FLAMMABLE GAS ANALYZER

Distance communication

SUMMARY

Development of a flammable gas analysis cell featuring long-distance communication, real-time analysis, and remote visualization on an external device.

Paul VANDEWIELE

[SEE5 – 2025 : 2026]

Table des matières

Flammable gas analyzer

Introduction :

In the field of gas detection, measurements are most commonly performed using wired systems. Yet detecting flammable gases is crucial, both for private individuals and for businesses. In France alone, approximately 460 deaths per year result from house fires. With a system capable of anticipating leaks of flammable or explosive gases, a significant portion of these fatalities could be prevented.

To avoid requiring individuals or companies to undertake extensive installation work, a radio-frequency-based remote communication system represents a highly attractive solution.

General Information About Gases :

Gases are often misunderstood, and their hazards underestimated. For example, many people do not know that mixing detergent with bleach produces chlorine gas — a toxic compound responsible for numerous household accidents every year.

These dangerous situations are too often dismissed under the assumption that “it won’t happen to me.” In reality, domestic gas installations such as natural gas feeding a boiler can become a source of fire or even explosion in case of a leak. Today, there is no universal, simple system capable of warning users about such dangers.

Membrane-Based Measurement :

Flammable gases such as propane, butane, methane, and explosive gases like hydrogen can be measured using membrane-based sensor cells. Their lifespan varies depending on manufacturer specifications, with a typical maximum around five years.

When gas molecules reach the membrane, they cause a variation in the voltage output of the sensor — often in the microvolt range. Based on the sensor model, calibration, and supplier data, these signals can be converted into meaningful units.

Gas concentrations are commonly expressed in ppm (parts per million) or percentage. For very low trace concentrations, some analyzers measure in ppb (parts per billion).

Functionnal analysis :

Objectives :

The Flammable Gas Analyzer System is developed with several primary objectives in mind:

The system aims to continuously monitor and measure the concentration of various flammable gases, including methane, propane, butane, and hydrogen. This ensures that any potential gas leaks are promptly detected, providing an essential layer of safety.

Another key objective is to process and analyze gas concentration data in real-time. The system converts raw sensor readings into meaningful units, such as parts per million (ppm) or percentage, allowing for accurate and immediate assessment of gas levels.

The system is also designed to transmit data wirelessly to a remote display module. This feature enables users to monitor gas levels from a distance, providing convenience and enhancing safety by allowing real-time observation without the need for physical proximity to the gas source.

In terms of safety, the system is equipped to activate a motor that ventilates the area if dangerous gas concentrations are detected. This automatic response helps to mitigate risks by reducing gas buildup, thereby ensuring user safety.

To ensure reliability, the system is capable of functioning locally even without a WiFi connection. This means that critical safety measures remain operational regardless of the wireless communication status, providing an additional layer of security.

Finally, the system is designed to adhere to relevant standards and regulations concerning radio-frequency communication, cybersecurity, and electromagnetic compatibility. This ensures that the system operates safely, securely, and reliably in various environments, meeting international standards and regulatory requirements.

Components

To achieve these objectives, the Flammable Gas Analyzer System is structured around several key components, each playing a crucial role in its operation:

At the core of the system is the Gas Sensor Module, which is responsible for measuring gas concentration and managing sensor heating. This module comprises a gas sensor that detects the presence of flammable gases, an analog-to-digital converter (ADC) for transforming sensor signals into digital data, an ESP32 microcontroller for processing this data, and a heating element to ensure the sensor operates at optimal conditions.

The Display Module serves as the user interface of the system, presenting gas concentration levels and system status in real-time. It includes an ESP32-C6 microcontroller for processing and communication, an LCD or OLED screen for visual output, and a user interface that allows for interaction and configuration.

For wireless communication and data security, the system incorporates a Communication Interface. This component manages WiFi communication and ensures data encryption for secure transmission. It consists of a WiFi client for connecting to networks, a WiFi hotspot for creating a local network, and an HTTP/HTTPS server for handling data requests and responses.

The Motor Control component is designed to activate a motor in response to dangerous gas concentrations. This module includes a motor driver to control the motor's operation and the motor itself, which can be used to ventilate the area by opening windows or vents.

A Power Supply unit is integral to the system, providing the necessary electrical power to all components. This ensures that the system operates continuously and reliably.

Finally, the Security Subsystem is dedicated to ensuring data encryption and secure communication. This subsystem safeguards the integrity and confidentiality of data transmitted between components, protecting against unauthorized access and potential cyber threats.

Together, these components form a cohesive system that effectively detects, measures, and responds to the presence of flammable gases, ensuring safety and compliance with relevant standards.

Functionnal requirements

The functional requirements of the Flammable Gas Analyzer System are designed to ensure accurate detection, real-time analysis, remote visualization, and robust safety measures. These requirements are essential for the system's reliability, user safety, and compliance with international standards. Below is a detailed description of each category of functional requirements:

1. Detection and Measurement

The system must accurately detect and measure the concentration of flammable gases such as methane, propane, butane, and hydrogen. This involves using membrane-based sensor cells that respond to the presence of gas molecules by generating a voltage variation. The system must convert these signals into precise measurements, expressed in parts per million (ppm) or percentage, ensuring high sensitivity and accuracy.

2. Data Processing

The system must process and analyze gas concentration data in real-time. This involves converting raw sensor readings into meaningful units (ppm or percentage) through analog-to-digital conversion and microcontroller-based calculations. The system should also log and store data for historical analysis, ensuring that users can track gas concentration trends over time.

3. Wireless Communication

The system must transmit data wirelessly to a remote display module using a WiFi connection. This communication must be reliable and secure, adhering to standards such as EN 300 328 for radio frequency communication. The system should use encryption protocols (e.g., HTTPS/TLS) to ensure data integrity and confidentiality. Additionally, the system must handle potential interferences and maintain communication robustness in various electromagnetic environments.

4. User Interface

The system must display gas concentration and system status on an LCD/OLED screen, providing users with real-time information. The user interface should be intuitive and easy to navigate, allowing users to quickly understand the current gas levels and any alerts or warnings. The display module should also provide options for users to configure settings, such as adjusting alert thresholds or resetting the system.

5. Safety Measures

The system must activate a motor to ventilate the area in case of dangerous gas concentrations, ensuring user safety. This involves setting predefined thresholds for gas concentration levels. When these thresholds are exceeded, the system should automatically trigger the motor to open windows or vents, reducing the risk of fire or explosion. The system must also include audible and visual alarms to alert users of dangerous conditions.

6. Local Operation

The system must function locally even without a WiFi connection, maintaining safety measures. This means that critical functions, such as gas detection and motor activation, should continue to operate independently of the wireless communication link. The system should have a degraded mode that ensures essential safety features remain active even if the WiFi connection is lost.

