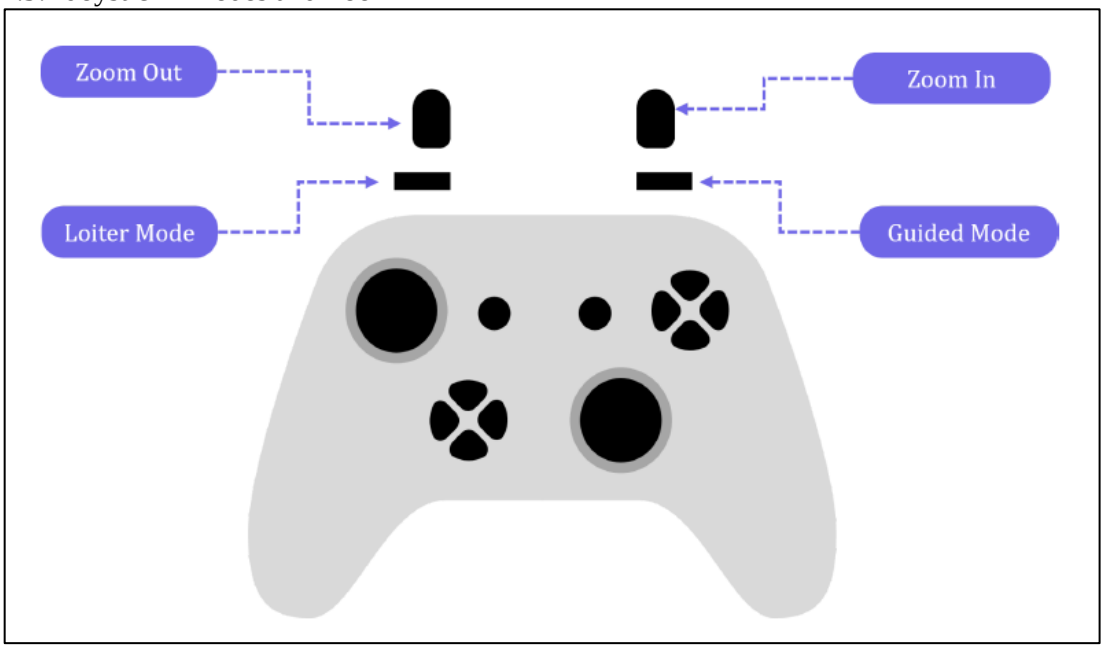
Training Document: Use Case

Table of Contents



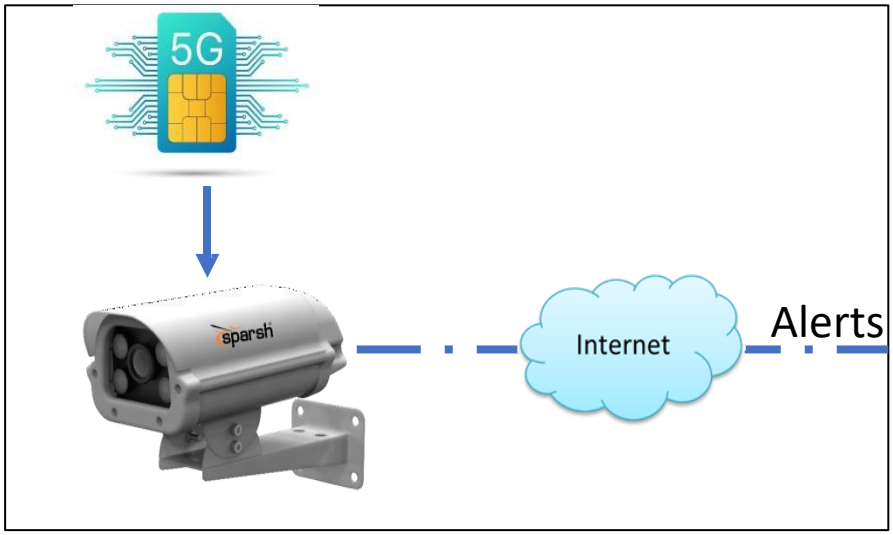
5G Use Cases

1. **5G CAMERA**

1.1 Use Case Development with 5G Camera:

INTRODUCTION: 5G CAMERA:

It is a Next Generation camera with a perfect blend of looks and features for any security requirement. A 100% “Made in India” product with best-in-class technology, robust mechanical, cloud support and service centers all over the country. Leveraging the high transmitted power of 5G, Sparsh 5G Camera can transmit or receive video signals over the Internet wirelessly by simply powering the camera and inserting a SIM card, eliminating the need of complicated cable and fiber connections. Compared with add-on routers, the built-in 5G module enhances the mobility of its deployment, providing a reliable security solution.



1.2 Devices Used for Development

1.2.1 Device Parts

The Sparsh 5G Camera consists of the following essential components:

- **Camera Sensor**: High-resolution imaging sensor with night vision support.
- **Processor**: Integrated AI-capable processing unit for edge computing.
- **5G Module**: High-speed 5G connectivity for seamless data transfer.
- **Storage**: Internal and expandable storage for video retention.
- **Power Supply**: Power over Ethernet (PoE) or battery support.
- **I/O Ports**: USB, Ethernet, and GPIO for connectivity.

1.2.2 Sensor Specifications

Specifications	SC-IM82NP-I (Z)(S)(H)
Camera	
Image sensor	1/2.7" Progressive CMOS Sensor
Effective Pixels	3840(H)x2160(V)
Min. Illumination	Color: 0.01 Lux @F1.2, B/W: 0.001 Lux@F1.2, 0 Lux at IR ON
S/N Ratio	>60dB
IR Distance	50-60Mtr
Shutter Speed	1/25sec ~ 1/100000 sec
IR On/Off Control	Auto/ Manual
IR LEDs	4 Array LEDs
Lens	
Lens Type	Motorized
Mount Type	M14
Focal Length	Motorized 2.7-13.5mm Lens
Max. Aperture	F1.2
Angle Of View	Horizontal: 98° to 34° Vertical: 52° to 19° Diagonal: 116° to 40°
Focus Control	Auto/Manual
Video	
Compression	H.265SE/H.265/H.264
Streaming Capability	3 Streams
Resolution	8MP/5MP/4MP/2MP/D1/ VGA /CIF
Streams	**Mainstream:** 3840x2160(4K) @15fps/ 2592X1944 (5MP)/ 2560X1440 (4MP)/ 2304X1296 (3MP) 1920X1080(2MP) @25/30fps, **Sub Stream:** VGA (640x480)/CIF (352×288) @15/25fps **Third Stream:** D1 (704x576)/ VGA (640x480)/CIF (352×288)/720P (1280x720) @15/25fps
WDR	120dB
Bit Rate	221Kbps-8Mbps
Bit Raye Control	CBR/VBR
Day/ Night	Automatic/Color/Black and white
Exposure Mode	Automatic/Manual
BLC Mode	On/Off
HLC Mode	On/Off
Profiles	Auto, Low Light Priority, High Light Priority
White Balance	Indoor/Outdoor/Automatic
Gain Control	Auto/Manual
Noise Filter	Auto (1-6 Levels)
Digital Zoom	16X, Area's selection with Mouse
Anti - Flicker	On/Off

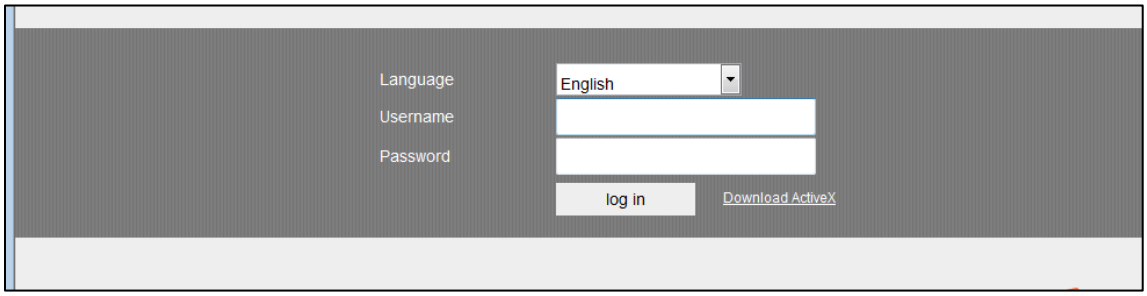
Sensor Specifications continued….

AE Reference	1-255 Level
AE Sensitivity	1-10 Level
Flip	Off / On
IR Reverse	Support
Mirror	Off / On
Text Overlay	Title, Date & Time, Weekday
Privacy Masking	Yes (4 zones)
Events	
Motion Detection	22X18 Zones
Video Blind	Support
Abnormality	No Disk, Disk Error, Disk No Space, Network Cable Disconnected, IP Address Conflict
Smart Functions (By Camera)	Human Detection, Intrusion Detection, Line crossing, Object Lost, Object Left, Scene Change, Audio Detection
Smart Functions (By Software)	License Plate Recognition, Face Detection & Recognition, People Counting, Object Detection/Classification, object pattern recognition models supported through software
Event Actions	Record alarm, Linkage alarm output, Sound alarm, Email link, Upload FTP, Snapshot
PTZ (Manual)	
Pan	0° ~360°
Tilt	0° ~90°
Safety	
Security	Authorized username and password, HTTPS with password, RTSP Validation, User Access Log, User Authentication, Watermark, IP address filtering, 802.1x; IP/MAC filtering; HTTPS; trusted upgrade; trusted boot; firmware encryption; generation of X.509 certification
ONVIF Authentication	ON, OFF
RTSP Authentication	Digest, None
Audio	
Compression	G.711A/U
Talk Back	Support
Network	
Ethernet	10/100M adaptive Ethernet interface
Protocol	TCP/IP, UDP, RTP, RTSP, RTCP, HTTP, HTTPS, DNS, DDNS, DHCP, FTP, NTP, SMTP, UPNP, SMTP, IPv4, 3G/4G/5G
Band Support	5G: LB: n5/8/20/28; MB: n1/3/4/66, HB: n7/38/40/41/48/77/78/79 4G: LB: B5(18/19/26)/8/20/28; MB: B1/3/4/66, HB: B7/34/38/39/40/41/42/43/48
SIM Card	1x Nano SIM card support
Interoperability	ONVIF Profile S & G
Max. user Access	20 Users
Edge storage	Local PC for instant recording, one clicks Snapshot, one clicks triple Snapshot
Web Viewer	IE, Chrome, Firefox, Safari
Management Software	Sparsh VMS

1.3 Utilities and Configuration

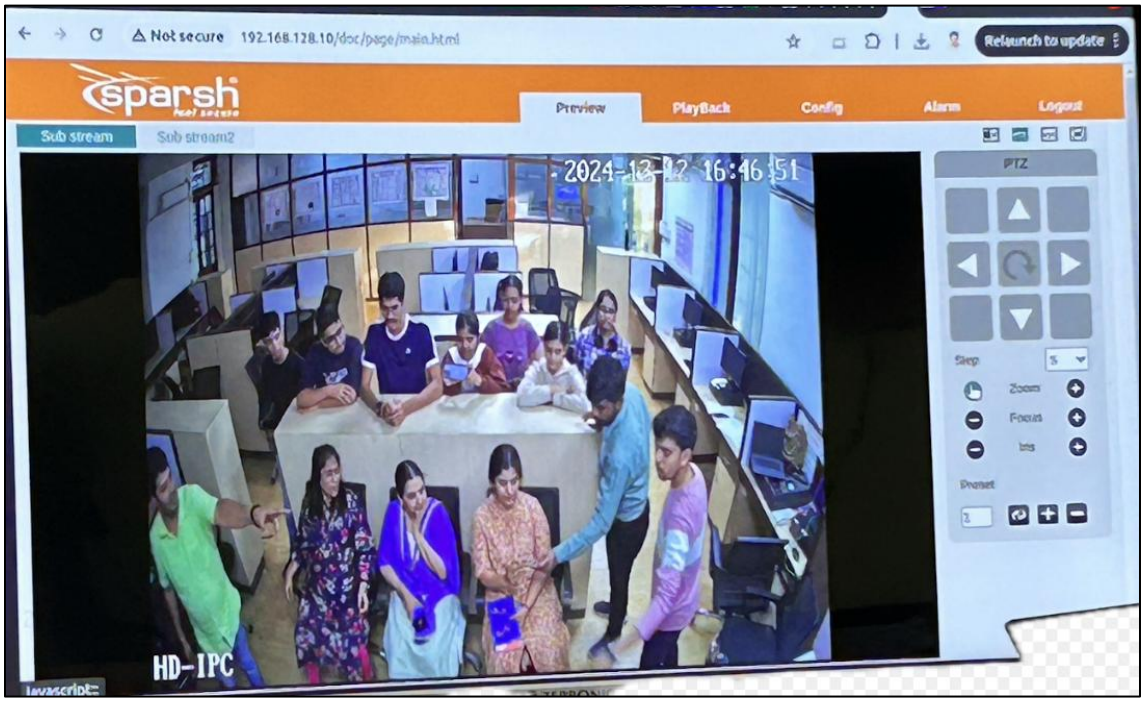
1.3.1 Camera page login & Configuration

Connect the lan cable to your PC open the web browser and use https://192.168.128.10 IP to open the camera login page use below credential
USER NAME : admin
PASSWORD : admin123



1.3.2 Preview interface：

The **camera preview interface** is the user interface (UI) that allows users to view and manage live feeds from their 5G cameras.



