Improved Robotic Platform to perform Maintenance and Upgrading Roadworks: The HERON Approach

Grant Agreement Number: 955356

D6.1: Secure Communication and Networking infrastructure

Work package	WP6: Communication and Networking Solutions, DSS, IMS and CoP
Activity	Task 6.1: Secure Data Communication
Deliverable	D6.1: Secure Communication and Networking infrastructure
Authors	Dimitrios Kokolakis, Elena Avatangelou,
Status	Final (F)
Version	1.0
Dissemination Level	Public (PU)
Document date	27/07/2023
Delivery due date	30/06/2023
Actual delivery date	27/07/2023
Internal Reviewers	Nikos Bakalos (ICCS), Ilias Gkotsis (SATWAYS)
	This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under grant agreement no 955356.

Document Control Sheet

Version history table			
Version	**Date**	**Modification reason**	**Modifier**
0.1	22/05/2023	Initial Table of Contents and initial content	INAC
0.2	23/06/2023	Content edits	INAC
0.3	26/06/2023	Initial comments on document structure	SATWAYS
0.4	28/06/2023	Pre-final version sent for internal peer review	INAC
0.5	29/06/2023	Comments on the prefinal version	STWS, ICCS
0.6	21/07/2023	Updated version	INAC
0.7	21/07/2023	Peer-reviewed version ready for submission	STWS, ICCS, INAC
1.0	27/7/2023	Final version for submission	INAC

Legal Disclaimer

Table of Contents

List of Tables

List of Figures

Abbreviation List

Abbreviation	Definition
CPU	Central Processing Unit
DPIA	Data Protection Impact Assessment
GDPR	General Data Protection Regulation
HDD	Hard Disk Drive
IDS	Intrusion Detection Systems
IPsec	Internet Protocol Security
NIS	Network and Information Security
MitM	Man-In-The-Middle
MQTT	Message Queuing Telemetry Transport
TLS	Transport Layer Security
VPN	Virtual Private Network
SSD	Solid-State Drive
SSH	Secure Socket Shell
SSL	Secure Sockets Layer
UAV	Unmanned Aerial Vehicles
UGV	Unmanned Ground Vehicle
WIPS	Wireless Intrusion Prevention Systems
WPA	Wi-Fi Protected Access

Executive Summary

This report is written in the context of WP6 - Secure Communication and Networking infrastructure of the HERON project. The deliverable describes the security requirements deriving from the most common EU Privacy and Cyber Security Directives which are described in section 2, analyses the importance and need of a secure data communication layer to mitigate any threats which might occur in a network communication system where many different components exchange critical data. The document also aims to analyse how cyber security best practices can be applied, including the use of Transport Layer Security (TLS), SSH mechanism, SSL, to ensure the overall system is not compromised. This document also describes the setup and deployment of a Kafka cluster in a dedicated server which will handle all the communications between the HERON project core components. All tools responsible for sharing their data will publish it to the Kafka cluster and the services can consume them for further processing.

1 Introduction

1.1 Purpose of the Document

The purpose of this document is to present the design and implementation of the communication and networking layers and protocols to enable the automated vehicles for maintenance and upgrading efficiently communicate with the control center.

The document is the outcome of Task 6.1 Secure Data Communication.

Chapter 2 of the document presents EU Directives on Privacy and Cyber Security. Chapter 3 focuses on the Data communications, Threats and Solutions. Chapter 4 presents the Secure Data Communication and Networking Infrastructure. Chapter 5 presents the Infrastructure and Deployment setup.

1.2 Intended Audience

The document's target group is mainly the HERON consortium partners. Nevertheless, the information presented in the document is of special importance to both technical partners and end-users involved in the deployment and implementation of the HERON pilot cases.

1.3 Interrelations

This deliverable interacts with all other technical WPs, namely WP3-WP7. It is also related to D2.2 HERON Architecture Specification.