7. Compliance and Security

The system must adhere to relevant standards and regulations for radio-frequency communication, cybersecurity, and electromagnetic compatibility. This includes compliance with standards such as EN 300 328 for WiFi communication, EN 303 645 for IoT cybersecurity, EN 301 489 for electromagnetic compatibility, and EN 62368-1 for health and safety. The system should implement secure communication protocols, regular firmware updates, and robust data protection measures to ensure compliance and user safety.

Standards

Finally, to ensure the proper functioning of the system in compliance with applicable standards, the Flammable Gas Analyzer System is designed according to the following key standards:

The system adheres to EN 300328 V2.2.2, which specifies the requirements for radio frequency communication. This includes the use of designated frequency bands, limitations on transmission power, and minimum bandwidth requirements to ensure reliable and interference-free wireless communication.

Additionally, the system complies with EN 303645 V2.1.1, which outlines cybersecurity requirements for IoT devices. This standard ensures secure communication through encryption protocols, mandates regular and secure software updates, and enforces data protection measures to safeguard user information and system integrity.

The system also follows EN 301489, which covers electromagnetic compatibility. This standard ensures that the system operates reliably in various electromagnetic environments, minimizing interference with other electronic devices and maintaining robust performance under different conditions.

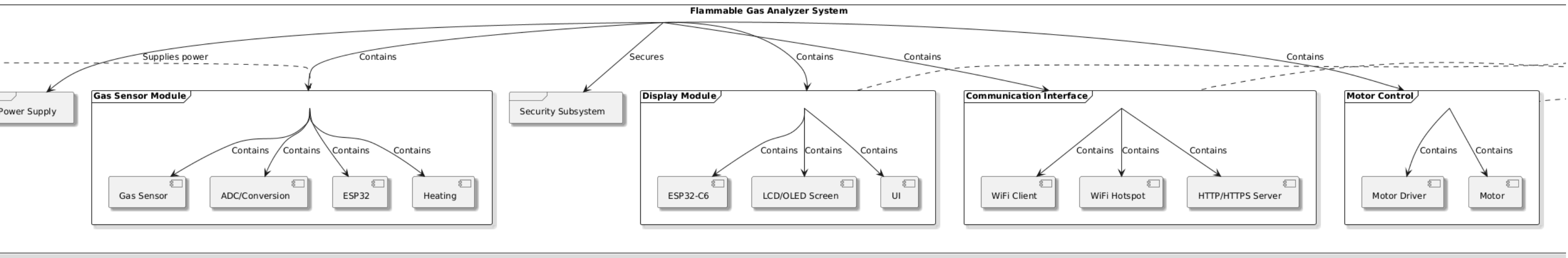
Lastly, the system is designed in accordance with EN 62368-1, focusing on health and safety requirements. This includes protection against electric shock, thermal protection to prevent overheating, and fire safety measures to mitigate risks associated with electrical and mechanical components.

By adhering to these standards, the Flammable Gas Analyzer System ensures reliable operation, user safety, and compliance with international regulations.

SYSml diagrams :

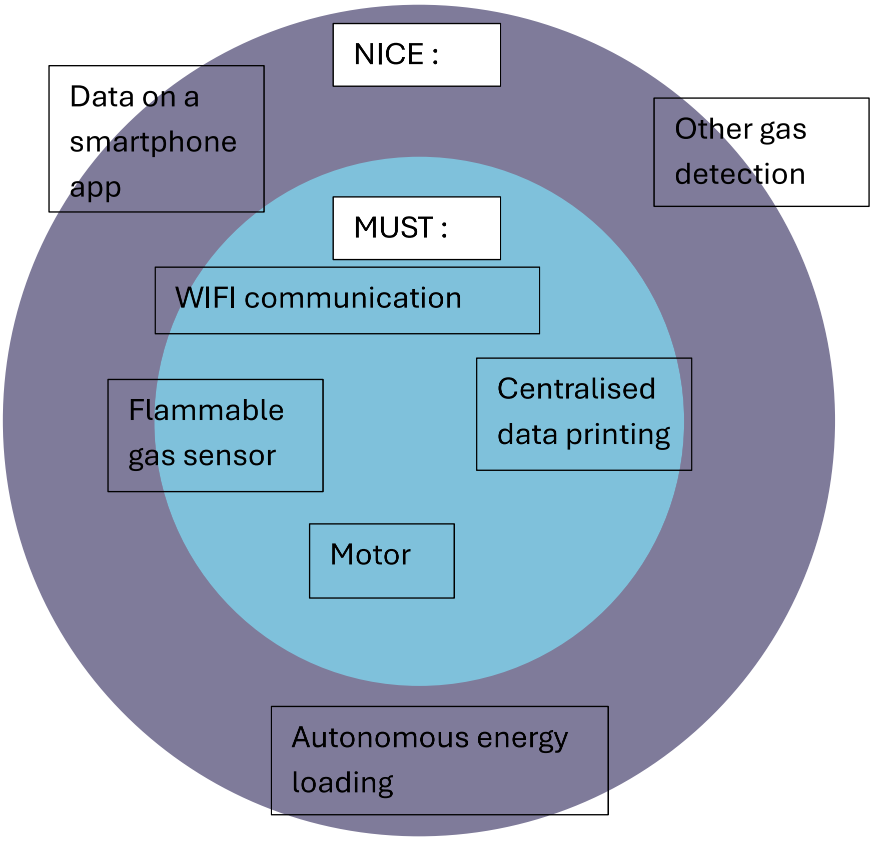
Block definition diagram

The SysML Block Definition Diagram (BDD) presented here provides a structured and visual representation of the system architecture for the Flammable Gas Analyzer. This diagram is a fundamental tool for system design, integration, and analysis, as it defines the components, their relationships, and their roles within the overall system.