1.3.3 Local Config:

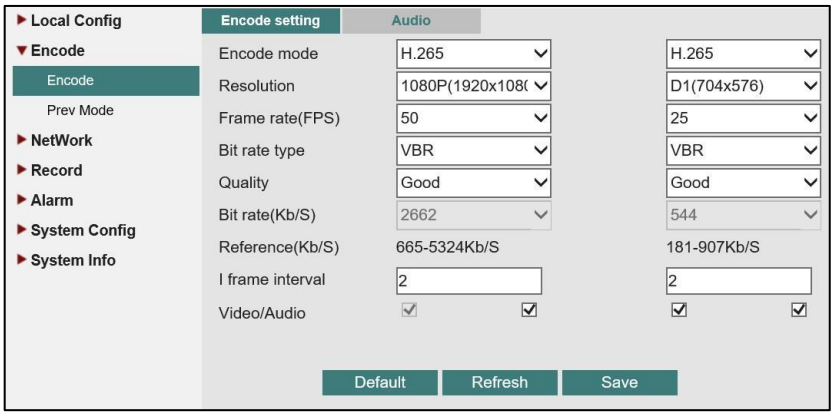
This configuration of the camera can be done.

A. Encode:

Encoding of video and audio are as follow:

i. Encode setting:

Options to adjust the video resolution (e.g., 720p, 1080p, 4K) bit rate, frame rate or to adjust the video stream quality, particularly for bandwidth management.



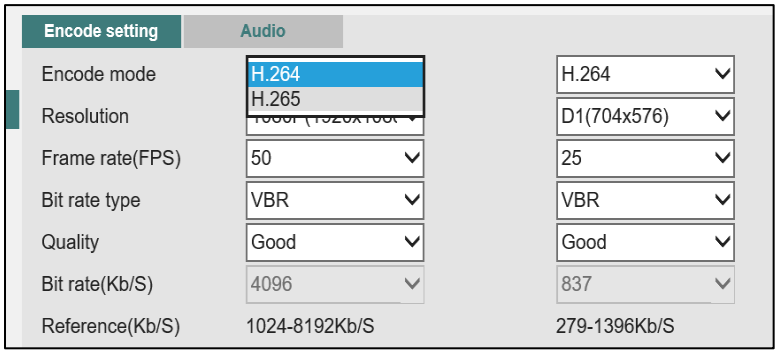
Camera is running on three streams:

a) Mainstream

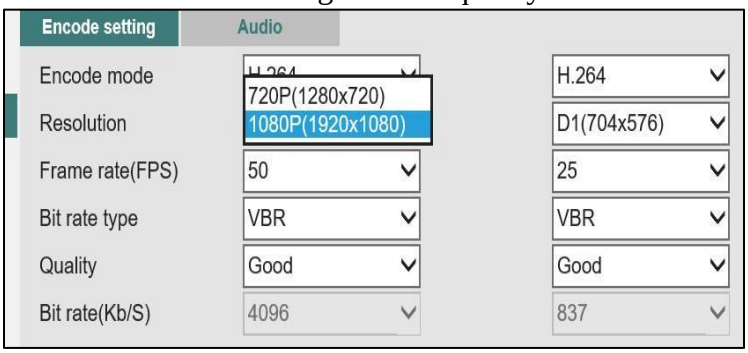
b) Sub stream

c) Third Stream

Choose the video compression standard maintained on the 2 MP camera.



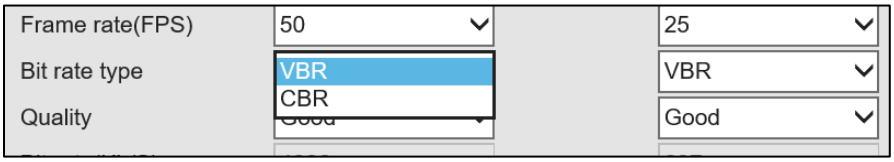
Resolution: We can set the resolution according to video quality need.



Frame rate: The number of frames shown or recorded in one second of video. A higher frame rate results in smoother motion, while a lower frame rate can cause motion to appear choppy.In mainstream we can only set the fps upto 50 but in sub stream upto 25 only. Select according to use.

Bit rate type: There are two types which are follow as (i)VBR

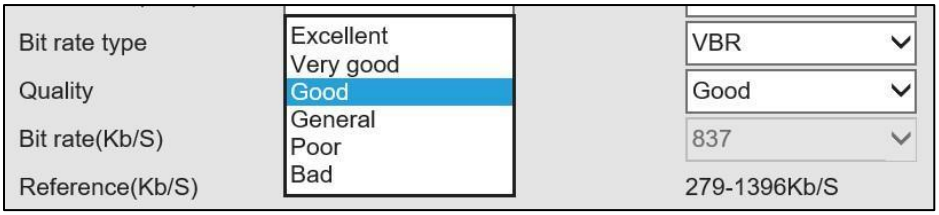
(ii)CBR



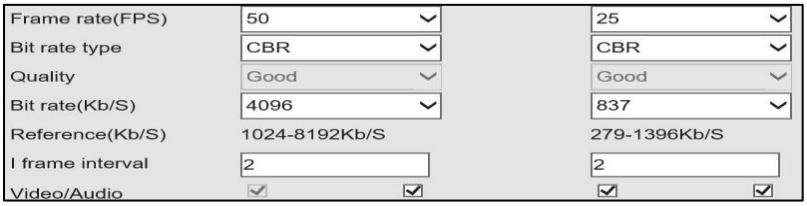
VBR (Variable Bit Rate) and **CBR (Constant Bit Rate)** are two common video encoding methods used in media compression. They refer to how the **bit rate** (the amount of data used

per second in video/audio encoding) is managed during the encoding process. The bit rate directly affects video quality and file size.

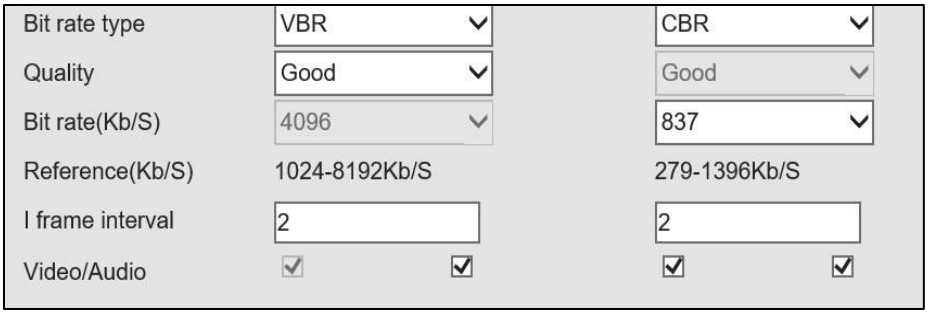
Quality: Quality can be set according the video requirement which will directly affect the bandwidth consumed.



Bit rate: When we set the video encode on CBR bit rate type then we manually config the bit rate of the video encode.



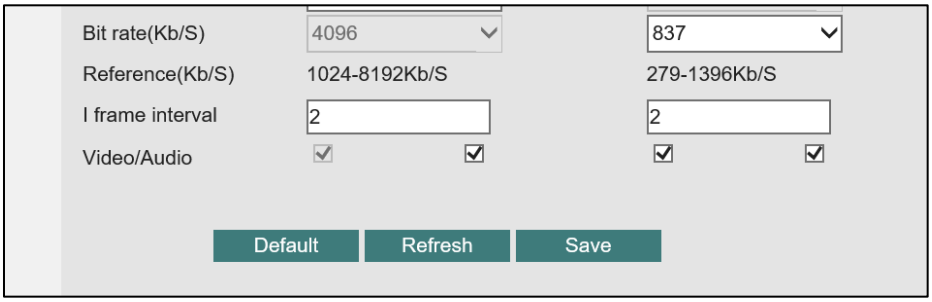
I frame interval: The **I-frame interval** (also known as **Keyframe interval**) is an important setting in video encoding and streaming. It refers to the frequency at which **I-frames (Intra-coded frames)** are inserted into the video
stream..For 2mp bullet camera by default value is 2.



Default: It is used for setting the value as default.

Refresh: It is used for updating from previous.

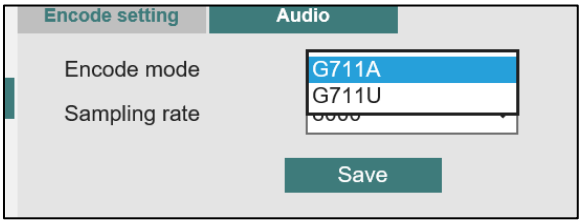
Save: It is used for saving the configuration.



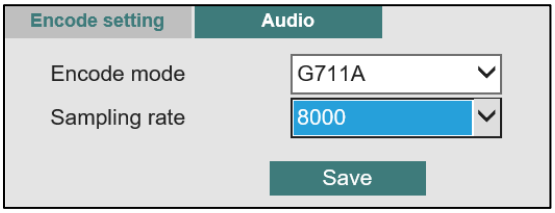
ii. Audio:

In this we have done the audio encoding setting.

Encode mode: We have used the audio format “G711A” and “G711U” for audio compression standards.



Sampling rate: the sampling rate should be 8000 Hz or more than it due to the smoothness of audio.

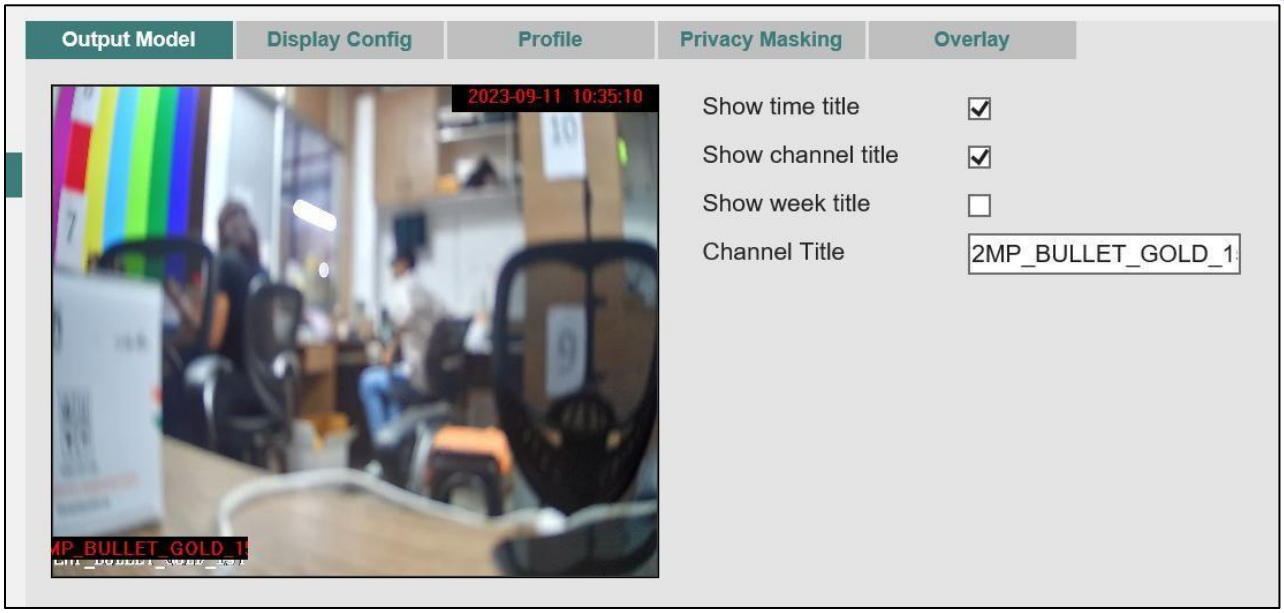


1.4 Prev Mode:

1.4.1 Output model:

Output model is used to set the on screen changes to be displayed on the live view feed.

(i) Show time title
(ii) Show channel title
(iii) Show week title
(iv) Channel title



1.4.2. Display config:

Image Color: **Image color settings** control how the camera processes and displays colors in the video feed.

(v) **Profile:** If we want to change the profile as day/night.

(vi) **Brightness:** Controls the overall lightness or darkness of the image.

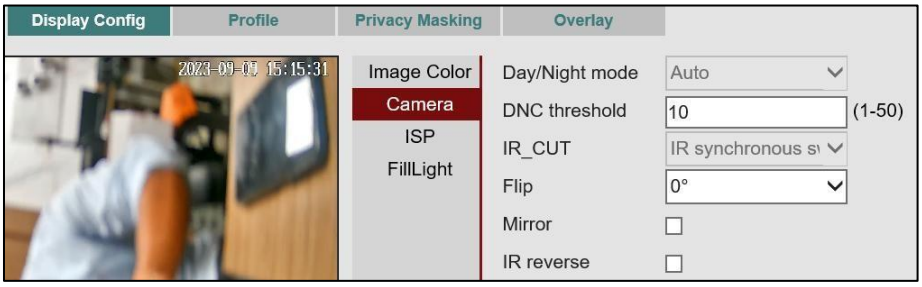
(vii) **Contrast**: Enhances the clarity of an image by making shadows darker and highlights brighter, making the subject stand out more clearly.

(viii) **Saturation:** Controls the intensity of colours in the image. Increasing saturation makes colors more vivid, while decreasing it results in a more washed-out or grayscale image.

(ix) **Tone:** Helpful when colors appear unnatural due to lighting (e.g., a yellowish tint under tungsten lights).

(x) **Sharpness**: Controls the clarity and crispness of the image.

1.4.3 Camera:



Day/night mode: Determines how the camera adjusts to different lighting conditions (daytime or nighttime).

DNC threshold: By adjusting the DNC threshold, you can manage how aggressive the camera is at removing noise, which helps maintain image clarity, especially in dark environments

IR_CUT: it is synchronous with the amount of light sensed by LDC.

Flip/mirror: The **Flip/Mirror** function is a setting that allows you to **flip or mirror** the video feed, which is particularly useful when the camera is mounted in certain orientations or positions.It is used to set for real image that should be seen on screen if camera is set inverted or alternate position.

