ArtEmis

funded by the European Union

Awareness and resilience through European multi sensor system

Deliverable 3.1 – Requirement Specification of Network Platform

Version 1.0 – 31/08/2023

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or of the European Commission-Euratom. Neither the European Union nor the granting authority can be held responsible for them.

Document type	Deliverable
Document number	3.1 version 1.0
Document title	Requirement Specification of Network Platform
Authors	Peter Sjödin and Mats Nilson
Release date	31/08/2023
Contributing partners	KTH, GSI
Dissemination level	Public

Version	Short description	Main author	Coordinator
1	First release	P. Sjödin (KTH) 31/08/2023	A. Nyberg (KTH) 31/08/2023

Abstract

This document describes the requirement specification of the communication controller, *gateway*, that connects a sensor to cloud servers on the Internet. The document specifies the communication technologies to be used between the sensor system and the gateway, and between the gateway and the cloud servers.

The gateway is designed to have an external power supply, which allows for a variety of external power sources. It is also weather-proof, so that it can be located outdoors.

A prototype gateway design will be developed and made available for testing and evaluation together with the sensor system. Proper operation of the communication between sensor system and gateway will be validated, as well as communication between gateway and cloud sensors.

Table of contents

Disclaimer 2
Abstract 3
Table of contents 4
1 Introduction 5
2 Requirement Specification 6
2.1 Gateway and Sensor 6
2.2 Internet Connectivity 7
2.3 Gateway and Server Communication 7
3 Timeline 8

1 Introduction

This document specifies the requirements for the network platform of the artEmis project, to be developed and realized in WP3. The purpose of the network platform, henceforth referred to as the *gateway*, is to provide connectivity to the sensor system developed in WP1, in order to provide means for the delivery of sensor data to servers in the Internet "cloud", and to allow remote control and monitoring of sensors.

A gateway is located in the vicinity of a sensor system. The communication between the gateway and the sensor system takes place using short-range, wired communication technology. The long-range connection to the Internet should rely primarily on narrowband 4G and 5G mobile communication. Other means of Internet connectivity could also be used if available, such as Wireless LAN and LAN.

The main components of a gateway are processor, RAM memory, and I/O ports for short-range and long-range communication. The gateway should take its electrical power from an external power supply, thereby supporting a wide range of power sources: grid power outlet, power bank, solar panel, etc. The gateway should be possible to place outdoors, with a weather-proof casing. Furthermore, the gateway should have low cost, and sufficiently low energy consumption to allow off-grid operations.

The gateway reads data from the sensor and sends the data to Internet servers. To compensate for delays and interruptions in communication, the gateway should store sensor data internally in buffers until the data can be delivered to the server (or servers). Moreover, the gateway should allow for remote configuration and monitoring by accepting configuration commands from the Internet, and perform the commands either on the gateway itself or on the sensor system.

Communication with the gateway and its associated sensor system should be carried out using open standardized protocols for Internet-of-Things applications. The data format for sensor data should be based on open standards, and, to facilitate prototype development and testing, primarily be a text-based format (not binary).

Communication between Internet servers and a gateway and its associated sensor system must be reliable and secure. Therefore, transactions between gateways and servers should be protected.

An overview of a complete system with radon sensors, gateway, and cloud servers, as well as the various technologies used for communication between them, is shown in Figure 1.