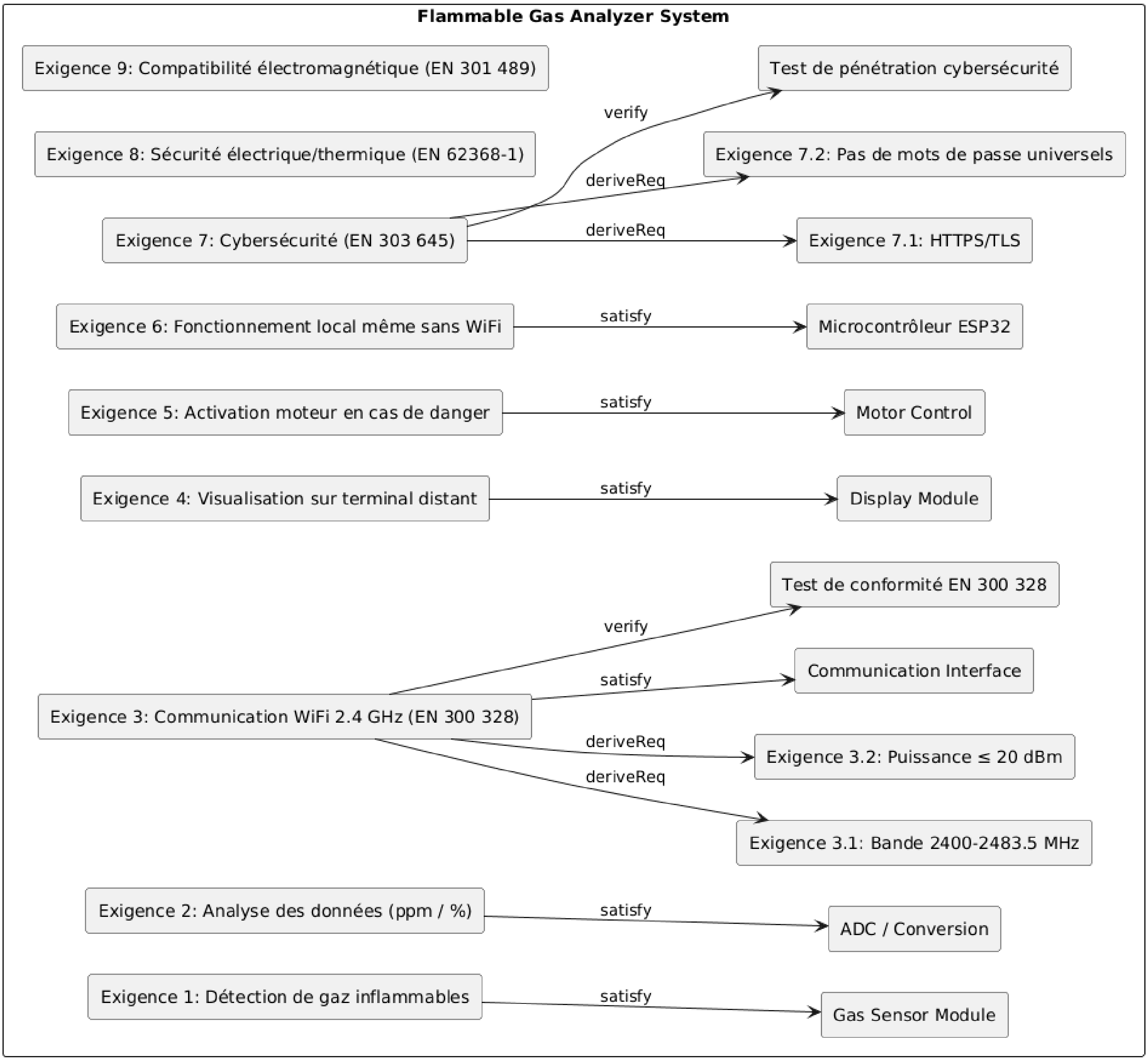
Must/Nice

The Must/Nice diagram shows what is mandatory and what can be updated or added later.



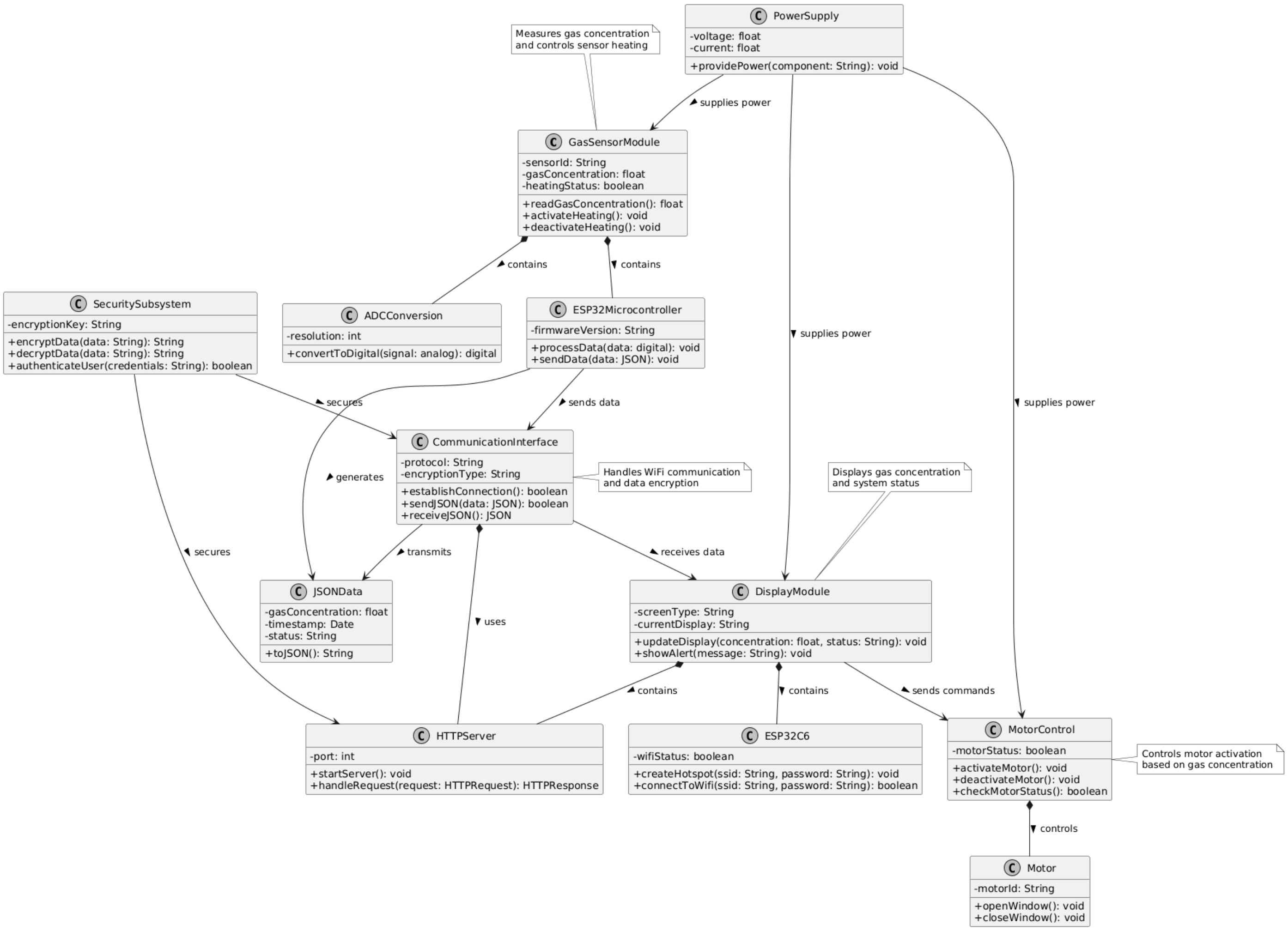
Requirements diagram :

The SysML Requirements Diagram presented here provides a structured and visual representation of the key system requirements for the Flammable Gas Analyzer. This diagram serves as a critical tool for system design, validation, and compliance, ensuring that all functional and non-functional requirements are clearly defined, traceable, and linked to their respective components and verification methods.