2 EU Directives on Privacy and Cyber Security

2.1 Privacy and Cybersecurity Requirements elicitation based on EU directives

2.1.1 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) [1] is a comprehensive EU directive aimed at protecting individuals' privacy and personal data. When invoking GDPR-based privacy and cybersecurity obligations, the following subcategories might be considered:

- **Data Protection Impact Assessment (DPIA).** DPIA is an abbreviation for Data Protection Impact Assessment. It is a procedure meant to assist companies in identifying and assessing the potential risks and consequences of specific data processing operations on individuals' privacy and data protection rights. DPIA is a critical tool for ensuring GDPR compliance and mitigating any potential threats to personal data. The DPIA introduces the requirement for periodic assessments of the data collected from the HERON components.

- **Consent Management.** Consent is an essential component of GDPR compliance [2]. Eliciting consent management needs entails assembling the appropriate controls, methods, and procedures for getting and managing user consent. This includes getting explicit consent for sensitive personal data processing, providing clear and detailed information about the aims of the processing, providing choices to withdraw consent, and maintaining consent records.

- **Data Subject Rights.** GDPR provides data subjects with different rights in relation to their personal data [3]. Exercising data subject rights requires collecting the required steps and processes to allow persons to exercise their rights. This includes requirements for granting individuals access to their personal data, facilitating data rectification, enabling data erasure (the "right to be forgotten"), allowing individuals to restrict processing, facilitating data portability, and providing mechanisms for objecting to data processing activities.

- **Data Breach Notification.** In the event of a personal data breach, the GDPR requires to swiftly and efficiently notify supervisory authorities and impacted individuals [4]. Eliciting data breach notification standards entails collecting the essential controls and procedures for detecting, analyzing, and reporting data breaches. This includes standards for timely disclosure, breach notification content, interaction with relevant authorities, and breach incident documentation.

2.1.2 Network and Information Security (NIS) Directive

The NIS Directive [5] intends to improve EU Member States' and Critical Infrastructure operators' cybersecurity capabilities. Subcategories may be included when evoking privacy and cybersecurity requirements based on the NIS Directive:

Incident Response and Management

The processes and procedures that businesses use to detect, respond to, and recover from cybersecurity problems are referred to as incident response and management. It entails taking

a coordinated approach to dealing with security breaches, unauthorized access, system failures, data breaches, or any other incident that jeopardizes the confidentiality, integrity, or availability of information systems.

Security Measures and Controls
Defining security measures and controls requires putting in place adequate technological and organizational safeguards to protect network and information systems. Capturing needs for access controls, encryption mechanisms, monitoring systems, and security incident detection procedures is part of this. Furthermore, requirements may include the installation of security patches and updates, personnel security awareness training, and the usage of safe configuration practices for systems and devices.

Risk Assessment and Management
Risk assessment and management refers to the process of recognizing, evaluating, and prioritizing risks regarding an organization's assets, activities, and objectives. It entails examining potential threats, vulnerabilities, and impacts to determine the likelihood and potential consequences of bad events. The purpose of risk assessment and management is to enable companies to make informed decisions and take appropriate actions to successfully minimize or address identified risks.

Information Sharing and Cooperation
Information sharing and collaboration refers to the joint efforts and information exchange between different entities to improve cybersecurity and solve common risks and difficulties. In the context of privacy and cybersecurity standards, information sharing and cooperation are critical in boosting situational awareness, enabling effective incident response, and creating a collective defense approach.

2.1.3 ePrivacy Directive

The ePrivacy Directive [6] is concerned with the privacy and security of electronic communications. Subcategories may be included when evoking privacy and cybersecurity requirements based on the ePrivacy Directive:

Consent for Electronic Communications
This section addresses the requirements and procedures for gaining user consent for electronic communications. Considerations for gaining valid consent for the use of cookies, electronic marketing communications, and tracking technology are included. The section discusses the significance of explicit consent, offers advice on how to give cookie opt-out procedures, and emphasizes the importance of adhering to electronic marketing regulations.

Confidentiality of Communications
Confidentiality of Communications addresses the protections required to ensure the confidentiality and privacy of electronic communications. It underlines the importance of policies and safeguards to secure the storage, monitoring, and interception of personal communications. The section emphasizes the necessity of protecting the privacy of electronic communications and preventing illegal access or interception.

Security of Electronic Communications
This section focuses on the security and integrity of electronic communications. It specifies the standards for establishing security measures to safeguard electronic communications against

attacks and weaknesses. This involves using encryption, data protection measures, and safeguards to prevent illegal access or communication interception.