IR reverse: The purpose of this function is to adjust the way infrared light is used or the way it impacts the camera's image.

1.4.4 ISP:

Exposure mode: The **exposure mode** controls how the camera adjusts the exposure time, or how long the camera's sensor is exposed to light, to capture an image. It is crucial in ensuring the camera produces well-lit images, especially in environments with changing light conditions.Its value is up to 1/100000 for BLC and HLC of the video encoding in the camera.

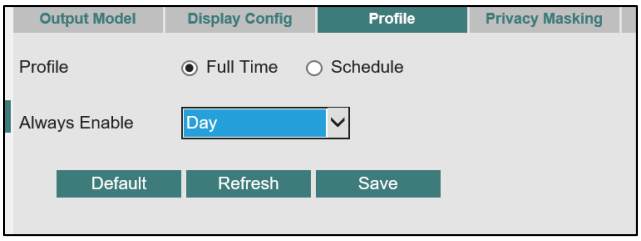
BLC: It is a feature designed to help the camera deal with situations where there is **strong light** coming from behind the subject being captured, which typically causes the subject to appear very dark.

HLC: It is a feature that helps reduce the effects of **bright light sources** (such as headlights, street lights, or spotlights) that can create glare or overexposure, making the subject difficult to see.

Fill Light :It refers to the additional light sources used to **illuminate** a scene in low-light conditions. It supplements the camera's existing light (usually infrared light at night) to provide better visibility.

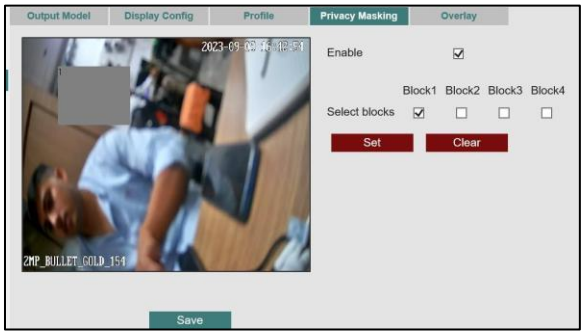
1.4.5 Profile:

Used to schedule camera view settings for full time day/night or can be scheduled for particular hours.



1.4.6 Privacy Masking:

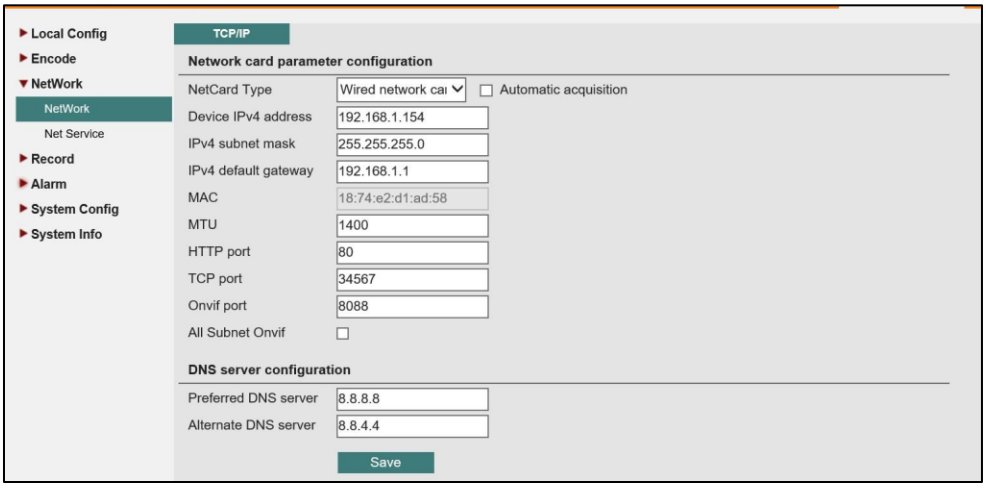
It is a feature that allows you to block out certain areas of the camera's field of view, so they are not recorded. It allows you to block out sensitive areas of the camera's view while still recording the rest of the scene.



1.4.7 Overlay:

It displays additional information on the video feed, such as text, logos, timestamps, or other visual markers, that are superimposed onto the live or recorded video.Alignment of the text such as left align or right align can be done by text align.

1.5 Network:



1.5.1 TCP/IP:

We use TCP/IP.

Network card parameter config:

(xi) Net card type: we used wired network cards.

(xii) Device IPv4 address: we manually provide the IP to the device.

(xiii) All the port no and mask are by default set.

(xiv) A **MAC (Media Access Control) Address** is a unique identifier assigned to the network interface card (NIC) of a device, used for communication on a network.

(xv) MTU: **MTU (Maximum Transmission Unit)** is a network setting that defines the largest size of a data packet that can be sent over a network without needing to be fragmented. It is an important setting for ensuring efficient and reliable communication in computer networks, as it determines the maximum amount of data that can be transmitted in a single packet.

(xvi) HTTP port: The **HTTP (Hypertext Transfer Protocol)** port is primarily used to access the **web interface** of network cameras, NVRs, and other devices over the network using a **web browser**.By default is 80.

(xvii) TCP port: **TCP (Transmission Control Protocol)** ports are used for the **data transmission** between devices in a Camera system. These ports allow for reliable, ordered

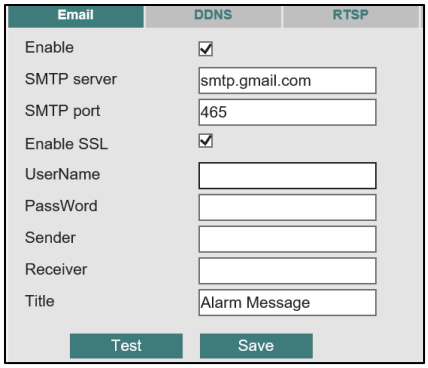
delivery of video streams, remote controls, and management commands.

(xviii) Onvif port: **ONVIF ports** are essential for the proper functioning and interoperability of Camera systems, especially for **IP cameras** and **network video recorders (NVRs)**.DNS server configuration: When configuring a Camera system, setting up the DNS server correctly ensures that devices can access the network and communicate with each other.

1.6 Net Service:

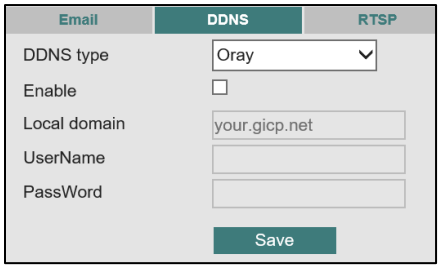
1.6.1 Email:

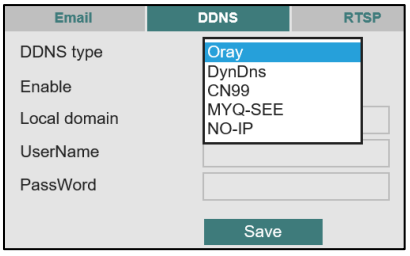
Setting up **email alerts** allows you to receive notifications (like motion detection alerts, system errors, or triggered alarms) directly to your email address. This feature is useful for remotely monitoring your security system, ensuring that you're always notified of any events that require attention, even when you're not actively checking the system.



1.6.2 DDNS:

When using DDNS with your Camera system, you can assign a **domain name** (like myCamera.dyndns.org) to your
camera changing public IP address. This allows you to access your Camera system by typing a domain name into a browser instead of a changing IP address and can be accessed from anywhere in the world.

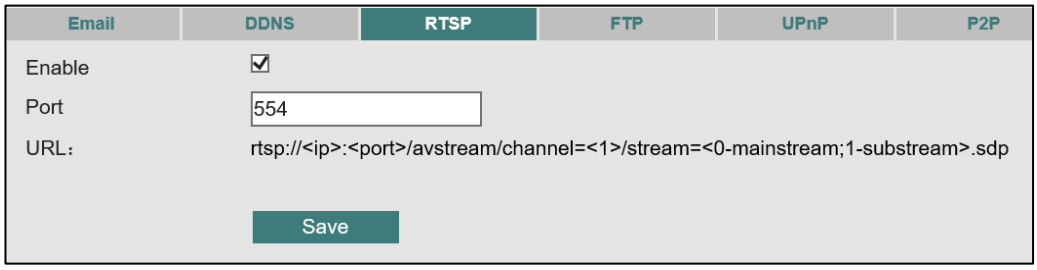




In DDNS we select the DDNS type and provide the user at which we want the DDNS to come.

1.6.3 RTSP:

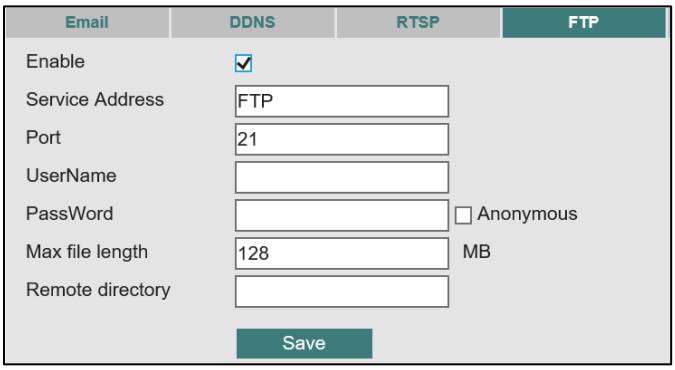
RTSP (Real-Time Streaming Protocol) is commonly used for transmitting video and audio from Camera cameras.



Camera cameras that support RTSP allow you to stream live footage over a network to devices like computers, mobile phones, or specialized monitoring software.Can access it on VLC by copying the URL.

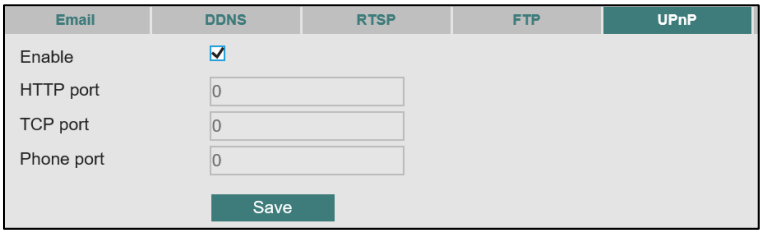
1.6.4 FTP:

FTP is used to upload or download video footage from cameras to a remote server or cloud storage.



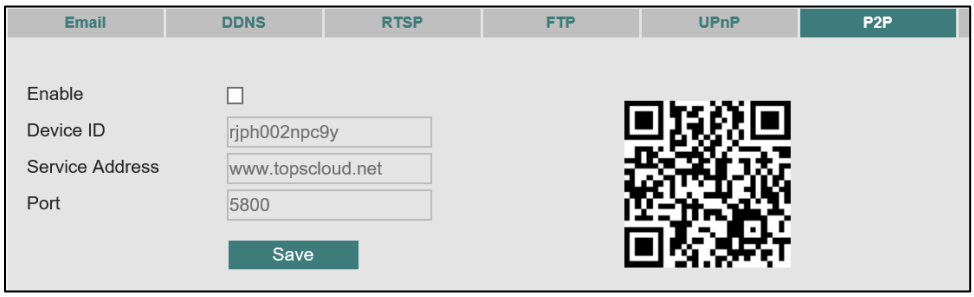
1.6.5 UPnP:

It can automatically configure certain network settings, such as port forwarding, without needing manual intervention. This can make setting up remote access to the camera easier, as UPnP enables the camera to automatically open the necessary ports in your router to allow access from outside your local network



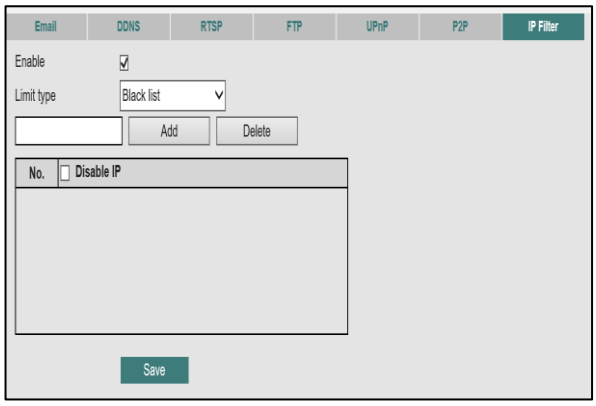
1.6.6 P2P:

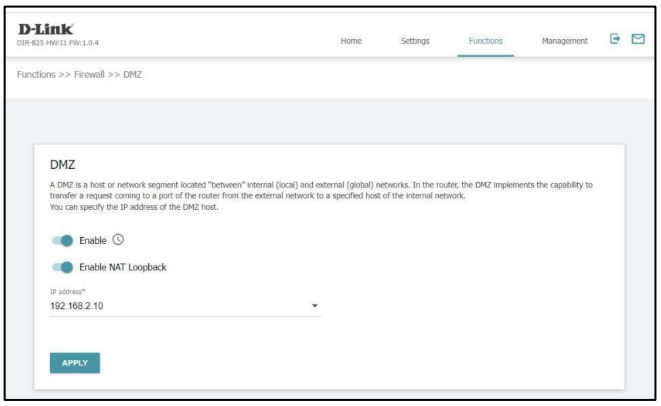
P2P (Peer-to-Peer) Camera refers to a type of surveillance camera system that uses P2P technology to establish a
direct connection between your Camera camera and a viewing device, such as a smartphone, tablet, or PC, without the need for port forwarding or a static IP address.