Flammable Gas Analyzer System
Exigence 9: Compatibilité électromagnétique (EN 301 489)
Test de pénétration cybersécurité
verify
Exigence 8: Sécurité électrique/thermique (EN 62368-1)
Exigence 7.2: Pas de mots de passe universels
deriveReq
Exigence 7: Cybersécurité (EN 303 645)
deriveReq
Exigence 7.1: HTTPS/TLS
Exigence 6: Fonctionnement local même sans WiFi
satisfy
Microcontrôleur ESP32
Exigence 5: Activation moteur en cas de danger
satisfy
Motor Control
Exigence 4: Visualisation sur terminal distant
satisfy
Display Module
Test de conformité EN 300 328
verify
Communication Interface
satisfy
Exigence 3: Communication WiFi 2.4 GHz (EN 300 328)
deriveReq
Exigence 3.2: Puissance ≤ 20 dBm
deriveReq
Exigence 3.1: Bande 2400-2483.5 MHz
Exigence 2: Analyse des données (ppm / %)
satisfy
ADC / Conversion
Exigence 1: Détection de gaz inflammables
satisfy
Gas Sensor Module

Class diagram :

The provided Class Diagram visually represents the object-oriented structure of the Flammable Gas Analyzer System. This diagram is a fundamental part of the system's design documentation, as it outlines the classes, their attributes, methods, and relationships within the system. It serves as a blueprint for understanding how different components interact and collaborate to achieve the system's objectives.


PowerSupply
-voltage: float
-current: float
+providePower(component: String): void
Measures gas concentration and controls sensor heating
supplies power
GasSensorModule
-sensorId: String
-gasConcentration: float
-heatingStatus: boolean
+readGasConcentration(): float
+activateHeating(): void
+deactivateHeating(): void
contains
contains
SecuritySubsystem
-encryptionKey: String
+encryptData(data: String): String
+decryptData(data: String): String
+authenticateUser(credentials: String): boolean
ADCConversion
-resolution: int
+convertToDigital(signal: analog): digital
ESP32Microcontroller
-firmwareVersion: String
+processData(data: digital): void
+sendData(data: JSON): void
supplies power
supplies power
secures
sends data
CommunicationInterface
-protocol: String
-encryptionType: String
+establishConnection(): boolean
+sendJSON(data: JSON): boolean
+receiveJSON(): JSON
generates
Handles WiFi communication and data encryption
Displays gas concentration and system status
secures
transmits
receives data
JSONData
-gasConcentration: float
-timestamp: Date
-status: String
+toJSON(): String
uses
DisplayModule
-screenType: String
-currentDisplay: String
+updateDisplay(concentration: float, status: String): void
+showAlert(message: String): void
contains
contains
sends commands
HTTPServer
-port: int
+startServer(): void
+handleRequest(request: HTTPRequest): HTTPResponse
ESP32C6
-wifiStatus: boolean
+createHotspot(ssid: String, password: String): void
+connectToWifi(ssid: String, password: String): boolean
MotorControl
-motorStatus: boolean
+activateMotor(): void
+deactivateMotor(): void
+checkMotorStatus(): boolean
Controls motor activation based on gas concentration
controls
Motor
-motorId: String
+openWindow(): void
+closeWindow(): void

Use case :

The use cases down bellow are designed to have an idea of how the system shall react in different situations. Normally, we should have a lot of use cases but just a few are writen here.

Use Case ID	Use Case Name	Actor(s)	Description	Precondition	Main Flow	Postcondition
UC01	Detect Flammable Gas	System, User	The system continuously monitors the environment for flammable gases.	The system is powered on and the gas sensor is operational.	1. The gas sensor detects gas concentration. 2. The system processes the sensor data. 3. If the gas concentration exceeds a predefined threshold, the system triggers an alert.	The user is alerted to the presence of flammable gas.
UC02	Measure Gas Concentration	System	The system measures the concentration of flammable gases in ppm or percentage.	The gas sensor is active and calibrated.	1. The gas sensor reads the analog signal. 2. The ADC converts the analog signal to a digital value. 3. The microcontroller processes	The gas concentration is displayed on the user interface.

					the digital value to determine the gas concentration.	
UC03	Activate Heating Element	System	The system activates the heating element of the gas sensor to ensure accurate readings.	The system is powered on.	1. The microcontroller sends a command to activate the heating element. 2. The heating element reaches the required temperature.	The gas sensor is ready to provide accurate readings.

Specifications - normes :

Standards play a critical role when designing systems involving radio-frequency communication. The tables below summarize the normative requirements applied to this flammable gas detector project.

Norme EN 300 328 V2.2.2 – radio frequency :

1. STANDARD EN 300 328 V2.2.2 - RADIO FREQUENCY			
WiFi Transmission 2.4GHz - MANDATORY Directive RED 2014/53/EU Article 3.2			
FREQUENCY BAND AND SPECTRAL OCCUPATION			
Complete Title	**Standard Number/Paragraph**	**Regulatory Requirement**	**Application to Functional Need**
Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz band	EN 300 328 V2.2.2 Clause 4.2.1	Mandatory frequency band: Transmission between 2400 MHz and 2483.5 MHz / Reception between 2400 MHz and 2483.5 MHz	BIDIRECTIONAL COMMUNICATION: The WiFi hotspot and data transmission between the two modules must operate strictly within this band. This concerns: (1) Transmission of gas data from sensor module to display module (2) WiFi hotspot created by display module (3) Possible HTTP responses/acknowledgments
Wideband transmission systems	EN 300 328 V2.2.2 Clause 4.3.1.1	Minimum frequency occupation of 20 MHz for non-adaptive equipment	BANDWIDTH: The chosen transmission technology (WiFi 802.11b/g/n/ac) must occupy at least 20 MHz of bandwidth per channel for compliance
TRANSMISSION POWER - CRITICAL			
Wideband transmission systems	EN 300 328 V2.2.2 Clause 4.3.1.3	Maximum Equivalent Isotropically Radiated Power (EIRP): 20 dBm (100 mW) for non-adaptive equipment	SENSOR TRANSMITTER: The module transmitting gas data must NOT exceed 20 dBm EIRP. WIFI HOTSPOT: The WiFi access point must NOT exceed 20 dBm EIRP. Requires measurement in accredited laboratory taking into account antenna gain
Wideband transmission systems	EN 300 328 V2.2.2 Clause 4.3.1.4	For non-adaptive equipment: Limitation of Medium Utilization (MU) factor or obligation to use LBT/DAA if MU > 10%	GAS DATA TRANSMISSION FREQUENCY: If continuous transmission >10% of time → EITHER limit the frequency of gas measurement transmission, OR implement Listen Before Talk mechanism to verify channel is clear before transmission
SPURIOUS EMISSIONS - NEW LIMITS V2.2.2			