Privacy and Security in Online Services
This section focuses on the privacy and security concerns that online service providers must handle. It specifies rules for user consent processes, such as getting informed consent for data collection and processing. It also underlines the significance of having privacy policies that clearly describe how user information is handled and protected. Additionally, the section emphasizes the importance of secure data handling methods and mechanisms to protect user information from unwanted access or disclosure.

3 Data communications: Threats and Solutions

Data security is essential in the world of quickly developing technology, especially in applications where dependability and autonomy are crucial. This includes the case of HERON which involves using 4G/5G or WIFI networks to connect a physical machine e.g. a robotic vehicle, to a control node. The potential threats and risks related to data security are still present and call for regular monitoring and modification despite the improved speed and wide reach these technologies offer. The major threats and solutions per communication type will be discussed hereafter.

3.1 4G-5G Connection

Man-In-The-Middle Attacks (MitM)

These are sophisticated assaults that take place when a third party intervenes in a communication between two entities, giving them the opportunity to potentially intercept, alter, or divert the data. This could have serious repercussions in the context of 4G/5G communications for robot-to-control node systems, such as incorrect commands being delivered to the robot or sensitive data being retrieved from the data flow.

- **Threat mitigation:** To prevent MitM attacks, strong encryption and authentication mechanisms must be implemented. The identity of the persons engaged can be guaranteed, and the integrity and secrecy of the communication can be safeguarded, thanks to Transport Layer Security (TLS), which incorporates certificate-based authentication. Furthermore, regular network traffic monitoring and the use of intrusion detection systems (IDS) can aid in the early detection of such attacks.

Eavesdropping/Interception:

In this case, someone is listening in on the conversation between the robot and the control node without authorization. The possibility of a data breach, including the extraction of private operating parameters or proprietary techniques, increases if the data is not encrypted.

- **Threat mitigation:** The key to preventing eavesdropping is robust end-to-end encryption. It's crucial to select encryption methods that are acknowledged by the cybersecurity community as secure. Another recommended practice is to update encryption keys on a regular basis. To further strengthen the system's security, secure key management systems should be used.

Physical Attacks

This refers to actual physical manipulations of the robot, such as tampering with its hardware, removing private data from its memory, or inflicting direct harm that might compromise its functionality.

- **Threat mitigation:** A tamper-detection system that sounds an alarm in the event of a physical breach could be built to prevent physical attacks. This can involve using tamper-resistant hardware or tamper-evident seals. Additionally, it is crucial to take preventative measures like limiting access to the robot to authorized individuals only.

Malware Attacks

An attacker may take control of the system, extract data, or interfere with regular operation if they were able to infect the robot or the control node with malware.

- **Threat mitigation**: The first lines of protection against malware are up-to-date antivirus and antimalware programs. A secure boot procedure can also help verify that the system hasn't been tampered with prior to startup. Finally, network security tools

like firewalls and IDS/IPS systems can aid in preventing malware from entering a system over a network connection.

3.2 WI-FI Connection

Man-In-The-Middle Attacks (MitM)

When an adversary intercepts the communication between the robot and the control node using WiFi, similar to a 4G or 5G environment, they may be able to alter, reroute, or even invent the data being transferred.

- **Threat mitigation:** To reduce MitM attacks, strong encryption and authentication procedures must be used. WiFi Protected Access 3 (WPA3) offers stronger encryption and personalized data encryption, as well as improved security for wireless networks. Furthermore, by encrypting all data exchanged over the WiFi network, the use of a Virtual Private Network (VPN) can add adegree of security.

Eavesdropping/Interception:

A WiFi network's lax security could be used by an unauthorized party to listen in conversations between the robot and the control node. The data may be directly interpreted if sufficient security steps weren't taken, which could result in data breaches.

- **Threat mitigation:** Using robust, modern encryption is essential for preventing eavesdropping. WPA3 offers great security, but WPA2 with a strong and distinctive passphrase should be used in cases when WPA3 is not an option. It's critical to regularly update these passphrases and to follow solid security procedures.

Physical Attacks

These include any sort of physical manipulation, from tampering with hardware to taking data from memory, with the robot or the WiFi network.

- **Threat mitigation:** It is essential to implement tamper-detection techniques and to provide secure physical storage for the WiFi and robot equipment. Access to these gadgets physically should be closely regulated and observed.

