to their quantity, size and complexity. Probability of occurrence is hard to predict and the consequences can be various. Nevertheless, any hacking attack is a serious problem that cannot be ignored in any way. It can affect critical system and infrastructure components, and elements that appear to be insignificant. On the other hand, each successful attack or information leak may lead to consequences, such as increasingly successful attacks, malfunction of the infrastructure and system or complete discredit of the company. Therefore, for attack on V2X communication systems the risk is evaluated as "Low" due to its critical impact (4) and lowest possible probability of occurrence (0). Information leak accessible by lower-level employee despite the high probability of occurrence (5) should be "Low", thus its low impact (1), while for high-level employee should be "Medium" due to the access to the technical side of the infrastructure which raises the impact criticality to medium (2) despite the lower probability of occurrence (3).

- Loss of statistical has a relatively high probability of occurrence (4) due to a lack of security measures used for protecting these files, but because of backups the overall impact is estimated as only "Medium" (2). Because of that, the overall risk is evaluated as "Medium".

- Misuse of the system is broken down into two possible scenarios. The first one happens when someone gains access to another users account and its risk is evaluated as "Low" due to its high criticality (3) and low probability of occurrence (1). The second scenario is a situation when a single user logs is to the system multiple times. Here, the risk is evaluated as "High" due to its higher probability (6) and high criticality (3).

- Due to multiple implemented countermeasures the probability of a failure of telecommunication equipment is very low (0), so despite the critical impact (4) of this risk, it is still evaluated as "Low". This is, of course, given that all planned controls are implemented in due time.

- Due to the variety of technical failures that the company and its processes might face, this risk of equipment malfunction is broken down into two: Failure of employee equipment which is evaluated as "Medium" due to relatively high probability (6) and low criticality (1) and failure of V2X devices which is evaluated as "Low" due to its very low probability (1) and despite its high criticality (3-4).

- The risk of fire has critical consequences (with a value of 4) and the lowest possible probability of occurrence (0). This gives as a product value of $0 \cdot 4 = 0$ and this the risk is evaluated as "Low"

5 Risk treatment

- **Threat**: Specialised hacking attack
  Assets: All communication processes, documentation of the companies processes, trust of the infrastructure's users, security systems
  Data leakage caused by a lower-level employee is "Low" level risk. In addition, a low-level employee does not have access to sensitive data like technical documentation so risk is acceptable. A higher-level employee has access to confidential documents that have a medium impact on criticality process, so the estimated risk is "Medium". The risk is therefore acceptable but should be avoided as much as possible. In order to avoid this risk, it would be advisable to consider a few improvements that do not require a high budget: All the disks should be encrypted when given to an employee. Email security policy should also be implemented. All emails inside the company should be kept encrypted and all pieces of information should be sent as encrypted files. Periodic check of all employees' software version on their devices.

  For other hacking attacks, things are not such easy. V2X is a very complicated system and difficult to manage, and defending against hacker attacks requires enormous knowledge and proper diligence. A successful hacker can take control of the system, manipulate data, disrupt the system, etc. This can have a direct impact on the lives of V2X system users. Therefore, it was marked as "Low" risk despite the high impact because appropriate efforts have been made to secure the entire system. The risk is acceptable, but due to the discovery of newer and newer attacks and gaps in the existing security systems, we would propose to implement some additional functionalities that will allow you to be prepared for possible future attacks:

  - Conducting regular penetration tests and audits.
  - Using only trusted libraries and proven ready-to-use solutions because some libraries require additional research and testing.
  - Cooperation with companies and universities dealing with the security of computer systems to have the latest knowledge in the field of security.
  - Follow all relevant security-related scientific journals to track new types of attacks and potential vulnerabilities in existing solutions.

- **Threat**: Loss of statistical data
  Assets: Good relation with past and new possible contractors, trust of the infrastructure's users
  Taking into account all of the sources of data loss and possible short term impact on the company's name this risk was evaluated as "Medium" which is acceptable but minimising it is advised. Additional security measures such as data encryption should be implemented to lower the probability of loss to 2 out of then. This would drop the overall risk to "Low" which is highly preferable especially due to that fact that such a change is neither difficult not expensive to implement.

- **Threat**: Misuse of the system
  Assets: Undisturbed services, trust of the infrastructure's users, some of the communication processes
  The first scenario (i.e. someone gaining access to another user's account) has a "Low" risk and this is acceptable.

  The second scenario (i.e. someone logging into the system multiple times) has a level of risk evaluated as "High" which is unacceptable. However, the probability of such an event may be lowered by implementing these new controls.

  - Conducting regular tests and audits.
  - Analysing data on login and logout times as well as the GPS locations of login actions.
  - Sending warnings to users about that are suspected to have abused the system.

– Drawing consequences from serious system abuse.

These would lower the probability of such an incident to 1 out of 10 and would thus make change the risk to "Low" which is acceptable.

- **Threat**: Failure of telecommunication equipment
  Assets: All communication processes, trust of the infrastructure's users
  The risk of this threat was evaluated as "Low" which is acceptable, even for critical communication processes such as collision avoidance. Never the less, the company should still strive to lower this risk even further when possible as such a failure can have drastic consequences.

- **Threat**: Equipment malfunction
  Assets: Undisturbed services, technical infrastructure, documentation of the companies processes
  Looking at the assets that relate to this threat, we observe that "Medium" risk relates to processes of low criticality and only "Low" risk relates to high and critical processes. For this reason the risks are accepted. In the event of an incident, the basic activity is to verify and estimate the damage. In the event of damage to the infrastructure responsible for the communication protocol, the appropriate department should be notified to carry out repairs as soon as possible.

- **Threat**: Fire
  Possible assets: All communication processes, undisturbed services, documentation of the companies processes
  The occurrence of a fire can affect high criticality processed, but since its estimated level of risk is low it is considered as acceptable.

6 Risk acceptance

This section is to be filled by the companies management.