1.6.7 IP filter:

IP filtering works by specifying which IP addresses or ranges are allowed (whitelisted) or blocked



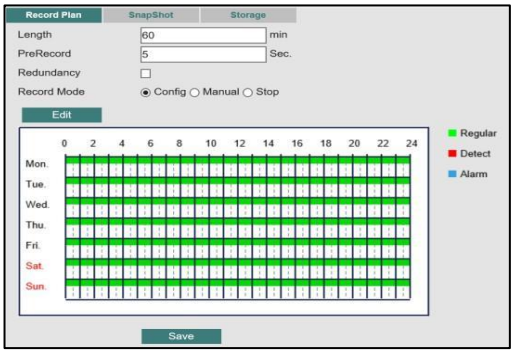


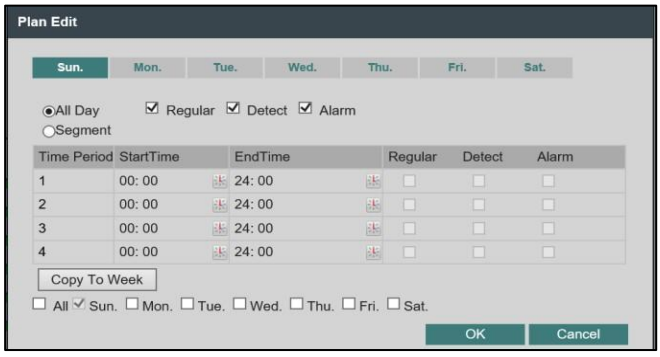
(blacklisted) from accessing the camera or Camera system. For example, you can set your Camera system to allow access only from specific IP addresses, such as your home or office IP, and block others

1.7 Record:

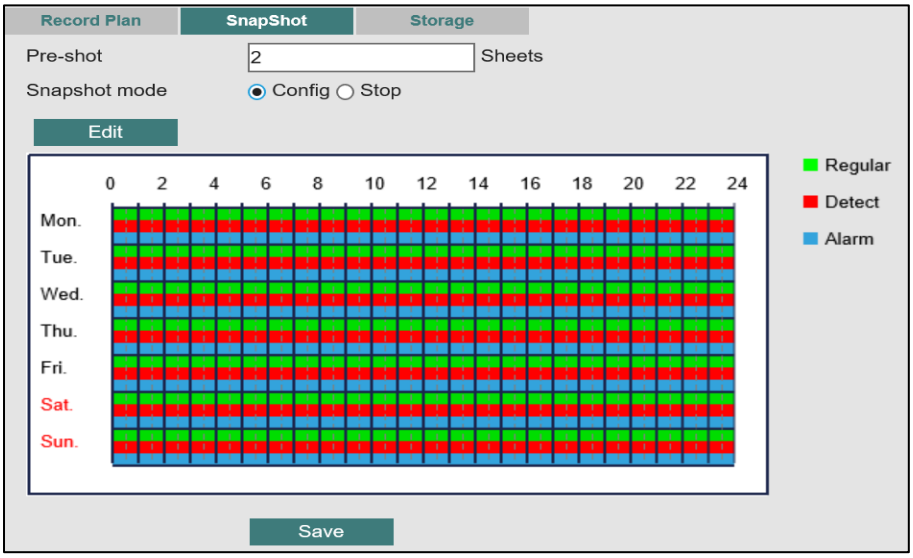
1.7.1 Record Plan:

A **record plan** allows you to define when and how your Camera system records footage. This feature is useful for managing storage space and ensuring cameras record during specific times, based on your needs.





(i) Length is provided for what time the record should be require.
(ii) Pre-record: the camera records a few seconds or minutes **before** an event (such as motion detection or an alarm trigger) actually occur.
(iii) Redundancy The main goal of redundancy in recording is to protect against data loss, minimize downtime, and ensure that the system continues recording even if a failure occurs in the primary storage system.
(iv) Record mode: if we want to config, it then it can, if manually then it can be set, if stop to record then it can be.



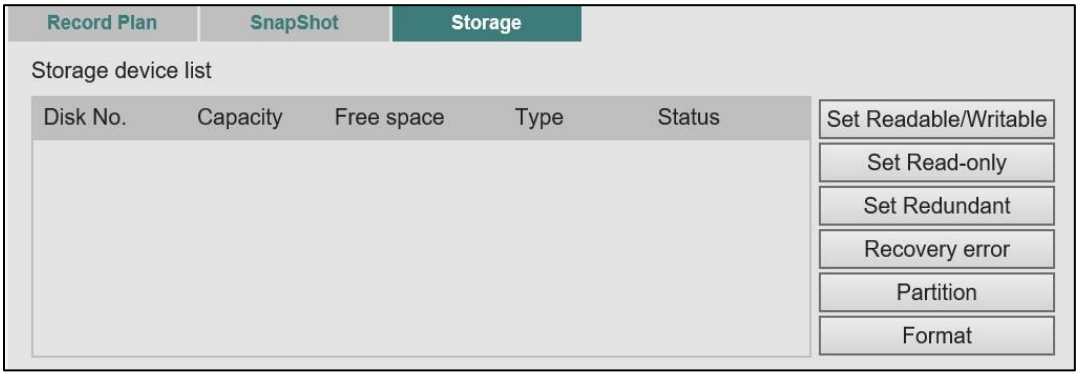
1.7.2 Snapshot:

The **Snapshot Function** lets you take still images from the live video feed or from recorded footage. This can be useful for capturing specific moments (like an intruder entering a room or an important event) and storing them separately from video recordings.

1.7.3 Storage:

Storage device shows here and the setting can be made how to use the storage device and can be formatted if required.

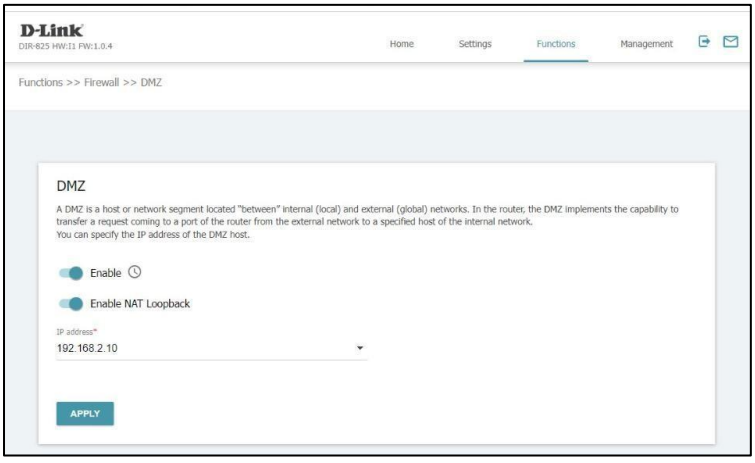
Storage Read/Write: Ensures efficient data transfer speeds for continuous recording and smooth playback. **Redundant Storage**: Duplicates data across multiple storage devices to prevent data loss in case of failure. **Recovery Cover**: Implements backup and failover systems to restore footage and maintain functionality after a failure.



1.8 Seamless integration with 5G networks

1.8.1 Enabling 5G setting

5G is enabled as soon as the SIM card is activated in the camera. To enable viewing of cameras over 5G, enable DMZ service from router web GUI as below. Enter camera IP address and save.



1.8.2 To Access the 5G Modem info follow below steps:

- Connect to the camera's LAN network by using the LAN port from camera and connect with the PC
- To get the 5G modem Info open browser(Chrome , firefox) in address bar enter the 192.168.128.1 ip address
- Check the IP address assigned to 5G SIM camera in that page
- Once you have identified the 5G SIM IP address, open Firefox in the Camera VM.
- Enter the 5G SIM IP address in the browser to access the camera feed

1.9 Demonstration of Use Cases

1.9.1 Steps to Connect and Integrate 5G Sparsh Camera Feed with AI/ML Object & Human Detection

A. Connect to the Camera's LAN Network

- Use an Ethernet cable to connect the **camera's LAN port** to your **PC**.
- Ensure that the PC is set to obtain an IP address automatically or configure it manually if required.

B. Retrieve 5G Modem Information

- Open a web browser (**Chrome or Firefox**).
- In the address bar, enter **192.168.128.1** and press **Enter**.
- This will open the 5G modem's web interface.

C. Check the 5G SIM Camera's Assigned IP Address

- Navigate to the **status or network settings page** in the modem interface.
- Locate the **IP address assigned to the 5G SIM camera**.
- Note down this **5G SIM IP address** for the next step.

D. Access the Camera Feed

- Open **Firefox** inside the **Camera VM**.
- In the address bar, enter the **5G SIM IP address** and press **Enter**.
- The camera's live feed should now be accessible.

E. Integrate Camera Feed with AI/ML Object & Human Detection

- To integrate the live camera feed into the **AI/ML object & human detection system**, use the **RTSP stream link**:
  rtsp://admin:admin123@<camera_IP>/avstream/channel=1/stream=0.sdp
- Where <camera_IP> is the **5G SIM IP address** retrieved earlier.
- This **RTSP stream** can be fed into AI/ML-based detection models for real-time processing and analysis.

1.10 Troubleshooting (If Unable to Access the Feed)

- Ensure that the camera is powered on and properly connected to the **LAN network**.
- Verify that the **5G modem** is active and providing an IP address.
- Check firewall or security settings that may block network access.
- Restart the camera, PC, or modem if necessary and repeat the steps.
- Confirm that the **AI/ML system supports RTSP streaming** and is configured correctly.

2. IOT GATEWAY-

2.1 Features of IoT Gateway

2.1.1 Hardware

Mobile	5G Sub-6Ghz SA/NSA 2.1/3.3Gbps DL (4x4 MIMO), 900/600 Mbps UL (2x2); 4G (LTE) – LTE Cat 20 2.0Gbps DL, 200Mbps UL; 3G – 42 Mbps DL, 5.76Mbps UL
CPU	Quad-core ARM Cortex A7, 717 MHz
Flash storage	256 MB
RAM	256 MB
Powering options	4-pin power socket, 9-50 VDC
SIM	2 x SIM slot (Mini SIM – 2FF), 1.8 V/3 V
Antenna connectors	4 x SMA for Mobile, 2 x RP-SMA for WiFi, 1 x SMA for GNSS
Ethernet	5 x 10/100/1000 Ethernet ports: 1 x WAN (configurable as LAN), 4 x LAN
Wifi	802.11b/g/n/ac Wave 2 (WiFi 5) with data transmission rates of up to 867 Mbps (Dual Band, MU-MIMO), 802.11r fast transition, Access Point (AP), Station (STA)
Wireless mesh/roaming	Wireless mesh (802.11s), fast roaming (802.11r)
GNSS	GPS, GLONASS, BeiDou, Galileo, QZSS
Inputs/Outputs	On 4-pin socket: 1 x Digital input, 1 x Digital open collector output
Other	1 x USB host, 1 x Grounding screw
Status LEDs	3 x connection status LEDs, 3 x connection strength LEDs, 10 x Ethernet port status LEDs, 4 x WAN status LEDs, 1x Power LED, 2 x 2.4G and 5G WiFi LEDs
Operating temperature	-40 °C to 75 °C

Housing	Aluminum housing, DIN rail (can be mounted on two sides), flat surface placement
Dimensions	(W x H x D) 132 x 44.2 x 95.1 mm
Weight	533 g

2.1.2 Software

Operating system	RutOS (OpenWrt based Linux OS)
Mobile features	Multiple PDN, Auto APN, Band lock, SIM switch, Operator black/white list, Data/SMS limits
Network features	Routing, Failover, Firewall, DHCP, DDNS, Load Balancing, VoIP passthrough, Connection monitoring
Monitoring and Management	WEB UI, CLI, SSH, CALL, SMS, TR-069, SNMP, JSON-RPC, MQTT, MODBUS, RMS
VPN and tunneling	OpenVPN, IPsec, GRE, PPTP, L2TP, Stunnel, DMVPN, SSTP, WireGuard, ZeroTier
Cloud solutions	RMS, FOTA, Azure IoT Hub, Cloud of Things, Cumulocity, ThingWorx
Hotspot	External/Internal Radius, SMS OTP, MAC authentication, Walled Garden
GNSS	NMEA forwarding, AVL, Geofencing

To know more about the feature of RUTX50 you can go to the link given below:

RUTX50 Industrial 5G Router

2.2 IOT Gateway Architecture

Component	Description
Processor (CPU)	ARM-based processor, likely ARM Cortex-A7 for routing and data processing.
Networking Interfaces	4G LTE WAN, Gigabit Ethernet LAN, Dual-band Wi-Fi (2.4 GHz and 5 GHz), Serial (RS232/RS485), SIM card slot.
Operating System	OpenWrt-based Linux OS for flexibility and customization.
Storage	Flash memory with optional microSD for additional storage.
Power Supply	DC input range with PoE (Power over Ethernet) support.
Security Features	VPN support (IPsec, OpenVPN, WireGuard), firewall, encryption.
Management and Monitoring	Web interface for configuration, RutOS Cloud for centralized management.
Redundancy & Failover	WAN failover for automatic connection switching between LTE, Ethernet, and Wi-Fi.
Environment & Durability	Ruggedized design, built to endure harsh conditions (temperature, dust, vibration).
Expansion & Customization	I/O ports for sensors and custom industrial applications.

2.3 Communication Protocols Used In IoT Gateways

The **RUTX50** is a powerful industrial IoT gateway by **Teltonika Networks**, designed for various industrial applications. It supports multiple communication protocols, ensuring reliable and flexible communication across different IoT devices and networks.

Here's a breakdown of the key **communication protocols** supported by the **RUTX50**:

2.3.1 Cellular Protocols

2G (GSM/GPRS): For basic connectivity in areas where higher-speed networks aren't available.
3G (UMTS/HSPA): Offers improved data speeds compared to 2G, typically used in medium-level data communication.
4G LTE: High-speed cellular network for modern IoT applications requiring fast data transfer and reliable connectivity.
5G: With the latest update, the RUTX50 supports **5G** for ultra-fast speeds, lower latency, and support for massive IoT device connectivity.