Communication denial by means of wireless interference and jamming

The goal of this kind of assault is to interfere with the WiFi connection, cutting off communication between the robot and the control node. A device that fills the area with radio signals at the same frequency as the WiFi network may be used by the attacker to effectively drown it out.

- **Threat mitigation**: Frequency hopping techniques, in which the robot and the control node quickly flip between various frequency channels to communicate, can be utilized to neutralize this threat. Additionally, it is possible to identify and pinpoint the sources of radio interference by using Wireless Intrusion Prevention Systems (WIPS).

Malware Attacks

An attacker could seize control of the system, steal confidential data, or interfere with its operation if they are successful in inserting malware into the robot or the control node.

- **Threat mitigation:** Using up-to-date antivirus and antimalware software, making sure that the boot processes are secure, and implementing network security measures like firewalls and IDS/IPS systems can help prevent the entry of malware and lessen its consequences if it already exists on the system.

4 Secure Data Communication and Networking Infrastructure

4.1 Importance of Secure Data Communication and Networking Infrastructure

The need for secure data communication and networking infrastructure in today's linked digital landscape cannot be emphasized. Organizations rely largely on the efficient exchange of data across diverse systems, devices, and users. However, this dependency introduces possible risks and vulnerabilities that can jeopardize data confidentiality, integrity, and availability. As shown in Figure 1 below the overall system will include different communication protocols for the components of the Heron project so the data exchange and the Secure Data Communication layer must ensure this information stays secure. In this section, we emphasize on the need of having a secure data communication and networking infrastructure.