Wideband transmission systems	EN 300 328 V2.2.2 Clause 4.3.1.10.3	Band 694-862 MHz: Limit at -36 dBm/100kHz (REINFORCED in V2.2.2, was less strict before)	ACTUATOR MOTOR: Electric motors generate EM disturbances that can create harmonics in this band (4G/5G LTE frequencies). MANDATORY TEST: Motor operating + WiFi active simultaneously. EMC filtering necessary (ferrites, capacitors, shielding)
Wideband transmission systems	EN 300 328 V2.2.2 Clause 4.3.1.10.3	Band 470-694 MHz: Limit at -54 dBm/100kHz	ANALOG GAS SENSOR: Gas sensor heating circuits (MQ require 5V heating) and analog measurement circuits can generate RF noise. Design: analog/digital separation, filtering, shielding
Wideband transmission systems	EN 300 328 V2.2.2 Clause 4.3.1.10.3	Band 1-12.75 GHz: Limit at -30 dBm/MHz	WIFI 2.4GHz HARMONICS: The 2nd and 3rd harmonics of WiFi signal (4.8 GHz, 7.2 GHz) fall within this band. Mandatory RF filtering, careful antenna routing, tests in anechoic chamber
RECEIVER BLOCKING - MAJOR CHANGE V2.2.2			
Complete Title	**Standard Number/Paragraph**	**Regulatory Requirement**	**Application to Functional Need**
Wideband transmission systems	EN 300 328 V2.2.2 Clause 4.3.1.12.4	Blocking signal level: -34 dBm for ALL receiver categories (NEW - old standard: -47/-53 dBm)	COMMUNICATION ROBUSTNESS: WiFi receivers (display module receiving data, sensor module receiving hotspot) must maintain reliable communication even in presence of interference at -34 dBm. CRITICAL for residential environment with multiple WiFi. Test with spurious signal generator mandatory
Wideband transmission systems	EN 300 328 V2.2.2 Clause 4.3.1.12.3	Performance criterion: Packet Error Rate (PER) or Frame Error Rate (FER) ≤ 10% during blocking test	GAS DATA RELIABILITY: During tests, transmission of gas concentration values must maintain PER ≤10% even with interference. Important for safety alarms
ADAPTIVE MODES (IF APPLICABLE)			
Complete Title	**Standard Number/Paragraph**	**Regulatory Requirement**	**Application to Functional Need**

Wideband transmission systems	EN 300 328 V2.2.2 Clause 4.3.1.5	Adaptive equipment: Listen Before Talk (LBT) mechanism with Clear Channel Assessment or Detect and Avoid (DAA)	IF ADAPTIVE TECHNOLOGY CHOSEN: System must detect occupied channels and avoid transmitting. Useful for coexistence with other domestic WiFi. Validation tests of LBT/DAA mechanism mandatory
Wideband transmission systems	EN 300 328 V2.2.2 Clause 5.4.6	Tests verifying adaptive mechanisms: Verify correct detection of channel occupation and channel switching/deferral	FUNCTIONAL TESTS: If adaptive system, demonstrate that detection of other WiFi works and system changes channel or waits

Norme EN 303 645 V2.1.1 – cybersecurity IoT :

2. STANDARD EN 303 645 V2.1.1 - IoT CYBERSECURITY			
Consumer Internet of Things Security - 13 Categories, 68 Provisions			
5.1 - NO UNIVERSAL DEFAULT PASSWORDS			
Complete Title	**Standard Number/Paragraph**	**Regulatory Requirement**	**Application to Functional Need**
Cyber Security for Consumer Internet of Things: Baseline Requirements	EN 303 645 V2.1.1 Provision 5.1-1	Prohibition of universal default passwords. Each device must have unique identifiers or force change upon first use	WIFI HOTSPOT: SSID and WiFi password CANNOT be identical for all devices (e.g., "GasDetector/12345678" everywhere). EITHER generate unique password per device, OR force user to define own password at first startup. HTTP SERVER: If authentication on HTTP server, no universal "admin/admin"
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.1-2	If authentication required, simple mechanism for user to change credentials	USER INTERFACE: Provide means for user to change WiFi hotspot password via interface (buttons on display module, HTTP server web interface, or dedicated application)
5.2 - VULNERABILITY MANAGEMENT			
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.2-1	Public contact point for reporting security vulnerabilities	MANUFACTURER OBLIGATION: Publish email address or web form allowing security researchers/users to report discovered flaws. Provide internal handling process
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.2-2 RECOMMENDED	Vulnerability disclosure policy and correction timeline	BEST PRACTICE: Document how vulnerabilities are handled and within what timeframe (e.g., critical patches within 90 days)
5.3 - SOFTWARE UPDATES			
MANDATORY			
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.3-1	Firmware and software must be updatable securely	MICROCONTROLLERS: Both modules (sensor+motor and display) must have firmware update capability. Possible methods: (1) USB port with secure bootloader (2) Over-The-Air (OTA) update via WiFi (3) Protected programming port. Cryptographic signature of updates MANDATORY

Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.3-3	Defined support period during which updates are provided	PRODUCT LIFESPAN: Define and communicate minimum support duration (e.g., "Security updates guaranteed 5 years after purchase"). Important for safety detector
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.3-4 RECOMMENDED	Automatic update with user deferral option	OTA FUNCTIONALITY: If implemented, allow automatic updates but leave user control (e.g., notification + button "Install now/Later")
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.3-13	Verify authenticity and integrity of updates before installation	FIRMWARE SECURITY: Use digital signatures (RSA, ECDSA) to verify firmware comes from legitimate manufacturer and has not been modified. Reject any unsigned update
5.4 - SECURE STORAGE OF SENSITIVE PARAMETERS			
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.4-1	Sensitive data stored securely (credentials, cryptographic keys)	SYSTEM MEMORY: WiFi password, HTTPS encryption keys, HTTP server credentials must be stored encrypted in flash memory. Use AES-128/256 encryption. NO plain text storage accessible by memory reading
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.4-3	Cryptographic keys stored securely, protected against unauthorized access	KEY PROTECTION: Ideally use hardware secure element (secure element, TPM) or at minimum protected memory zone with hardware encryption of microcontroller
5.5 - SECURE COMMUNICATION			
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.5-1	Appropriate secure communication (encryption of sensitive data)	HTTP SERVER → HTTPS: Gas concentration data transmitted between modules must be encrypted. CRITICAL: Switch from HTTP to HTTPS (TLS 1.2 minimum). Prevents interception/modification of gas values (man-in-the-middle attack could display false values and prevent alarm)
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.5-2	Sensitive credentials must not be transmitted in clear text	AUTHENTICATION: If password for HTTP server, transmission in HTTPS only. No Basic Auth in clear HTTP

Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.5-5 RECOMMENDED	Use recognized and up-to-date cryptographic protocols (avoid SSL, TLS <1.2)	PROTOCOL CHOICE: TLS 1.2 minimum (TLS 1.3 preferable). Disable SSL, TLS 1.0, TLS 1.1 (vulnerable). Self-signed certificates acceptable for closed IoT but document risk
5.6 - MINIMIZE ATTACK SURFACES			
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.6-1	Exposed network ports and services must be minimal and justified	HTTP SERVER: Expose ONLY the HTTP server necessary for function. Disable: (1) Telnet (2) SSH if not used (3) Network debug services (4) UPnP (5) All non-essential ports. Software firewall to block unused ports
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.6-2	Unused network services must be disabled	WIFI HOTSPOT: Configure with client isolation (AP isolation) to prevent communication between devices connected to hotspot. DNS/DHCP only if necessary
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.6-7 RECOMMENDED	Physical debug interfaces disabled or protected	PROGRAMMING PORTS: If JTAG/SWD/UART accessible, protect them by: (1) Deactivation in production (2) Password protection (3) Location not accessible to user (4) Epoxy resin on connector
5.7 - SOFTWARE INTEGRITY			
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.7-1	Verifiable firmware/software integrity (secure boot)	SECURE BOOT: Microcontrollers must verify firmware signature at startup. Prevents execution of malicious firmware. If microcontroller supports, enable hardware secure boot
5.8 - PERSONAL DATA PROTECTION			
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.8-1	Personal data protected against unauthorized access	MEASUREMENT HISTORY: If system records history of gas measurements with timestamp (allows inferring presence/habits), this data is GDPR personal data. Encrypted storage mandatory
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.8-3	Data minimization (collect only necessary)	DESIGN: Do not collect/store unnecessary data. For gas detector: current concentration + recent history sufficient. No need for user profiling, geolocation, etc.
5.9 - RESILIENCE TO FAILURES			

Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.9-1	System remains operational or fails safely in case of failure	WIFI CONNECTION LOSS: If communication between modules fails, sensor module must CONTINUE to actuate motor locally in case of danger. Do NOT depend solely on WiFi link for safety. Autonomous degraded mode mandatory
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.9-2 RECOMMENDED	Telemetry data for system health monitoring	DIAGNOSTICS: Monitor: WiFi signal quality, battery/power status, sensor errors, restart counter. Display on screen or send alerts if anomaly
5.11 - EASE OF DATA DELETION			
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.11-1	User must be able to easily delete their personal data	RESET FUNCTION: Physical button or menu option to: (1) Erase measurement history (2) Reset WiFi settings (3) Return to factory configuration. Clear user documentation
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.11-3	Upon decommissioning, personal data securely deleted	DECOMMISSIONING: "Complete erasure" function overwriting flash memory (not simple deletion) before recycling/reselling device
5.12 - EASE OF INSTALLATION			
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.12-1	Secure installation and maintenance easy to perform	USER EXPERIENCE: Sensor connection process to WiFi hotspot must be simple (WPS, QR code, intuitive web interface). Clear installation documentation including security aspects
5.13 - INPUT DATA VALIDATION			
Cyber Security for Consumer IoT	EN 303 645 V2.1.1 Provision 5.13-1	Input data validation to prevent injections	HTTP SERVER: Validate all user inputs (URL parameters, POST). Prevent: (1) SQL injection if database (2) OS command injection (3) XSS on web interface (4) Buffer overflow. Sanitization + size limits mandatory

Norme EN 301 489 – electromagnetic compatibility:

3. STANDARD EN 301 489 - ELECTROMAGNETIC COMPATIBILITY			
Part 1 (General) + Part 17 (WiFi/Bluetooth) - RED 2014/53/EU Article 3.1(b)			
ENVIRONMENT AND TEST CONDITIONS			
Complete Title	**Standard Number/Paragraph**	**Regulatory Requirement**	**Application to Functional Need**
EMC standard for radio equipment and services - Part 1: Common technical requirements	EN 301 489-1 V2.2.3 Clause 4.1	Environmental profile: Equipment must function in normal and extreme conditions declared by manufacturer	ENVIRONMENT DEFINITION: Declare operating range (e.g., temperature -10°C to +50°C, humidity 10-90%, for residential use). System must be EMC compliant throughout this ENTIRE range
CONDUCTED EMISSIONS - POWER SUPPLY PORTS			
EMC standard - Part 1	EN 301 489-1 V2.2.3 Clause 7.3	Conducted emissions on DC power supply ports: Limits according to frequency bands (150 kHz - 30 MHz)	ELECTRICAL POWER SUPPLY: Both modules (sensor and display) powered by mains or batteries must not inject excessive disturbances into power cables. TESTS: (1) Sensor power supply with gas heating circuit (2) Motor power supply during actuation (3) Display power supply with screen. EMC filters (inductors, X/Y capacitors) on power supply inputs mandatory
EMC standard - Part 1	EN 301 489-1 V2.2.3 Clause 7.4	Harmonics and flicker: Reference EN 61000-3-2 and EN 61000-3-3 if mains powered >75W	IF MAINS POWERED: Window opening motor can draw significant currents. If total system power >75W, harmonics tests mandatory. Power factor correction if necessary
RADIATED EMISSIONS - EM DISTURBANCES			
EMC standard - Part 1	EN 301 489-1 V2.2.3 Clause 8.2	Radiated emissions 30 MHz - 1 GHz: Limits to avoid interference with other equipment	GAS SENSOR + MOTOR: Following elements radiate EM disturbances: (1) Sensor heating circuit (5V heating element) (2) Electric motor with brushes or PWM (3) LCD/OLED screen (pixel clock). MEASUREMENTS: Tests in anechoic chamber with entire system active (heated sensor + WiFi + motor in motion). Housing shielding, shielded cables for motor