2.3.2 Wi-Fi (802.11 a/b/g/n/ac)

Wi-Fi (2.4 GHz and 5 GHz): The gateway supports Wi-Fi for both connecting to local networks and functioning as an access point. It can communicate with other IoT devices over Wi-Fi, offering flexible wireless networking options.

2.3.3 Ethernet (Wired LAN)

Gigabit Ethernet: The RUTX50 supports **10/100/1000 Mbps Ethernet ports** for stable wired connections, ideal for setting up local area networks (LAN) or integrating IoT devices that require consistent data transfer.

2.3.4 VPN (Virtual Private Network) Protocols

OpenVPN: Supports secure tunneling for remote access to IoT networks, ensuring encrypted communication between remote devices and the gateway.
IPSec: Another secure VPN protocol for encrypted communications between devices and the internet.
PPTP and **L2TP**: Alternatives for VPN tunneling, ensuring that devices connected to the gateway are secure and protected from external threats.

2.3.5 MQTT (Message Queuing Telemetry Transport)

MQTT: A lightweight and efficient messaging protocol often used in IoT environments for sending and receiving small data packets between devices and cloud-based systems. It's ideal for low-bandwidth and high-latency networks.

2.3.6 Modbus (RTU/TCP)

Modbus RTU and **Modbus TCP**: These are widely used protocols in industrial automation. They enable communication with industrial equipment, such as PLCs (Programmable Logic Controllers) and sensors, allowing data exchange between IoT devices and control systems.

2.3.7 CoAP (Constrained Application Protocol)

CoAP: A specialized protocol designed for low-power and constrained devices. It operates over UDP and is suitable for IoT devices with limited resources, such as low-power sensors or actuators in smart cities and industrial systems.

2.3.8 SNMP (Simple Network Management Protocol)

SNMP: The gateway can use SNMP to monitor and manage connected devices, providing a way to retrieve information like performance metrics, operational status, and error logs. It's useful in large networks where network administrators need to ensure that devices are working properly.

2.3.9 TR-069 (CPE WAN Management Protocol)

TR-069: Allows the remote management and configuration of IoT devices over broadband networks. This protocol enables the gateway to be monitored, updated, and configured remotely, making it easier to maintain a large fleet of IoT devices.

2.3.10 HTTP/HTTPS

HTTP/HTTPS: The RUTX50 supports both HTTP and HTTPS protocols for web-based management. Secure HTTPS is typically used for accessing the gateway's configuration interface or communicating with cloud-based services while ensuring data security.

2.3.11 NTP (Network Time Protocol)

NTP: Ensures that the RUTX50 gateway synchronizes its clock with an NTP server, which is important for time-sensitive applications like logging and event tracking in IoT systems.

2.3.12 IPv4 and IPv6

IPv4: Supported for standard networking, allowing for communication between devices in an IP-based network.
IPv6: Future-proof protocol supporting an increased number of devices and networks, which is particularly useful for large-scale IoT deployments.

2.3.12 LAN/WAN Routing

The **RUTX50** is capable of routing between different networks (LAN/WAN), allowing seamless communication and access between devices connected to local networks and external networks (including the internet).

2.3.13 PPP (Point-to-Point Protocol)

PPP: This protocol is used for encapsulating network-layer protocol information and is typically used in the configuration of VPNs or dial-up connections, especially in cellular or remote scenarios.

2.3.14 RADIUS (Remote Authentication Dial-In User Service)

RADIUS: This protocol provides centralized authentication, authorization, and accounting for users who connect to the network, often used in enterprise environments for managing access control.

2.3.15 DLNA (Digital Living Network Alliance)

DLNA: This protocol allows the sharing of media between devices connected to the network, although it is more relevant for multimedia IoT use cases (e.g., video surveillance systems).

2.4 VLAN

A **VLAN** (Virtual Local Area Network) is a network technology that allows you to partition a physical network into multiple logical networks. Each VLAN acts as a separate network, even if the devices are on the same physical network infrastructure.

2.4.1. Simultaneous Server and Multiple Clients (VLAN for Server and Client Networks)

The RUTX50 allows you to create multiple VLANs (Virtual Local Area Networks) on its LAN and WAN interfaces. This can be used to separate server and client networks, where one VLAN could serve as a server network and another as a client network.

A. Steps to Configure VLAN for Server and Client:

1. **Access the RUTX50 Web Interface:**
    - Open a browser and go to the router's IP address (192.168.1.1).
    - Login with your credentials.
2. **Create VLANs:**
    - Go to **Network** > **VLAN**.
    - Add a VLAN by clicking the **Add** button.
    - Assign a VLAN ID (for example, VLAN 10 for the client network and VLAN 20 for the server network).
    - Assign specific interfaces to these VLANs. For example:
        - VLAN 10: Assign the WAN and LAN ports that will be used for clients.
        - VLAN 20: Assign the LAN ports that will be used for the server network.
3. **Assign IP Addresses for Each VLAN:**
    - Go to **Network** > **Interfaces**.
    - Select the interface for each VLAN and assign different IP addresses (e.g., 192.168.10.1 for VLAN 10 and 192.168.20.1 for VLAN 20).
    - Configure appropriate DHCP settings if needed.
4. **Configure Routing:**
    - Go to **Network** > **Firewall** and create firewall rules to ensure traffic flows correctly between the server and client VLANs.
    - Set up routing rules for each VLAN if they need to communicate with external networks.
5. **Test and Verify:**
    - Once you've set up the VLANs and interfaces, you should be able to connect devices to the corresponding VLAN ports and verify that the network segregation is working as intended.

B. VPN Client and Server Support

The RUTX50 also supports VPN services for both server and client connections. It can act as a VPN server (e.g., OpenVPN or IPsec) and connect to remote VPN servers as a client.

C. VPN Server Configuration (e.g., OpenVPN Server):

1. **Access VPN Settings:**
   - Go to **VPN** > **OpenVPN Server**.
2. **Enable the OpenVPN Server:**
   - Turn on the OpenVPN server.
   - Choose the **Server IP Address** and configure other options like **Port**, **Protocol**, and **Encryption settings**.
   - Set up user authentication for VPN access.
3. **Create Client Certificates:**
   - You'll need to create certificates for the server and clients.
   - Download the server configuration and certificates, then distribute the client configurations to users who will connect.
4. **Firewall and Routing:**
   - Ensure the firewall allows OpenVPN traffic (typically UDP port 1194).
   - If clients need to access specific internal networks, set up routing rules.

D. VPN Client Configuration (e.g., OpenVPN Client):

1. **VPN Client Settings:**
   - Go to **VPN** > **OpenVPN Client**.
   - Enable the OpenVPN client and configure it to connect to the remote VPN server using the server's address, port, and credentials.
2. **Import Client Configuration:**
   - You can import a client configuration file or manually set up the connection parameters (e.g., server address, credentials, certificates).
3. **Verify the Connection:**
   - Once configured, the router will automatically connect to the VPN server when the interface comes up.
   - Check the status to ensure the VPN connection is active.

E. Port and Tag-Based VLAN

The RUTX50 supports **port-based** and **802.1Q tag-based** VLANs, which allow you to assign VLANs to specific ports on the router or create tagged VLANs for more granular network control.

F. Steps to Configure Port and Tag-Based VLAN:

1. **Port-Based VLAN:**
   - Go to **Network** > **VLAN**.
   - Create a new VLAN and assign it to a specific port (e.g., Ethernet port 1 or LAN 2).
   - For example, you can assign VLAN 10 to Ethernet port 1 for a client network and VLAN 20 to Ethernet port 2 for a server network.

-
2. **Tag-Based VLAN (802.1Q):**
   - Under the **Network** > **VLAN** section, enable 802.1Q tagging.
   - Set the **VLAN ID** for each tag and ensure the correct interface is tagged.
   - For instance, you might configure VLAN 10 with a tag 10 on certain ports and VLAN 20 with tag 20 on other ports.
   - On the receiving device (like a switch or another router), configure the same VLAN tag to allow the devices to communicate properly across the tagged VLAN.
3. **Configure Interfaces for Tagged VLAN:**
   - After setting up VLAN tags, go to **Network** > **Interfaces** and assign the tagged VLANs to specific interfaces.
   - This allows you to segment traffic between VLANs at the port level and ensures traffic from devices is properly tagged.
4. **Verify Configuration:**
   - Test connectivity by connecting devices to the appropriate ports or by configuring network devices to use tagged VLAN IDs.
   - Check for network isolation or communication as per your VLAN configuration.

2.5 Security

2.5.1. Firewall Rules

Firewall rules are used to control the inbound and outbound traffic on the router. You can create specific rules to allow or block traffic based on IP addresses, ports, protocols, and interfaces.

A. How to Configure Firewall Rules on the RUTX50:

1. **Login to the RUTX50 Web Interface:**
   - Open a browser and go to the router's IP address (usually 192.168.1.1).
   - Login with your credentials.
2. **Navigate to the Firewall Settings:**
   - Go to **Network** > **Firewall**.
3. **Create a New Rule:**
   - Click **Add New** to create a new firewall rule.
   - You can configure firewall rules for both **WAN** and **LAN** interfaces.
4. **Define Rule Parameters:**
   - **Action**: Choose either Accept (allow traffic) or Reject (block traffic).
   - **Protocol**: Select the protocol (TCP, UDP, ICMP, etc.).
   - **Source IP/Address**: Specify the source IP or range of IP addresses.
   - **Destination IP/Address**: Specify the destination IP or range of IP addresses.
   - **Port Range**: Specify the port or port range to filter.
   - **Interface**: Choose the interface (WAN or LAN).
   - **Logging**: Enable logging for the rule if you want to track the traffic matched by the rule.

5. **Apply the Rules:**
    - Click **Save & Apply** after configuring each rule.

Example Use Case:

To block incoming traffic from a specific IP address, you would:

- Set the **Source IP** to the unwanted IP address.
- Set **Action** to Reject.
- Apply this rule to the **WAN** interface to block external traffic from that IP.

2.6 DDoS Prevention

DDoS (Distributed Denial of Service) attacks can overwhelm your network by flooding it with large amounts of traffic. The RUTX50 has several built-in features to mitigate DDoS attacks.

2.6.1 DDoS Prevention Techniques on RUTX50:

1. **Limit Connection Count**:
   You can set limits on the number of simultaneous connections to prevent connection floods. This can be done through **Firewall settings**.
2. **Enable SYN Flood Protection**:
    - Go to **Network** > **Firewall** > **Advanced Settings**.
    - Enable **SYN Flood Protection** to block SYN floods, which are commonly used in DDoS attacks.
3. **Enable IP Filtering**:
    - Filter incoming traffic from suspicious IP addresses by adding them to the **Blackhole** or **Deny List** in the firewall settings.
    - Go to **Network** > **Firewall** > **Advanced** to configure **IP Filtering**.
4. **Rate Limiting**:
    - Rate limiting can help prevent the router from being overwhelmed by too many requests. Under **Network** > **Firewall**, enable the rate-limiting feature to limit the number of requests from any particular IP.
5. **Enable DoS Detection**:
    - Enable **DoS detection** to monitor and block traffic patterns that are typical of a DDoS attack (like flooding the network with large volumes of traffic).
    - Go to **Network** > **Firewall** > **DoS Protection**.
6. **Use a VPN**:
    - A **VPN** can obscure the actual public IP address of your network, making it harder for attackers to target it directly.
    - The RUTX50 supports both **VPN Server** and **Client** configurations (e.g., OpenVPN, IPsec).

2.7 Data Limit for SIM Card

To manage and control the data usage of the SIM card (which is particularly important for mobile data connections), the RUTX50 allows you to set data limits and track usage.

2.7.1 How to Set Data Limits on the RUTX50:

1. **Login to the Web Interface:**
   - Go to 192.168.1.1 and log in to the router.
2. **Navigate to the SIM Settings:**
   - Go to **Network** > **Mobile** > **Data Usage**.
3. **Set Data Limit:**
   - In the **Mobile Data** section, you can specify a **data usage limit**.
   - Enter the maximum data limit (in MB or GB) for the SIM card's usage.
   - Optionally, you can configure notifications to alert you when you approach the data limit.
4. **Apply and Monitor:**
   - Once set, the router will track the data usage and notify you when it reaches the configured threshold.

Example Use Case:

- Set a monthly data limit of 10GB to ensure that the SIM card doesn't exceed the monthly data allowance provided by the carrier.
- Set up a notification at 8GB of usage to inform the user that they are approaching the limit.

2.8 Blocking Unwanted Websites

You can block specific websites on the RUTX50 to ensure secure browsing, restrict access to undesirable content, or enforce company policies.

2.8.1 How to Block Websites on RUTX50:

1. **Login to the Web Interface:**
   - Go to 192.168.1.1 and log in.
2. **Navigate to the URL Filtering Settings:**
   - Go to **Network** > **Firewall** > **Web Filtering**.
3. **Enable URL Filtering**:
   - Enable the **URL Filtering** option.
4. **Add Blocked Websites**:
   - In the **Blocked URLs** section, you can specify a list of websites to block. For example, enter example.com to block access to this site.
   - You can use wildcards (e.g., *.example.com) to block entire domains or specific subdomains.

5. **Apply and Monitor**:
    - Click **Save & Apply** to activate the settings.
    - Test the configuration by trying to access a blocked website from a connected device.

Example Use Case:

To block social media websites (e.g., Facebook and Twitter):

- Enter facebook.com and twitter.com in the **Blocked URLs** section.
- Apply the changes, and users on the network won't be able to access these websites.

2.9 Guideline for SIM insertion

Here is a step-by-step guideline for inserting a SIM card into the RUTX50 router:

2.9.1 Power Off the RUTX50

Before inserting or removing a SIM card, always make sure the router is powered off to avoid any potential damage to the SIM card or the router's internal components.