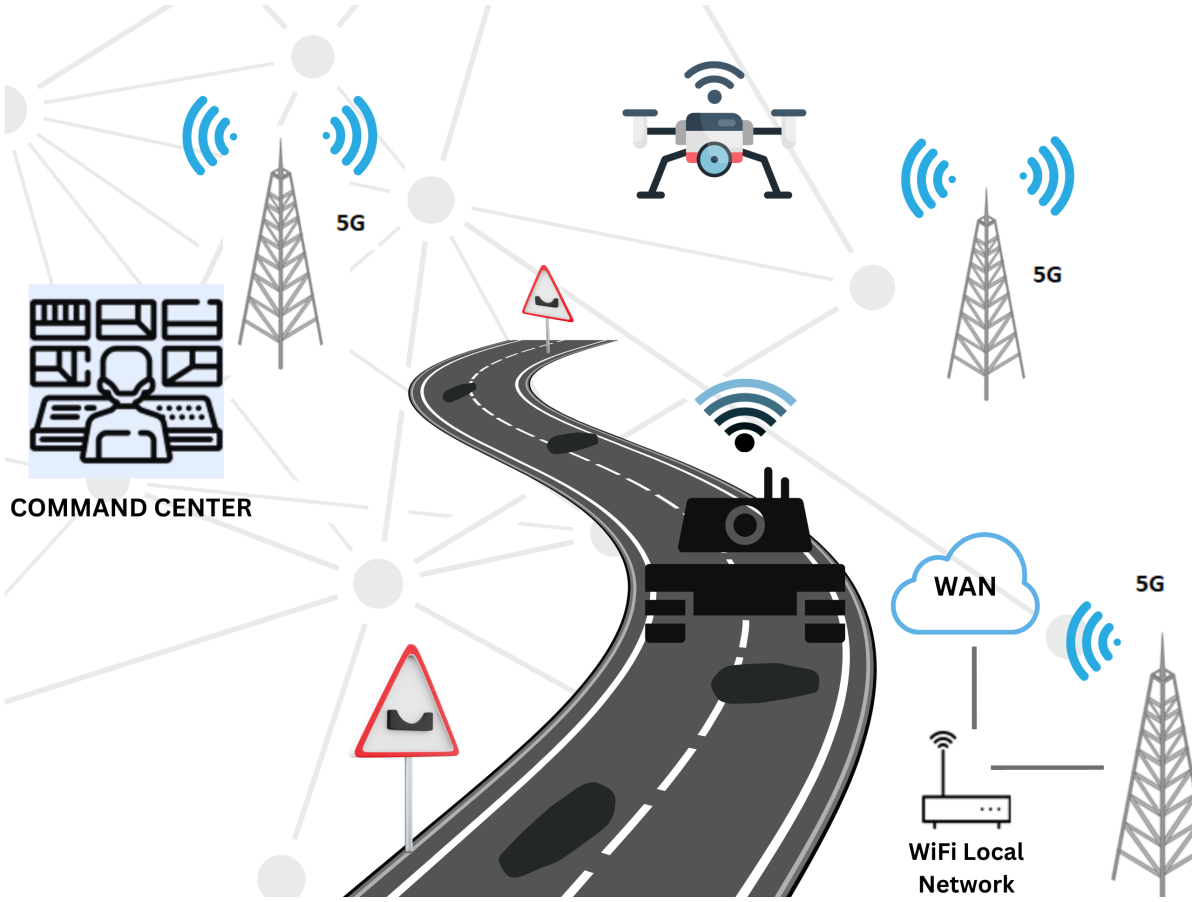

Figure 1: Communication protocols between components

Confidentiality

Secure data connection ensures that sensitive information is kept private and available only to authorized individuals or systems. Data can be protected during transmission by using encryption protocols such as SSL/TLS, preventing unlawful interception and eavesdropping. Confidentiality protects sensitive data, such as personal information, financial transactions, and intellectual property, from unauthorized access and data breaches.

Integrity

Data integrity is critical for ensuring the correctness and dependability of information. Mechanisms are used in secure data transfer and networking architecture to detect and prevent

data tampering or unwanted modifications during transmission. Digital signatures and hash algorithms, for example, aid in verifying the integrity of data, guaranteeing that it remains unchanged and trustworthy throughout the communication process.

Authentication
A solid networking infrastructure contains systems for validating the identity of communication entities. Authentication protects against illegal access and guarantees that data is only shared between trustworthy and confirmed sources. Mutual authentication can be performed by using protocols such as SSL/TLS, which allows both sides to confirm each other's identities before creating a secure connection.

Availability
Data and service availability are also addressed by a secure networking infrastructure. Distributed and fault-tolerant systems, such as Kafka clusters, ensure that data remains available even when hardware or network faults occur. Mechanisms such as redundancy, replication, and load balancing contribute to high availability and fault tolerance, reducing downtime and providing continuous access to vital data.

4.2 IoT Communication Security: Protocols for Securing Data Exchanged Between IoT Devices

4.2.1 Transport Layer Security (TLS)
TLS is a commonly used cryptographic technology for establishing secure network communication channels. It includes encryption, integrity, and authentication techniques to safeguard data sent between IoT devices. TLS verifies the validity of devices through digital certificates and secures data with symmetric encryption methods. It protects against eavesdropping and data manipulation by ensuring end-to-end encryption.

4.2.2 Datagram Transport Layer Security (DTLS)
DTLS is a TLS variant built for datagram-based communication protocols such as UDP (User Datagram Protocol). Because IoT devices frequently use UDP for lightweight, real-time connectivity, DTLS is an appropriate solution for securing IoT communication. It has similar encryption and authentication features to TLS while accounting for the unreliability of UDP connection.

4.2.3 Message Queuing Telemetry Transport (MQTT) with SSL/TLS
MQTT [7] is a lightweight communications protocol that is widely used in Internet of Things (IoT) applications. The communication between IoT devices and MQTT brokers can be secured by integrating MQTT with SSL/TLS. To ensure confidentiality, integrity, and authentication, MQTT transmission is encrypted using SSL/TLS. MQTT over SSL/TLS allows for secure and dependable communication between IoT devices and the central MQTT broker.

4.2.4 Secure Shell (SSH)
SSH is most commonly known for providing secure remote access, but it may also be used to provide secure communication channels between IoT devices. To authenticate devices and establish encrypted connections, SSH uses public-key cryptography. It supports secure shell

access, file transfers, and tunnelling, making it appropriate for secure IoT connection in certain applications.

4.2.5 IPsec (Internet Protocol Security)

IPsec (Internet Protocol Security) is a network layer security protocol that operates at the IP (Internet Protocol) level. It provides authentication and encryption services to ensure safe end-to-end communication between IoT devices by securing the complete IP packet. IPsec can be applied at the network infrastructure level, providing security for all network devices.