EMC standard - Part 1	EN 301 489-1 V2.2.3 Clause 8.3	Radiated emissions 1 GHz - 18 GHz: Including radio transmitter harmonics	WIFI HARMONICS: Already covered by EN 300 328 clause 4.3.1.10.3 but double check. 2.4 GHz harmonics in 4.8 GHz, 7.2 GHz, 9.6 GHz bands
IMMUNITY - RESISTANCE TO DISTURBANCES			
EMC standard - Part 1	EN 301 489-1 V2.2.3 Clause 9.2	RF radiated immunity: 80 MHz - 6 GHz, level 3 V/m to 10 V/m depending on equipment	SYSTEM ROBUSTNESS: Exposure to EM fields (other WiFi, 3G/4G/5G mobile phones, Bluetooth, microwave ovens) must NOT: (1) Cause false gas alarms (2) Prevent motor triggering in real danger (3) Corrupt screen display (4) Block WiFi communication. TESTS: Complete system operating in TEM or GTEM chamber with RF generator sweeping all frequencies
EMC standard - Part 1	EN 301 489-1 V2.2.3 Clause 9.3	Immunity to electrical fast transients (EFT/Burst): ±1 kV on power supply ports	POWER SUPPLY PROTECTION: Power supply circuits must withstand bursts of electrical transients (electrical network parasites). Varistors (MOV), TVS diodes, RC filters on power supply inputs
EMC standard - Part 1	EN 301 489-1 V2.2.3 Clause 9.4	Electrostatic discharge immunity (ESD): ±4 kV contact, ±8 kV air	USER HANDLING: Buttons, touch screen (if present), connectors must withstand ESD (static discharges from human body). Design: (1) TVS diode protection on inputs (2) Continuous ground planes (3) Housing avoiding charge accumulation
EMC standard - Part 1	EN 301 489-1 V2.2.3 Clause 9.5	50 Hz magnetic field immunity: Continuous exposure	LOCATION: System may be installed near transformers, electrical wiring. 50/60 Hz magnetic fields must not disturb analog gas sensor or electronics
PERFORMANCE CRITERIA DURING TESTS			

EMC standard - Part 1	EN 301 489-1 V2.2.3 Clause 6	During and after immunity tests: Unacceptable loss of function or degradation beyond specifications = FAILURE	SAFETY CRITERIA DEFINITION: Establish specific performance criteria: CRITERION A (no degradation): Gas measurement remains accurate ± 10%, display functions. CRITERION B (acceptable temporary degradation): WiFi communication may be interrupted BUT must automatically recover <5s. CRITERION C (tolerable temporary function loss): Display may freeze during test BUT no dangerous action. UNACCEPTABLE: False alarm, motor non-triggering in real danger, system crash
WIFI SPECIFICS - PART 17			
EMC standard for radio equipment - Part 17: Broadband Data Transmission Systems	EN 301 489-17 V3.3.1 Clause 4.2.1	Transmitter tests: Transmission at maximum power with normal modulation	WIFI TESTS: WiFi transmitter configured in continuous transmission at max power during emission measurements. Signal representative of real usage (gas measurement data packets)
EMC standard - Part 17	EN 301 489-17 V3.3.1 Clause 4.2.3	Immunity receiver tests: Wanted signal at level 30 dB above minimum sensitivity	RECEPTION ROBUSTNESS TESTS: Simulate gas data reception with correct WiFi signal + disturbances. Verify error rate remains acceptable
EMC standard - Part 17	EN 301 489-17 V3.3.1 Table 1	Technologies covered: Wi-Fi, Bluetooth, BLE, Zigbee in 2.4 GHz	TECHNOLOGY CHOICE: If using WiFi 2.4 GHz for sensor-display communication, this part 17 applies. If choosing other 2.4GHz tech (BLE, Zigbee), verify applicability
EXCLUSION BANDS			
EMC standard - Part 17	EN 301 489-17 V3.3.1 Clause 4.3	Exclusion bands for emission measurements: ±5% around operational frequencies	MEASUREMENT INTERPRETATION: During radiated emission tests, WiFi frequencies used (2400-2483.5 MHz ±5%) are excluded. Measure only spurious emissions outside this band

Norme IEC/EN 62638-1 : Health and safety :

4. STANDARD EN 62368 - Health & Safety			
Safety requirements for audio/video, information and communication technology equipment			
Complete Title	**Standard Number/Paragraph**	**Regulatory Requirement**	**Application to Functional Need (Project: Gas detection + motor + WiFi)**
Safety requirements for audio/video, information and communication technology equipment	EN 62368-1:2020 Clause 4	Hazard source analysis (Energy Hazard, Fire Hazard, Chemical Hazard...)	Identify: (1) Heating sensor energy source, (2) Window opening motor (mechanical energy), (3) Electrical power supply, (4) Possible battery, (5) 2.4 GHz RF sources, (6) Analyzed flammable gas → classify each source to apply appropriate protections.
Energy Sources Classification	Clause 5.2 / 5.3	Classification ES1, ES2, ES3 (Energy Source Levels)	Heating sensor = ES2 (high temperature). Motor = ES2 (mechanical forces). 5–12V power supply = ES1/ES2 depending on current. Implement barriers: insulation, closed housing, no user access.
Protection against electric shock	Clause 5.4	Limit access to hazardous conductive parts; Double insulation, SELV, PELV	Internal power supply for sensor and display must be SELV < 60VDC. User-accessible connectors protected by reinforced insulation. No accessible metal point connected to circuit > ES1.
Thermal protection and overheating	Clause 7.4	Allowable temperatures for plastic/PCB; protection against user burns	Gas heating sensor (MQ element or equivalent) must NOT raise external housing temperature beyond limit values. Provide: internal ventilation, heat dissipation, UL94-V0 materials.
Fire and fire propagation	Clause 6.4	Materials must limit fire propagation; UL94-V0 or V1 ratings recommended	Sensor housing + display module housing = UL94-V0 flame retardant plastic. Motor and motor electronics must be isolated from sensor area to avoid ignition in case of fault.
Abnormal electrical stress / overvoltages	Clause 5.6.2	Product must withstand transients and internal overcurrents	Add: resettable fuse (PTC) on motor power supply + TVS protection on module DC input. Prevents fire if motor stalls.

Batteries / Locally powered circuits	Clause 4.10	Safety requirements for batteries and charging	If sensor or display module uses battery: protections against overcharge, short-circuit, excessive temperature, BMS circuits mandatory.
Mechanical protection — Moving parts	Clause 8.2	Protection against injuries related to moving parts	Window opening motor = must be protected against pinching, limited torque, automatic stop if resistance detected. No gear must be accessible.
Operating temperatures and heating components	Clause 7.3	Temperature limits by material type and human contact	Sensor with membrane having internal heating must be thermally insulated from user housing. Add thermal cutoff if > manufacturer's max.
Protection against hazardous substances / Chemical	Clause 4.8	Prevent leakage of internal chemical substances	Sealed batteries. No internal solvent. Measured gas must NOT come into contact with unintended components (risk of corrosion → electrical leakage).
Internal wiring & insulation distances	Clause 5.5	Insulation distances (clearance, creepage) according to voltages	Between: (1) Motor and logic, (2) heating sensor and microcontroller, minimum distance according to pollution 2 (≥1–2 mm). Double-layer PCB with reinforced insulation on power side.
Mains power supply safety (if applicable)	Clause 5.4.9	External adapter must be certified EN 62368-1	Prohibition of using non-certified adapter. Provide CE/EN 62368-1 mains adapter.
RF energy protection	Clause 5.2.2	RF = Energy Source ES1	WiFi emission (<100 mW) safe. Ensure antenna does not touch any internal metal element to avoid local heating.
Functional safety related to risk	Clause 4.4	Prevention of dangerous situations due to failure	During WiFi loss → motor must operate locally (degraded mode). Gas alarm must be independent of communication.
User-accessible connectors	Clause 8.5	No accessible connector should expose hazardous voltage	USB ports (if OTA/Debug) must remain in SELV. No point at >35V must be [accessible]

Prototype

To ensure that this system is feasible and has the potential to be developed further, I created a prototype. This prototype focuses on building a system composed of two devices communicating remotely through a WiFi link.