- **Step 1**: Turn off the **RUTX50** by pressing the **power button** (or disconnecting the power supply).

2.9.2 Locate the SIM Card Slot

The **SIM card slot** is located on the **side** or **back** of the RUTX50 router, depending on the model. For the RUTX50, there are typically two SIM card slots (for **dual SIM cards**).

- **Step 2**: Locate the SIM card slot panel on the router.
    - **SIM 1** and **SIM 2** are usually labeled clearly next to the slots.

2.9.3 Open the SIM Slot Cover

- **Step 3**: Depending on the design, you may need to **open the plastic cover** to access the SIM card slots.
    - Some models have a small tab or latch that you can lift or slide to reveal the SIM slots.

2.9.4 Insert the SIM Card

- **Step 4**: **Insert the SIM card** into the designated slot (either **SIM 1** or **SIM 2**).
    - Ensure the **metal contacts** of the SIM card are facing **down** and **towards the router's internals**.
    - Align the **notch** of the SIM card with the slot to ensure correct orientation. The notch ensures the SIM is inserted in the correct way, preventing any damage to the card or slot. **Note**: The SIM card should click into place once it is properly inserted.

2.9.5 Close the SIM Slot Cover

- **Step 5**: After the SIM card is inserted, **close the cover** for the SIM card slot to keep it protected.
    - Ensure the cover is securely closed to prevent dust or moisture from entering.

2.9.6 Power On the Router

- **Step 6**: Once the SIM card is securely inserted, **power on the router** by pressing the power button or reconnecting the power supply.

2.9.7 Check for Network Signal

- **Step 7**: Wait for the router to boot up. It will automatically detect the inserted SIM card and attempt to connect to the mobile network.
    - Check the **LED indicators** on the front panel of the router to verify a successful connection:
        - **Signal LED**: Indicates the strength of the mobile network signal.
        - **LTE/4G Indicator**: Lights up once a mobile data connection is established.

2.9.8 Troubleshooting

If the SIM card is not recognized or the router fails to establish a connection, try the following troubleshooting steps:

- **Check the SIM card**: Ensure that the SIM card is active and properly inserted.
- **Check the network coverage**: Ensure that the router is in an area with mobile network coverage.
- **Check the APN settings**: Make sure the **Access Point Name (APN)** is correctly set up for your mobile carrier.
- **Reboot the router**: If necessary, power cycle the router after reinserting the SIM card.

2.10 APN Settings

2.10.1 Accessing the Web Interface

1. **Connect to the Router**:
    - Connect your computer to the router via **Wi-Fi** or **Ethernet**.
2. **Open the Web Interface**:
    - In your browser, enter the router's IP address (usually 192.168.1.1).
    - Login using your **username** and **password**. The default credentials are typically:
        - **Username**: admin
        - **Password**: admin (if not changed)

2.10.2 Navigate to the Mobile Settings

1. Once logged in, go to the **Network** tab on the left sidebar.
2. Select **Mobile** from the options under **Network**.

2.10.3 Configuring the APN Settings

1. In the **Mobile** section, you will see a sub-tab for **Data** settings.
2. Find the **APN Settings** section. Here, you will need to enter the relevant information provided by your mobile carrier.
    - **APN Name**: The APN provided by your carrier (e.g., internet, web.vodafone.com, fast.t-mobile.com).
    - **Username**: (Optional, depending on the carrier) Some carriers may require a username for connection (e.g., user).
    - **Password**: (Optional, depending on the carrier) Similar to the username, the password may also be required by some carriers (e.g., pass).
    - **Authentication Type**: (Optional) Select the authentication type, if required by your carrier:
        - **PAP** (Password Authentication Protocol)
        - **CHAP** (Challenge Handshake Authentication Protocol)
    - **MCC (Mobile Country Code)** and **MNC (Mobile Network Code)**: These are often auto-filled based on the SIM card and country. However, you can manually enter them if needed.
    - **APN Type**: Typically, the **default** APN type should be selected (you can choose **default, supl** if required).

2.10.4 Save the Settings

1. After entering the correct APN settings for your mobile carrier, click **Save & Apply** to save the configuration.

2.10.5 Reboot the Router

1. **Reboot** the router to ensure the new APN settings are applied properly. You can do this from the **System** tab, under **Reboot**.
2. After rebooting, the router should attempt to establish a mobile data connection using the new APN settings.

2.10.6 Verify the Connection

1. After rebooting, check the **LED indicators** on the front panel of the router:
    - **Signal LED**: Indicates the strength of the mobile network signal.
    - **LTE/4G Indicator**: This should light up if the connection is successful.
2. You can also check the **Status** page in the **Web Interface** to see the current mobile data connection status.

2.10.7 Common Troubleshooting Tips

1. **No Signal or No Connection**:
    - Check if the **SIM card** is properly inserted and active.
    - Verify that the **APN settings** are correct for your carrier.
    - Ensure you are in an area with **good mobile coverage**.
2. **APN Not Saving**:
    - Ensure there are no typos or formatting issues with the **APN** settings.
    - Double-check the **MCC** and **MNC** codes if manually entered.
3. **Check SIM Card Compatibility**:
    - Ensure the SIM card is compatible with the RUTX50 (micro or nano SIM).

3. 5G Indoor CPE

3.1 CPE system architecture

The PEGATRON MG54AX is a 5G Fixed Wireless Access (FWA) gateway that combines advanced connectivity features suitable for both residential and enterprise applications. Its key specifications are as follows:

- Processor: Qualcomm IPQ5018
- Memory: 128MB Flash and 512MB DDR RAM
- Wi-Fi: Wi-Fi 6 support with 2.4GHz 2x2 and 5GHz 4x4 configurations
- Ethernet Ports: Two 1GbE LAN/WAN ports
- 5G NR Support: Sub 6 GHz, compliant with 3GPP Release 16 in both Standalone (SA) and Non-Standalone (NSA) modes
- 5G Bands:
    - Sub 6 GHz: n1, n2, n3, n5, n7, n8, n12, n13, n14, n18, n20, n25, n26, n28, n29, n30, n38, n40, n41, n48, n66, n70, n71, n75, n76, n77, n78, n79
    - LTE Bands:
        - FDD: B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B66, B71
        - TDD: B34, B38, B39, B40, B41, B42, B43, B46(LAA), B48
        - DL 4x4 MIMO: B1, B2, B3, B4, B7, B25, B30, B38, B40, B41, B42, B43, B48, B66
- Operating Temperature: 0°C to +35°C
- Dimensions: 221 mm (H) x 110 mm (W) x 105 mm (D)

3.2 Wireless Access Interfaces

This **CPE** is a **5G Fixed Wireless Access (FWA)** device, which means it supports high-speed internet connectivity via 5G and wireless access technologies. Specifically, regarding wireless access interfaces for the MG54AX, the device likely supports the following:

3.2.1 5G NR (New Radio)

- **Interface**: **5G NR (Sub 6 GHz)** for high-speed wireless broadband connectivity.
- **Use Case**: The MG54AX is designed to provide internet access via 5G networks, supporting both **standalone** (SA) and **non-standalone** (NSA) modes of 5G.
- **Features**:
    - It supports **sub 6 GHz bands**, ensuring high-speed connectivity with reduced latency and increased reliability.
    - It allows users to leverage the **5G mobile network** to get internet access at much higher speeds compared to traditional 4G LTE.
    - Typical speeds range from **100 Mbps to over 1 Gbps**, depending on the deployment and network conditions.

3.2.2 Wi-Fi 6 (802.11ax)

- **Interface**: **Wi-Fi 6** for local wireless access within homes or businesses.
- **Use Case**: Provides high-speed Wi-Fi connections to devices such as smartphones, laptops, smart TVs, and IoT devices.
- **Features**:
    - It supports both **2.4 GHz** (2x2 MIMO) and **5 GHz** (4x4 MIMO) bands, providing higher throughput and efficiency compared to previous Wi-Fi standards.
    - Wi-Fi 6 allows for better handling of multiple devices simultaneously through technologies like **OFDMA** (Orthogonal Frequency Division Multiple Access) and **MU-MIMO** (Multi-User, Multiple Input Multiple Output), making it ideal for environments with many connected devices.

3.2.3 Ethernet (Wired)

- **Interface**: **Gigabit Ethernet** ports (1GbE LAN/WAN).
- **Use Case**: For wired broadband connectivity, especially for devices that need stable and high-speed internet access without relying on wireless.
- **Features**:
    - The MG54AX includes **Ethernet ports** that allow for direct wired connections to devices (e.g., PCs, servers, or network switches), providing more reliable connections than wireless.
    - It supports **LAN and WAN configurations**, which means it can be used as a gateway for distributing internet from 5G to other devices in a wired setup.

3.2.4 LTE (Fallback)

- **Interface**: **LTE** (4G) for areas with poor 5G coverage or as a fallback option.
- **Use Case**: In areas where 5G signal strength is insufficient or unavailable, the device can switch to **LTE** to provide internet access.

- **Features**:
    - The MG54AX supports a wide range of **LTE bands** (FDD and TDD), ensuring compatibility with various cellular networks worldwide.
    - LTE provides reliable connectivity at speeds lower than 5G but still offers decent performance for most use cases.

3.2.5 Key Wireless Access Interfaces for the MG54AX:

- **5G NR (Sub 6 GHz)** for ultra-fast 5G connectivity.
- **Wi-Fi 6 (2.4 GHz / 5 GHz)** for local wireless network access.
- **Gigabit Ethernet** for wired high-speed connections.
- **LTE** for fallback in areas with poor 5G coverage.

3.3 Security

3.3.1 Latest WPA Support

- **WPA3**: The latest Wi-Fi security protocol is likely supported, offering stronger encryption and protection against attacks like brute-force. It includes:
    - **Simultaneous Authentication of Equals (SAE)** to improve password security.
    - Enhanced protection for public networks with **Enhanced Open**.
    - Backward compatibility with **WPA2** for devices that do not yet support WPA3.

3.3.2 Rogue Access Point Detection and Prevention

- Modern devices typically include **rogue access point detection**, which identifies unauthorized access points attempting to connect to the network.
    - Alerts administrators when rogue access points are found.
    - Can block or restrict access to unauthorized access points, improving the overall security of the network.

3.3.3 IP Security (IPSec), PPTP, IP Filtering

- **IPSec (Internet Protocol Security)**: Provides secure encrypted communication over IP networks and is widely used for setting up **site-to-site** and **remote access** VPNs.
- **PPTP (Point-to-Point Tunneling Protocol)**: While less secure, it is sometimes supported for compatibility with older VPN clients. However, it's typically not recommended due to known vulnerabilities.
- **IP Filtering**: Allows filtering based on **source or destination IP addresses**, restricting or allowing traffic based on defined rules to prevent unwanted or malicious access.

3.3.4 MAC Address Authentication

- **MAC address filtering** is often available, allowing only devices with specific **MAC addresses** to connect to the network.
    - This adds an additional layer of security by controlling which devices can access the network.
    - However, **MAC addresses can be spoofed**, so while it's a useful measure, it shouldn't be relied upon as the sole security feature.

3.4 5G Network settings

3.4.1 Network Mode

- **Standalone (SA)**: Independent 5G network.
- **Non-Standalone (NSA)**: Uses 4G LTE as anchor, adding 5G for data.

3.4.2 5G Band Selection

- **Sub 6 GHz** for coverage and **mmWave** for ultra-fast speeds.
- The device may automatically select the best band, or you can manually choose.

3.4.3 Carrier Aggregation (CA)

- Combines multiple 5G bands for increased speeds.

3.4.4 APN Settings

- Manually configure **Access Point Name (APN)** for network access (based on carrier).

3.4.5 Roaming Settings

- Enable or disable **data roaming** while traveling.

3.4.6 IPv6/IPv4

- Supports **IPv6** for more efficient addressing, with **Dual Stack** for both protocols.

3.4.7 QoS Settings

- Prioritize traffic for specific applications like video or gaming.

3.4.8 DNS Settings

- Customize **DNS** servers for faster or more secure connections.

3.4.9 Signal Monitoring

- View **5G signal strength** and connection type.

3.4.10 Antenna Settings

- Manage **MIMO** or external antennas for better reception.

3.4.11 Security

- Enable **WPA3**, **firewall**, and **MAC filtering** for secure connections.

3.5 Wifi Settings

3.5.1 Wi-Fi Mode

- **2.4 GHz** and **5 GHz**: The device likely supports both **2.4 GHz** (for longer range) and **5 GHz** (for faster speeds and less interference).
- **Wi-Fi 6 (802.11ax)**: Supports the latest Wi-Fi standard for faster speeds, better capacity, and improved efficiency.

3.5.2 Wi-Fi SSID

- **SSID (Service Set Identifier)**: Set the name of your wireless network. You can have different SSIDs for **2.4 GHz** and **5 GHz** bands, or set the same SSID for both.

3.5.3 Wi-Fi Security

- **WPA3**: The latest security standard, offering stronger encryption.
- **WPA2**: Available for backward compatibility, though WPA3 is recommended for stronger protection.
- **Encryption**: Choose **AES** (Advanced Encryption Standard) for secure Wi-Fi encryption.

3.5.4 Channel Settings

- **Automatic Channel Selection**: The device can automatically select the best channel to avoid interference.
- **Manual Channel Selection**: Allows you to select specific channels for both **2.4 GHz** and **5 GHz** if you encounter interference.

3.5.5 Wi-Fi Bandwidth

- **20/40/80 MHz**: Set the bandwidth for your 5 GHz network. Wider bandwidth (80 MHz) offers faster speeds but may cause more interference.
- **20 MHz**: Typically used for the 2.4 GHz band to avoid congestion.