TLS, DTLS, MQTT with SSL/TLS, SSH, or IPsec, for example, assist protect IoT communication from unauthorized access, data interception, and alteration. Consider the unique requirements of your IoT ecosystem, such as the level of security, performance impact, and compatibility with your IoT devices and network infrastructure, when selecting an encryption protocol for IoT communication.

4.3 Architecture

Kafka [8] is a distributed streaming system for handling large-scale, high-throughput, and fault-tolerant data streams. Its architecture is built on the publish-subscribe model, in which producers publish messages to topics and consumers subscribe to those topics in order to receive those messages. Here's an overview of the Kafka architecture (Figure 2):

Topics

Kafka divides data into topics, which are logical groupings or records streams. Messages are published to certain subjects by producers, while consumers consume those messages by subscribing to specific topics. The partitioning of topics enables scalability and parallel processing.

Brokers

Kafka is a distributed system that uses a cluster of servers known as brokers. Each broker is in charge of a fraction of the overall data and provides topic partition storage and replication. Brokers are scalable and fault-tolerant, and they may be added or deleted from a cluster without interfering with the data flow.

Producers

The producers are in charge of publishing messages to Kafka subjects. They assign records to topics and partition them within topics. Producers can specify the partition manually or use the default partitioning approach, which is based on key hashing.

Consumers

Consumers read messages from partitions and subscribe to subjects. To allow for parallel processing, each consumer is assigned to one or more partitions inside a subject. Consumers can read messages at their own leisure and keep track of the reading progress using offsets.

ZooKeeper

ZooKeeper [9] is used by Kafka to coordinate clusters, manage configuration, and elect leaders. It also manages the Kafka brokers, topics, partitions, and consumer groups.

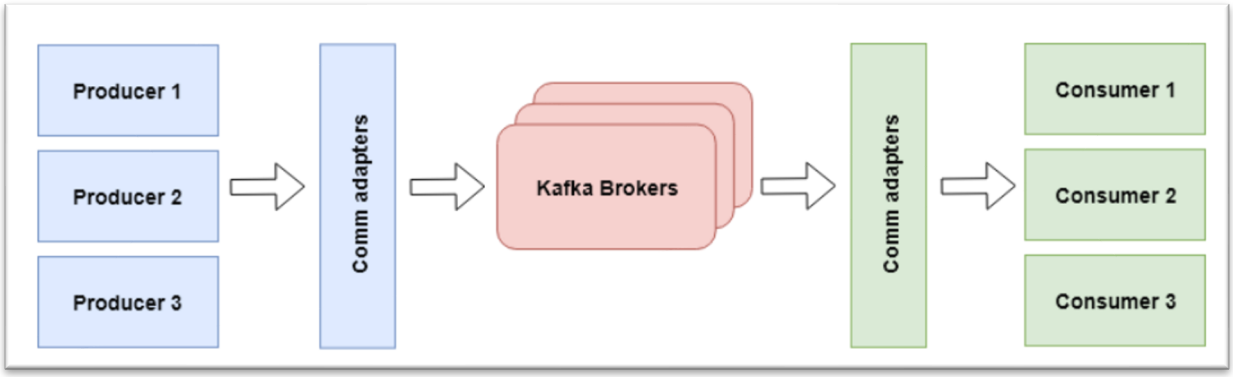

Figure 2: Kafka architecture

5 Infrastructure and Deployment setup

5.1 Ubuntu remote server

This section focuses on the architecture and deployment configuration required to create a safe and dependable environment for the Kafka cluster, which includes an Ubuntu remote server, a VPN connection, and the Kafka cluster itself for publishing and subscription operations.

5.1.1 Server Deployment

The infrastructure installation starts with the installation of an Ubuntu remote server. For hosting the Kafka cluster, an Ubuntu server provides a robust and secure operating system. The remote server should have enough resources to manage the predicted workload, such as enough CPU, memory, and storage space.

Furthermore, to reduce any vulnerabilities and unauthorized access, it is ensured that the remote server is correctly configured with up-to-date software packages, security updates, and firewall settings.