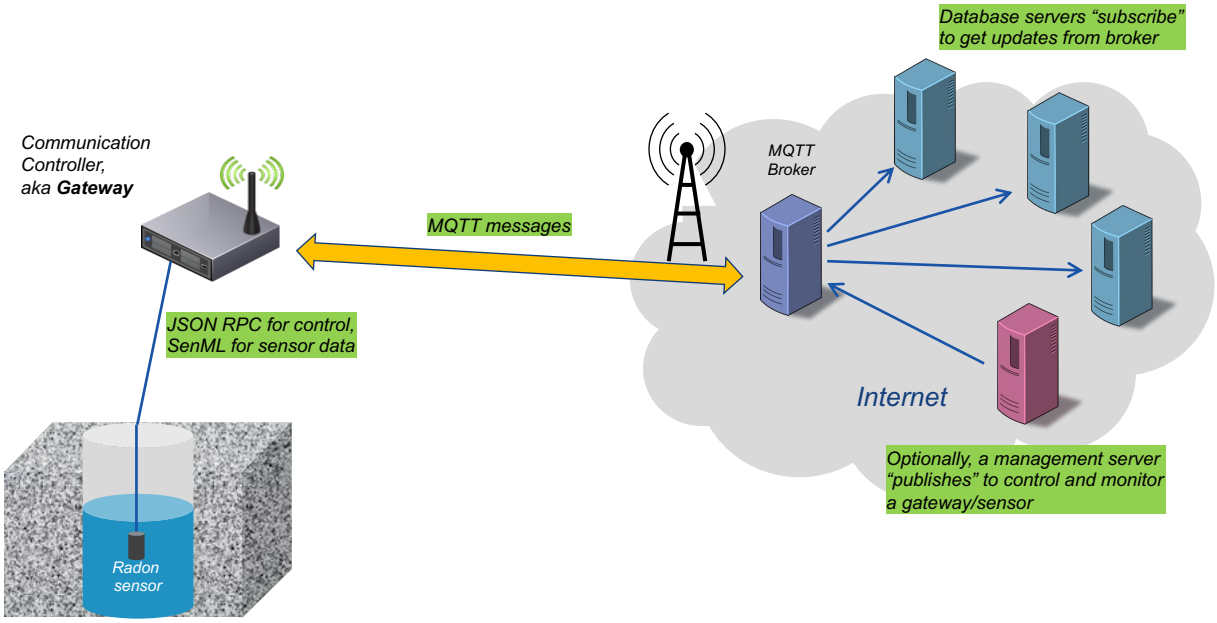

Figure 1: A complete system with radon sensors, gateway, and cloud servers

2 Requirement Specification

This section gives the requirement specifications for communication between sensor system and gateway and for communication between gateway and Internet servers.

2.1 Gateway and Sensor

The communication between gateway and sensor takes place over a RS-485 serial link. The requirements for communication and environment protection are shown in Table 1 and Table 2.

Communication	Protocol	Comment
Physical connection	RS-485 over twisted-pair cable	Point-to-point connection. Up to 20 m. (100 m and above should be possible)
Data link	Serial asynchronous half-duplex	Polling: gateway initiates communication.
Sensor control and monitoring	JSON-RPC	Gateway is RPC client; sensor is RPC server. Text encoding (UTF-8).
Sensor data	SenML	JSON/text encoding (UTF-8).

Table 1: Gateway to sensor communication

Property	Description
Dimension	200x120x60 mm
Material	ABS
Protection class	IP65

Antennas	Internal
Mechanical mount	TBD
Power supply	USB-C
Power feed for radon sensor	12 – 30V tentatively, combined with RS-485 twisted-pair cable

Table 2: Gateway enclosure

2.2 Internet Connectivity

The available communication technologies for connecting a gateway to the Internet are expected to vary between locations. Therefore, the gateway should support a variety of standards. Table 3 shows connection methods.

Technology	Comment
LTE-M	Cat M1 or Cat M2, Subscription required (nano-SIM)
NB-IoT	CAT NB1 or Cat NB2, Subscription required (nano-SIM)
GPRS	2G (GSM), Subscription required (nano-SIM)
IEEE 802.11	Wireless LAN (“Wi-Fi”) IEEE 802.11 b/g/n
IEEE 802.3	Ethernet 100 Mb/s

Table 3: Internet connection methods

2.3 Gateway and Server Communication

There are two types of communication between gateway and servers: control communication and sensor reports. The application protocol is MQTT, so all communication is between an MQTT server (broker) and a gateway.

It is expected that gateways are located behind NAT (Network Address Translation) devices, so gateways are not directly reachable from the public Internet. Therefore, communication must always be initiated by the gateway so that an address mapping is established in the NAT device. For this purpose, MQTT should be used for communication, with JSON-RPC commands carried as payload in MQTT publish messages. Both MQTT over TCP and MQTT-SN over UDP should be supported. The protocols are summarised in Table 4.

Application Protocol	Transport Protocol	Comment
MQTT	TCP	
MQTT-SN	UDP	MQTT-SN to MQTT gateway

Table 4: Application and transport protocols

A gateway should be able to act both as an MQTT publisher and as an MQTT subscriber. A gateway is an MQTT publisher when it sends sensor data, and when it responds to JSON RPC requests. It is an MQTT subscriber when it receives JSON RPC requests. The communication is summarized in Table 5.

Message	JSON RPC	MQTT	Comment

Control request	Request	MQTT subscribe	
Control response	Response	MQTT publish	
Sensor report	Notification	MQTT publish	

Table 5: Message exchanges

3 Timeline

Table 6 shows the timeline for planned variants of the gateway.

Variant	Date	Comment
Lab prototype with limited functionality	M11	At KTH
Lab prototype with complete data flow	M13	At KTH
First prototype for 2G/4G	M13	At KTH and GSI
Prototypes for selected test sites	M15	6 units
Further prototypes available	M16	

Table 6: Timeline