3.5.6 Guest Network

- Set up a separate **guest network** for visitors, isolating their traffic from your main network for security.

3.5.7 MAC Address Filtering

- **MAC Filtering**: Restrict network access to specific devices by allowing only certain **MAC addresses**.

3.5.8 Wi-Fi Power Settings

- **Transmit Power**: Adjust the power level for Wi-Fi signal range. Lower power can help reduce interference, while higher power offers better coverage.

3.5.9 Wi-Fi Optimization Features

- **OFDMA (Orthogonal Frequency Division Multiple Access)**: A feature of Wi-Fi 6 that improves efficiency by allowing simultaneous transmission to multiple devices.
- **MU-MIMO (Multi-User, Multiple Input, Multiple Output)**: Allows the device to communicate with multiple devices at once for better overall performance.

3.5.10 Wi-Fi Scheduling

- **Wi-Fi Scheduling**: Enable or disable Wi-Fi during specific times of the day for energy savings or security purposes.

3.6 Connecting 5G Indoor CPE to 5G and WiFi Network

3.6.1 Connecting to the 5G Network

1. **Insert SIM Card (if applicable)**:
    - Ensure your **5G SIM card** is inserted into the device.
2. **Power On the Device**:
    - Plug in and turn on you CPE. It should automatically start searching for available **5G networks**.
3. **Network Mode Selection**:
    - Access the device's **admin interface** via a web browser(by typing the device's IP address, 192.168.1.1).
    - Navigate to the **5G Network Mode** settings and select either:
        - **Standalone (SA)**: Full 5G network.
        - **Non-Standalone (NSA)**: 5G using 4G LTE for control.

3.6.2 Check Connection Status:

- Once connected, you should see the **5G status indicator** on the CPE or in the admin interface, confirming you're connected to the **5G network**.

3.6.3 Connecting to the Wi-Fi Network

1. **Wi-Fi Configuration (Router Mode)**:
   - Ensure the **Wi-Fi feature** on the device is enabled. This is usually enabled by default, but you can check or modify settings from the **Wi-Fi Settings** page in the admin interface.
2. **Wi-Fi Network Settings**:
   - **SSID (Network Name)**: Set the **Wi-Fi network name (SSID)**. You can have separate SSIDs for **2.4 GHz** and **5 GHz** bands or use the same SSID for both.
   - **Security Settings**: Set the **Wi-Fi security** to **WPA3** or **WPA2** for encryption. Use **AES** for the strongest encryption.
   - **Password**: Set a strong **Wi-Fi password**.
3. **Select Wi-Fi Band**:
   - Configure the **Wi-Fi bands**:
     - **2.4 GHz**: Better range but slower speeds, typically used for devices farther away.
     - **5 GHz**: Faster speeds, suitable for devices closer to the CPE with high data requirements.
4. **Connect Devices to Wi-Fi**:
   - On your phone, laptop, or any other Wi-Fi device, search for the **SSID** you set up.
   - Select the network and enter the Wi-Fi password to connect.
5. **Check Wi-Fi Connection**:
   - Once connected, you should be able to browse the internet using the **5G connection** shared via Wi-Fi.
   - The **CPE's Wi-Fi status indicator** should show that the device is broadcasting the Wi-Fi network.

3.6.4 Flexible guest access with device isolation Captive

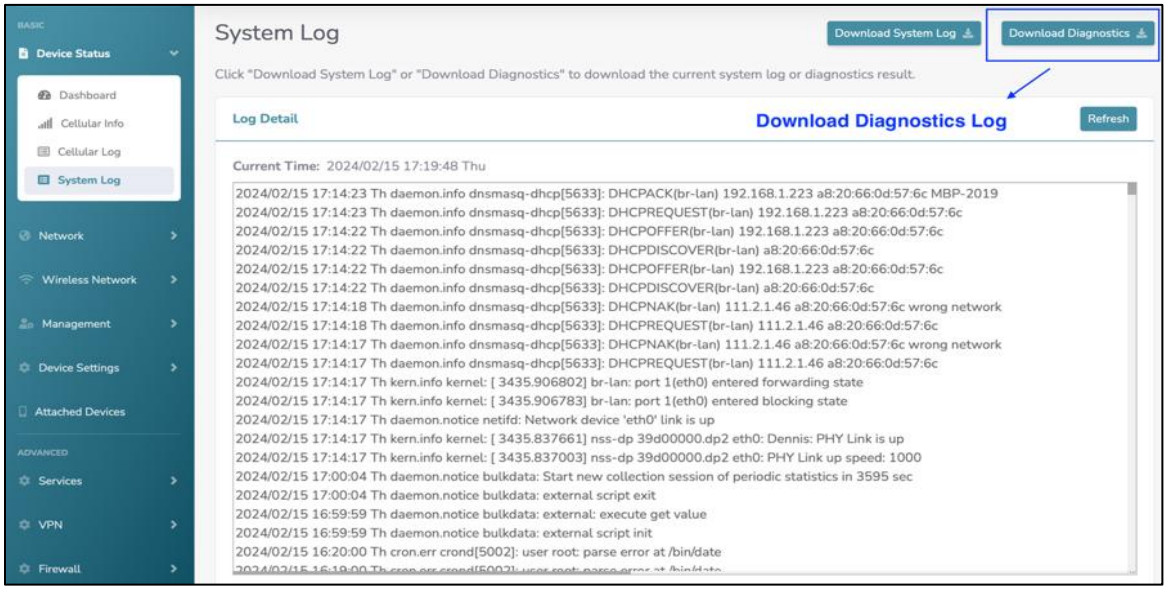
1. **Enable Guest Network**:
   - Access the admin interface and enable the **Guest Network** with a unique **SSID** (e.g., "Guest_Network").
2. **Device Isolation**:
   - Enable **Client Isolation** or **AP Isolation** in the guest network settings to prevent devices on the guest network from communicating with each other or your main network.
3. **Wi-Fi Security**:
   - Set **WPA2** or **WPA3** encryption with a password for the guest network.
4. **Enable Captive Portal**:
   - Turn on the **Captive Portal** feature, allowing you to customize a login page where guests can accept terms or enter a password.
5. **Apply Settings**:
   - Save the settings and restart the device if needed. Guests will now be isolated and redirected to the captive portal for access.

3.7 Trouble Shooting

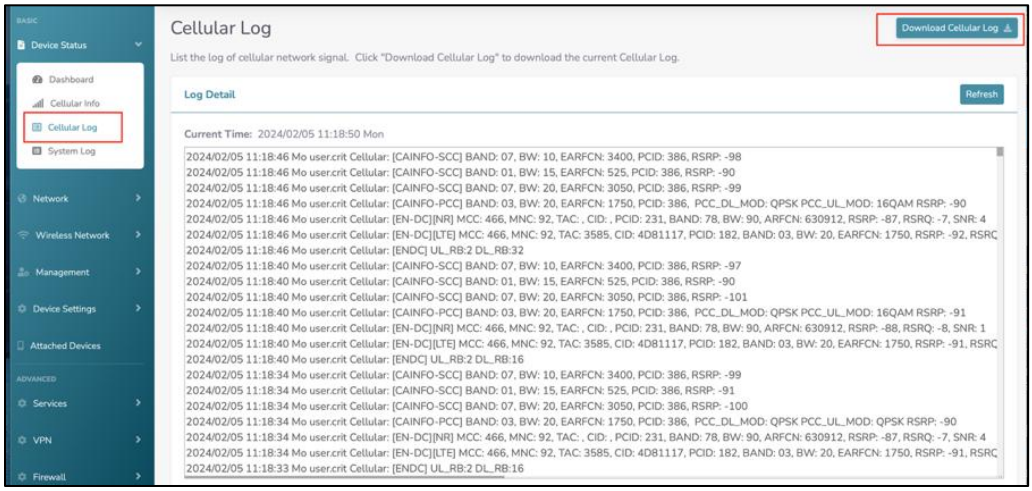
Steps to capture Diagnostics Log

1.1 Check Firmware version: access 192.168.1.1 Web GUI, go to “Device Status -> Dashboard -> FIRMWARE VERSION”, make sure Firmware version should be 2.0.1.x_x, in following picture the Firmware version is 2.0.1.1_01

1.2 Go to “Device Status -> System Log”, and press “Download Diagnostics” to download Diagnostics Log. (The Diagnostics also included Cellular Log).



1.3 If only the Cellular Log is required, go to "Device Status -> Cellular Log, and press “Download Cellular Log" to retrieve it.



3.7.1 General Troubleshooting Steps

1. **Check Physical Connections:** Ensure that all cables (power, Ethernet, SIM card) are securely connected.

2. **Reboot the Device:** Power cycle the MG54AX CPE by unplugging it from the power outlet, waiting 30 seconds, and plugging it back in.

3. **Check LED Indicators:** Observe the LED indicators on the front panel to identify potential issues. Refer to the device overview section for LED descriptions.

4. **Ping Test:** Use the ping command to test network connectivity. Open a command prompt or terminal and type `ping 192.168.1.1` (replace with the MG54AX's IP address). A successful ping indicates basic network connectivity.

5. **Web Interface Access:** Verify that you can access the MG54AX's web interface. If you cannot, check your computer's IP address and ensure it is on the same subnet as the MG54AX.

6. **Review System Logs:** Check the system logs in the web interface for error messages or warnings that may provide clues about the problem.

7. **Check SIM Card:** Make sure the SIM card is inserted correctly and is active. Try the SIM card in another device to confirm it is working.

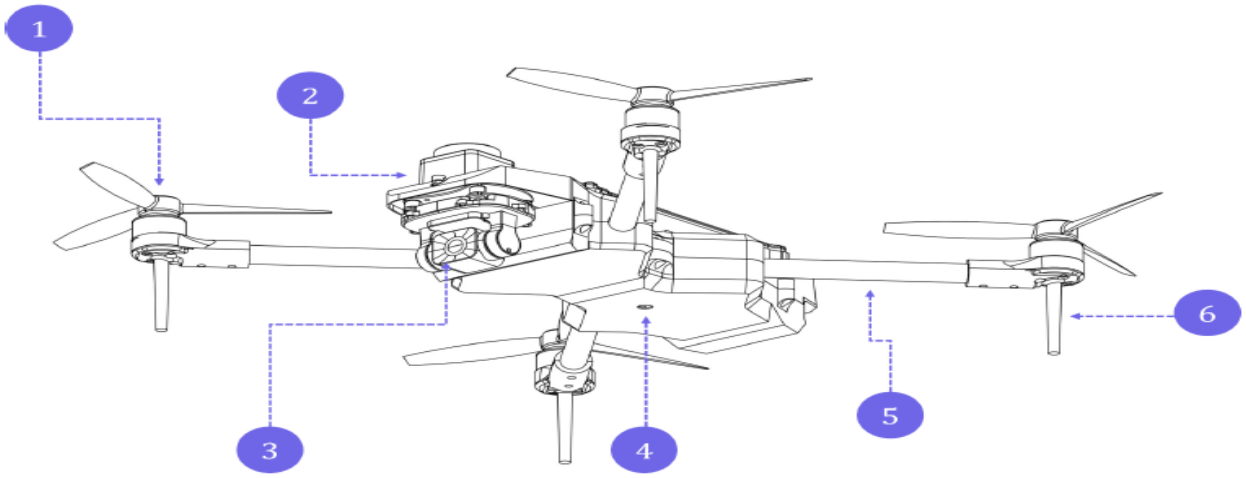
8. **Test with Different Devices:** Try connecting different devices (computers, smartphones) to the MG54AX to rule out device-specific issues

4. 5G Drone

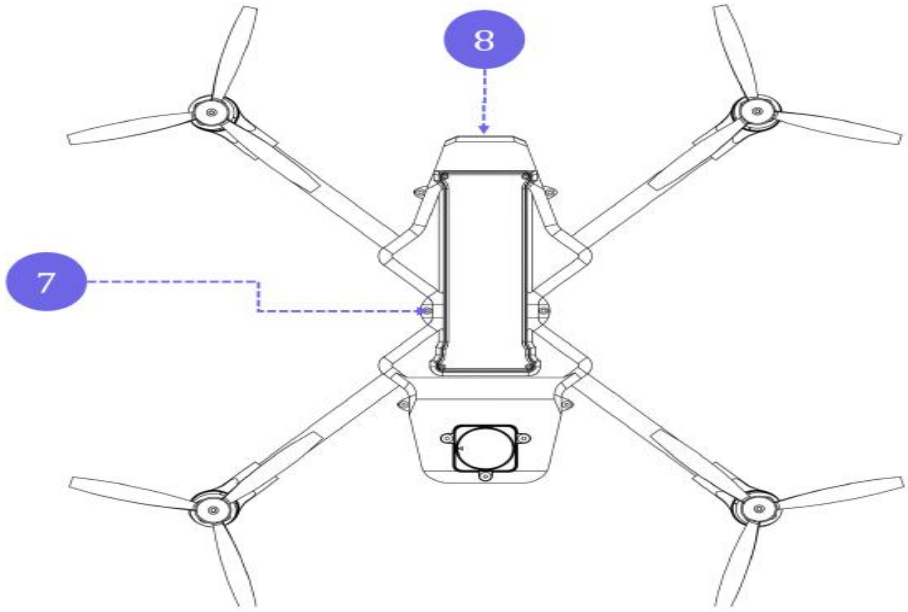
4.1 Introduction -

Suparna features both an 360 degree Laser Sensing System and Downward Vision Systems, allowing for hovering and flying indoors as well as outdoors and for automatic Return to Home. The aircraft has a maximum flight speed of 54 kmph in outdoor stable wind conditions and 15 kmph indoor environment (**This has been tested under controlled environment. Do not attempt to imitate**) and maximum flight time of 18 minutes.