5.1.2 Hardware Specifications

The performance and stability of the server hosting the Kafka cluster are critical for the system's efficient operation. To achieve the best performance and dependability, this section provides the recommended hardware specifications for the server’s memory, CPU, and hard drive.

Sufficient memory is required to satisfy the Kafka cluster's data storage and processing requirements. A minimum of 8GB of RAM is recommended for a basic Kafka configuration. However, the actual memory requirement may differ based on factors such as projected message throughput and data size. It is recommended to assign more RAM, such as 16GB or more, to ensure smooth functioning, especially when dealing with big message volumes or high-traffic circumstances.

The processor is in charge of handling the Kafka cluster's processing requests. To ensure efficient message handling and processing, a multi-core CPU with a high clock speed is suggested. Processors with at least four cores or greater are recommended. For the needs of the project, 4 VCPUs were used to allocate resources.

The storage capacity and performance of the Kafka cluster have a direct impact on message storage and retrieval. It is advised to use a high-capacity Hard Disk Drive (HDD) or a Solid-State Drive (SSD) with sufficient storage space. The actual storage capacity required is determined by factors such as estimated message volume and retention period. The disk used for the Kafka cluster is 500GB.

5.2 VPN Connection

A VPN connection is used to establish secure communication between the client and the Kafka cluster. A VPN establishes an encrypted tunnel across the public internet, protecting data privacy and integrity.

To establish a secure connection, both the Ubuntu remote server and the client devices must be configured, establishing Virtual Private Network (VPN) protocols such as OpenVPN or IPsec, producing and exchanging VPN certificates or shared keys, and establishing proper firewall rules to allow VPN traffic are all examples.

For the needs of the project, the WireGuard VPN [10] has been installed in the server by running some basic Linux commands. After the configuration, all the clients could connect to Kafka and publish or consume data.

5.3 Kafka Cluster for Publish and Subscribe

A Kafka cluster is created as part of the deployment preparation to support publish and subscribe activities. Multiple Kafka brokers collaborate to handle message storage, replication, and data delivery in the Kafka cluster.
Apache Kafka is being installed and configured on the Ubuntu remote server. This includes downloading the Kafka binaries, configuring configuration files (such as *server.properties*), and specifying cluster parameters like as the broker ID, port numbers, and replication factors.

To enable the publish and subscribe functionality, Kafka topics must be created. Topics are logical streams or categories that contain and consume messages. The Kafka command-line tools or programmatic interfaces can be used to build topics.

For testing purposes a topic named *heron.test.topic* in order to validate the publish and consume functionality.

5.4 Securing Kafka Cluster

It is critical to secure the Kafka cluster in order to safeguard data confidentiality, integrity, and authentication. This section focuses on the security procedures and configurations needed to assure the Kafka cluster's security.

5.4.1 SSL/TLS Configuration

SSL/TLS encryption is essential for securing communication between clients and Kafka brokers. This entails creating SSL/TLS certificates, establishing SSL/TLS properties in the *server.properties* file of the Kafka broker, and enabling SSL/TLS encryption for communication. Data transferred between clients and brokers is encrypted when SSL/TLS is enabled, protecting it from illegal access and eavesdropping.

```
#    FORMAT:
#      listeners = listener_name://host_name:port
#    EXAMPLE:
#      listeners = PLAINTEXT://your.host.name:9092
#listeners=PLAINTEXT://10.2.0.10:9092
listeners=PLAINTEXT://10.2.0.10:9092,SSL://10.2.0.10:9093
```

Figure 3: SSL/TLS configuration

5.4.2 SSL/TLS Certificate Authentication

To validate the identity of clients connected to the Kafka cluster, enable SSL/TLS certificate authentication. This ensures that only clients with valid and trusted certificates can connect to the server. Unauthorized clients are prohibited from accessing the Kafka cluster by implementing certificate authentication.

The basic configuration to enable TLS certificate authentication in a *client.properties* file is necessary from the client side which should be similar to the one depicted in Figure 4 below:

```
bootstrap.servers=<broker-hostname>:<ssl-broker-port>
security.protocol=SSL
ssl.keystore.location=<path-to-client-keystore-file>
ssl.keystore.password=<client-keystore-password>
ssl.key.password=<client-private-key-password>
ssl.truststore.location=<path-to-client-truststore-file>
ssl.truststore.password=<client-truststore-password>
```

Figure 4: Client-side SSL/TLS configuration

5.5 Use of Kafka and Components Communication

The majority of the components will use the Kafka cluster which will handle the communication among them. The Kafka cluster will allow the various components to either publish their data on various topics, while other components may act as consumers who subscribe to one or more topics and consume incoming messages.