Matériel

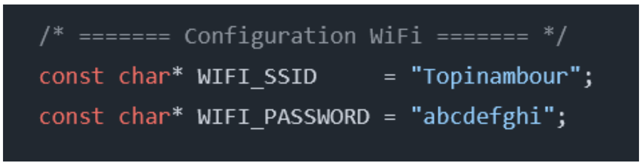
To build this prototype, the following components were used:

- Tab5 integrating an ESP32C6
- ESP32 (WROOM32)
- Smartphone for wifi hotspot
- UnitMQ (flammable gas detector)
- Motor

Codes

To implement this prototype, two separate programs were developed.
The first one handles data transmission, while the second handles data reception.
In reality, the system operates in semi-duplex mode, meaning both devices are capable of sending and receiving data.
However, the “transmitter” is designated as such because it handles both sensor data acquisition and its transmission.

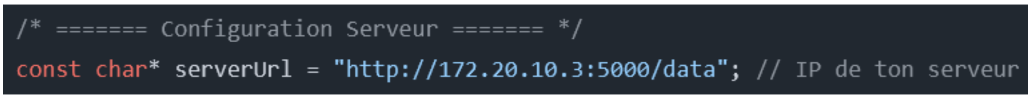
The corresponding programs can be found in the GitHub repository.
They enable data exchange over a WiFi network using a mobile hotspot (the smartphone).



```
/* ======= Configuration WiFi ======= */
const char* WIFI_SSID     = "Topinambour";
const char* WIFI_PASSWORD = "abcdefghi";
```

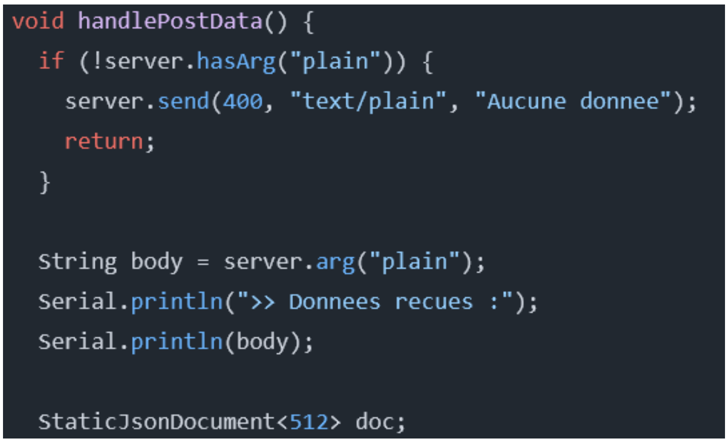
To send a data frame, establishing a WiFi connection is not enough.
For this reason, I implemented a **local HTTP server** on the receiver module.
This allows the transmitter to communicate with it as if it were a client subscribing to a WiFi-based server.
Additionally, data is sent in the form of a **JSON file**.

Server IP :



```
/* ======= Configuration Serveur ======= */
const char* serverUrl = "http://172.20.10.3:5000/data"; // IP de ton serveur
```

Server function and JSON table :

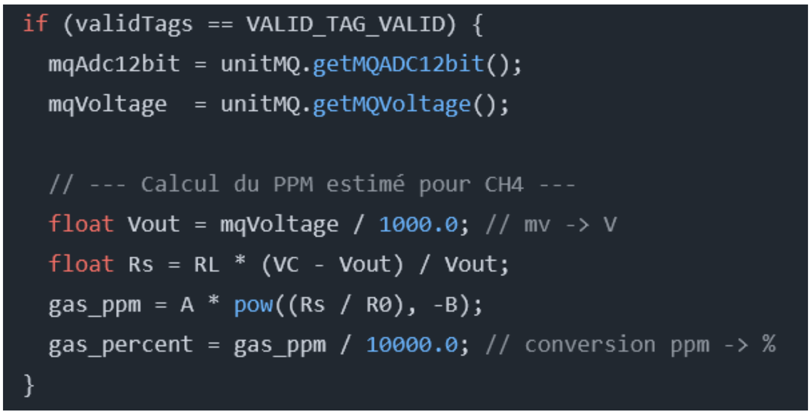


```
void handlePostData() {
  if (!server.hasArg("plain")) {
    server.send(400, "text/plain", "Aucune donnee");
    return;
  }

  String body = server.arg("plain");
  Serial.println(">> Donnees recues :");
  Serial.println(body);

  StaticJsonDocument<512> doc;
```

Finally, sensor data processing is performed directly within the transmitter's code, enabling raw sensor readings to be converted into usable units for gas analysis (percentage or ppm).



```
if (validTags == VALID_TAG_VALID) {
  mqAdc12bit = unitMQ.getMQADC12bit();
  mqVoltage  = unitMQ.getMQVoltage();

  // --- Calcul du PPM estimé pour CH4 ---
  float Vout = mqVoltage / 1000.0; // mv -> V
  float Rs = RL * (VC - Vout) / Vout;
  gas_ppm = A * pow((Rs / R0), -B);
  gas_percent = gas_ppm / 10000.0; // conversion ppm -> %
}
```

Application :

To see the prototype, you'll find a video in the github.

Thank you !

git_link

Conclusion

This project shows that building a flammable-gas analyzer with long-distance communication is not only possible but also practical. By combining a gas sensor, wireless data transmission, a remote display, and an automatic safety response, the system manages to address real everyday risks without requiring heavy installation or complex infrastructure.

Studying the different standards — radio communication, cybersecurity, EMC, and safety — helped shape a solution that can actually work in real conditions and stay compliant with modern requirements. The prototype confirms the concept: the modules communicate reliably, the sensor data is processed correctly, and the overall architecture (WiFi link, local server, JSON data exchange) works as expected.

This first version lays the groundwork for future improvements, such as adding more sensors, creating a mobile app, or moving toward an energy-autonomous design.

In short, the project proves that a connected, safe, and efficient gas-detection system can be built and expanded into a fully deployable product.