Different topics are created, based on their information. So the component which wants to have access to only traffic data will subscribe to the dedicated topic and gather the information needed. The same applies to all sensors and services which will use the Kafka cluster (e.g., UAV, UGV, Robotic systems, etc). Most of the data provided for both pilots by the CI operators are meteorological data, traffic data, message signs, and data regarding safety elements.

All components will be connected to the VPN network allowing secure communication. All services will be deployed in a pilot-specific server and the sensors or small vehicles (such as robots or UAVs) should use WiFi to send their produced data to the corresponding Kafka topics. Consequently, the data will be gathered for further processing. The latter will be performed in the middleware component which will provide to higher-level components the needed data.

Examples of HERON components that will communicate using the Kafka (based on the architecture provided in Figure 1Figure 2Figure 2: Kafka architecture) and VPN infrastructures are the following:

- Data from CI operators legacy systems (e.g. traffic data) will be transferred to HERON middleware layer for further processing, sending the later ones send through Kafka HERON consuming components by (e.g. ENGAGE COP-IMS platform)
- CI operator will manage a mission by sending respective information from the ENGAGE COP-IMS platform to the High Level Planner (HLP), through Kafka. For example they will actually send operating commands to the UGV

5.5.1 Topics

Within the HERON project, several topics that will be used for data exchange between the components will be created. Based on the current needs and technical development activities, those that are in place are listed in the table below. This is an initial version of the topics format (*project.tool.type-of-data*) which is subject to change in the future given additional requirements that may be identified.

Table 1 Initial version of HERON Kafka topics

Topics
heron.middleware.traffic-data
heron.middleware.meteo-data
heron.middleware.dynamic-message-signs
heron.middleware.maintenance-work-schedule
heron.middleware.inventory-data
heron.middleware.traffic-signs
heron.middleware.safety-elements
heron.middleware.engage-mission-commands

6 Conclusions

In D6.1 we analyse and identify the requirements arising from the most common EU Directives on Privacy and Cyber Security, namely the GDPR, NIS and e-Privacy directive along with their specific guidelines of interest to HERON. We discussed the key threats that might occur in a data communication network (focusing on the needs of the project) as well as how we can be prepared against them and mitigate the risk. Thereafter, we analyze the overall infrastructure (i.e., primarily the Kafka cluster, which handles all the necessary data flow from each component which make available through topics) and how this will provide a secure way for the components to exchange data. The server in which all the services and the Kafka will be deployed in each pilot will communicate via secure channels using TLS/SSL configuration not allowing third parties services to interfere. Moreover, VPN is introduced as a step further strengthening the overall infrastructure security of the communication between the HERON components.

References

1. General Data Protection Regulation (GDPR) – Official Legal Text. (2022, September 27). General Data Protection Regulation (GDPR). https://gdpr-info.eu/
2. Wolford, B. (2022). What are the GDPR consent requirements? GDPR.eu. https://gdpr.eu/gdpr-consent-requirements/
3. Rights of the Individual. (GDPR). European Data Protection Supervisor. https://edps.europa.eu/data-protection/our-work/subjects/rights-individual_en#:~:text=The%20GDPR%20has%20a%20chapter,decision%20based%20solely%20on%20automated
4. Art. 33 GDPR – Notification of a personal data breach to the supervisory authority - General Data Protection Regulation (GDPR). (2018, March 29). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-33-gdpr/
5. NIS Directive. (EU). ENISA. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new
6. EUR-Lex - 32002L0058 - EN - EUR-Lex. (EU). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
7. MQTT - The Standard for IoT Messaging. (n.d.). https://mqtt.org/
8. Apache Kafka. (Apache). Apache Kafka. https://kafka.apache.org/
9. Apache ZooKeeper. (Apache). https://zookeeper.apache.org/
10. Wireguard (Wireguard). WireGuard: fast, modern, secure VPN tunnel. https://www.wireguard.com/