4.2 Drone System Architecture



1:	Propellers	4:	Downward Facing Vision System
2:	360 Lidar	5:	Arms
3:	Gimbal Camera	6:	Landing Gear



7:	Removable Battery	8:	GPS & External Compass

4.3 System Specification-

Drone Type	Quadcopter
Frame Material	Carbon Fiber
Size (Propeller to Propeller)	470mm
Weight	1300gm
Extra Payload	500gm
Max Altitude-Outdoor	50 m AGL (◉Check Local Rules and Regulation)
Max Operating Altitude	750 m AMSL
Failsafe Features	1. Low Battery 2. Critical Battery 3. Ground Station Connection Loss
Indoor Features	360 Degree Obstacle Avoidance System. Vision Based Odometry 10cm Precision for Indoor Altitude Hold. Real Time Video Streaming. Position Visualizations in 2D/3D Space. ROS Support
5G Features	N78 Bands for Captive Networks. 5G Compatible Specialized GCS.
Battery Type	Li-ion 4 Cell
Battery Capacity	4500mAh
Battery Charging/Discharging Cycle	300
Flight Time	18 Minutes
Communication Channel Internet -	5G with LTE Fallback Or WiFi:6
Cruise Speed	54 kmph (Outdoor) 15kmph(Indoor)
GCS	iDronam for Enterprise

Hovering Accuracy Vertical:	±0.2 m (with Vision Positioning), ±1 m (with GNSS Positioning + Barometer) Horizontal: ±0.3 m (with Vision Positioning), ±1.5 m (with GNSS Positioning)
Operating Temperature	5° to 40° C
Image Sensor (Default)	1/2.7 Inch, 2 MP effective resolution
FOV	Horizontal 160°

4.4 Aircraft Highlights-

The Suparna represents a significant leap in unmanned aerial technology, offering a blend of high-speed connectivity, advanced navigation, and versatile functionality. This compact drone is designed for a variety of applications, from commercial and industrial use to recreational and research purposes.

5G Connectivity and Control: Equipped with support for a 5G nano SIM, this drone ensures seamless operation through high-speed cellular networks.

Dual Connectivity Options: Apart from 5G, the drone also features Wi-Fi connectivity, allowing it to operate efficiently in both urban and remote areas.

Advanced Processing Engine: Powered by an onboard processor, the drone is adept at AI/ML analytics, making it suitable for applications that require real-time data processing, such as image analysis and environmental monitoring.

Autonomy and Navigation: The drone boasts sophisticated autonomous capabilities like Visual Inertial Odometry (VIO) for accurate positioning, advanced path planning algorithms, and PX4 software for autonomous flight control.

360-Degree Obstacle Avoidance: With depth estimation and obstacle detection technology, the drone can navigate safely through challenging terrains. It employs mapping and Visual Obstacle Avoidance (VOA) systems to detect and avoid obstacles in all directions.

Payload Capacity: Designed to carry payloads of 500g, this drone is suitable for a variety of tasks, including delivery, surveying, and equipment transport.

Outdoor Navigation System: The inclusion of both GPS makes it reliable for critical missions.

Geo-Fencing: This feature allows users to set virtual boundaries for the drone, ensuring it operates within predefined areas, enhancing safety and compliance.

High-Performance Sensors: Equipped with sophisticated tracking and image sensors, the drone can capture high-quality images and videos, and efficiently track subjects or terrain features.

Connectivity and Ports: The drone includes a 5G modem supporting the available 5G bands, an Ethernet/management port, and dual-band Wi-Fi-6, providing various options for data transmission and device management.

Purpose and Target Users

The Suparna, with its advanced technological capabilities, is an invaluable tool tailored for a diverse group of users, including students, trainee professionals, researchers, and faculty members across various disciplines. This drone's unique features make it an ideal fit for educational, professional training, and research environments.

4.5 Sensitivity Of A Sensor

- **IMU Sensitivity**: Affects the drone's stability, control, and orientation, crucial for GPS-denied navigation.
- **Camera Sensitivity**: Improves performance in low-light conditions and accuracy of VIO for autonomous positioning.
- **LiDAR Sensitivity**: Ensures precise obstacle detection and mapping, crucial for collision avoidance and 3D environment modeling.
- **Barometer Sensitivity**: Allows precise altitude control, vital for maintaining stable flight during specific missions.
- **GPS Sensitivity**: Enhances positional accuracy for autonomous navigation, especially in open environments.

4.6 Limitation Of Sensors Devices

Sensors used in a drone provide critical data for navigation, obstacle detection, and stabilization, each sensor type comes with its own limitations. Understanding these limitations helps in designing systems to compensate for potential shortcomings and ensures reliable performance in various flight scenarios.

4.6.1 Camera (for Visual Inertial Odometry - VIO)

- **Limitations**:
  - **Low Light Conditions**: Cameras can struggle to perform well in low-light environments or in very bright conditions (e.g., direct sunlight). This can impact visual data used for VIO or obstacle detection.
  - **Motion Blur**: Rapid movement or poor lighting can cause motion blur, making it difficult to track visual features accurately.
  - **Limited Field of View**: Cameras have a limited field of view, which can restrict the area the drone can "see" at once, requiring careful planning for complete environment mapping.

- **Impact**:
  - **Visual tracking** may fail in low-light or highly dynamic conditions, requiring fallback systems like IMU or LiDAR for reliable navigation.

4.6.2 LiDAR (Light Detection and Ranging)

- **Limitations**:
  - **Limited Range**: LiDAR sensors typically have a limited range (usually tens to hundreds of meters). Objects beyond this range cannot be detected, limiting the drone's ability to plan long-range missions.
  - **Vulnerability to Environmental Conditions**: LiDAR can be affected by weather conditions, such as rain or fog, which may scatter the laser beams and reduce its accuracy.
  - **Cost and Power Consumption**: High-performance LiDAR units can be expensive and consume significant amounts of power, limiting the drone's operational time.
- **Impact**:
  - **Obstacle detection** may not be effective in poor weather or at long distances, potentially leading to collision risks in dynamic environments.

4.6.3 Barometer

- **Limitations**:
  - **Pressure Variations**: Barometers measure air pressure to estimate altitude, and they can be sensitive to atmospheric changes that aren't related to altitude (such as weather fronts).
  - **Temperature Sensitivity**: Barometers can be affected by changes in temperature, leading to inaccurate altitude readings if not properly calibrated.
  - **Low Precision**: Barometers often provide less precision compared to other altitude sensors, which can be a limitation in precision navigation or low-altitude flight.
- **Impact**:
  - **Altitude control** might suffer from minor inaccuracies, especially in rapidly changing environmental conditions, such as in mountainous or coastal areas where air pressure fluctuates frequently.

4.6.4 GPS (Global Positioning System)

- **Limitations**:
  - **Signal Loss**: GPS performance degrades significantly in GPS-denied environments, such as indoors, under dense canopies, or in urban canyons.
  - **Accuracy**: Standard GPS is typically accurate within 1-5 meters, and even high-precision systems like RTK (Real-Time Kinematic) GPS can still have some level of error, especially in difficult conditions.
  - **Vulnerable to Jamming/Interference**: GPS signals are susceptible to jamming or spoofing, where an external signal may disrupt the GPS system or provide false information.
- **Impact**:
  - **Autonomous navigation** relies on GPS for precise location tracking, and in the absence of GPS, the drone must rely on other sensors (like IMU or VIO) to avoid drift and maintain accuracy.

4.7 Safety Procedure-

Operating a Drone indoors requires careful attention to safety and precautionary measures to ensure both the operator's safety and the integrity of the drone. Here are some guidelines for the safe operation of the drone in indoor environments:

4.7.1 Pre-Flight Check:

1. Inspect the drone for any damage or loose parts.
2. Ensure all software and firmware are up-to-date.
3. Check the battery level and ensure it's adequately charged.
4. Test the drone's sensors and navigation systems to ensure they are functioning correctly.

4.7.2 Environmental Awareness:

1. Clear the area of people, pets, and fragile objects to minimize risk.
2. Be aware of the indoor space layout, including ceilings, walls, and any obstacles like furniture.
3. Avoid flying near air vents, as the airflow can affect the drone's stability.

4.7.3 Control and Supervision:

1. Always maintain a line of sight with the drone.
2. Do not rely solely on the drone's cameras or sensors; use visual supervision.
3. Keep the drone within a safe distance from the operator and bystanders.

4.7.4 Use of Safety Features:

1. Utilize the drone's obstacle avoidance systems to prevent collisions.
2. Engage geo-fencing features to limit the drone's operational area.
3. Use the drone's autonomy features wisely, especially in confined spaces.

4.7.5 Speed and Height Management:

1. Operate the drone at lower speeds to maintain control.
2. Avoid flying too close to the ceiling or too low to the ground to prevent crashes.

4.7.6 Interference Considerations:

1. Be aware of potential Wi-Fi or electronic interference in indoor environments that might affect drone control.
2. Test the 5G and Wi-Fi connectivity in the indoor area before flying.

4.7.7 Emergency Procedures:

1. Familiarize yourself with the drone's emergency stop function
2. Have a clear plan for what to do in case of a loss of control or other emergencies.

4.7.8 Training and Skill Level:

1. Ensure that the operator is adequately trained to handle the drone indoors.
2. Practice in a safe, controlled environment to build skill and confidence.

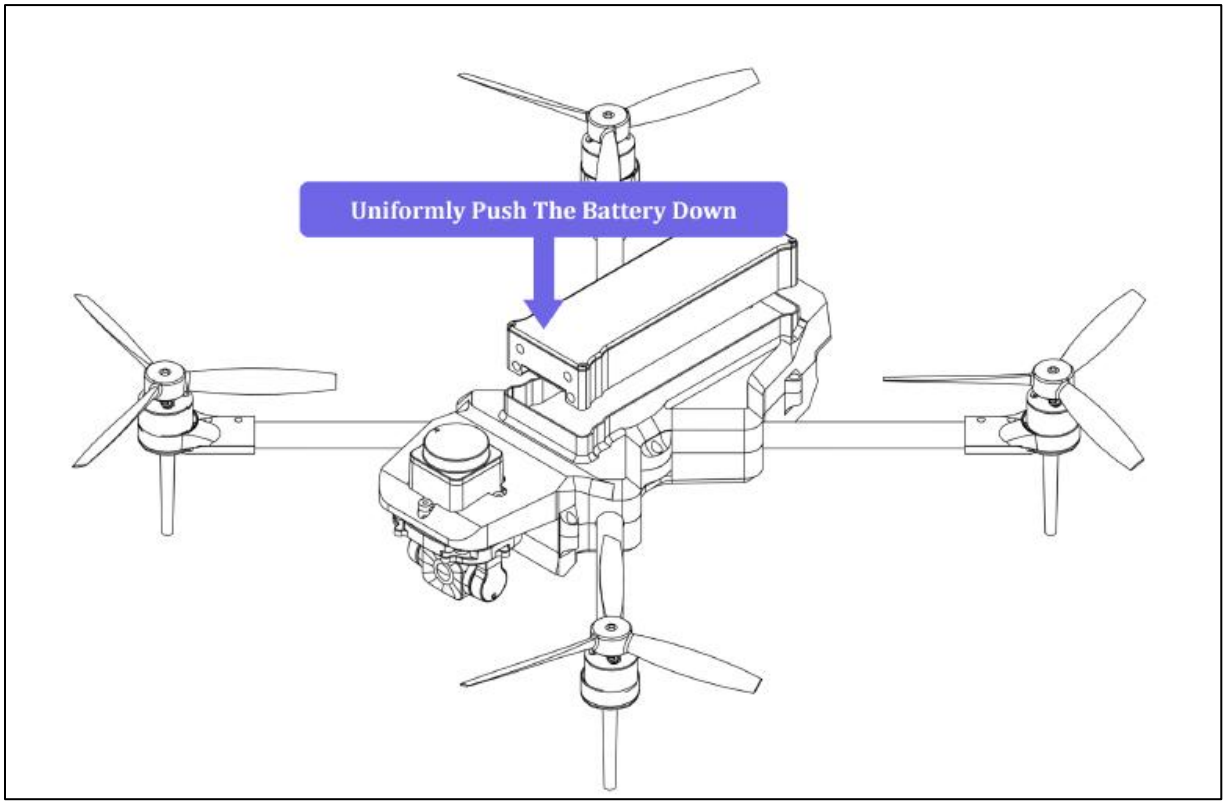
4.7.9 Legal and Ethical Considerations:

1. Abide by any institutional or organizational policies regarding drone usage indoors.
2. Respect privacy if the drone is equipped with cameras or recording devices.

4.7.10 Post-Flight Check:

1. After flying, inspect the drone for any damage.
2. Download and analyze any collected data if necessary.
3. Store the drone in a safe, dry place away from potential hazards.

4.8 Battery Handling-



Battery handling and storage are critical for maintaining the safety and longevity of the 5G-enabled mini drone. Proper care of the drone's batteries ensures optimal performance and reduces the risk of accidents. Here are detailed instructions for handling and storing the drone's batteries:

4.8.1 Charging the Battery:

Use only the charger provided with the drone or one recommended by the manufacturer.

1. Charge the battery in a well-ventilated area away from flammable materials.
2. Do not leave the battery unattended while charging.
3. Avoid charging the battery immediately after flight. Allow it to cool down first.

4.8.2 Handling the Battery:

1. Handle batteries with care. Avoid dropping them or subjecting them to impact.
2. Do not dismantle, puncture, or alter the battery in any way.
3. Keep the battery dry and away from water or moisture.
4. Avoid exposing the battery to extreme temperatures, both hot and cold.
5. If the battery appears swollen, discolored, or damaged in any way, do not use it.

4.8.3 Storage of the Battery:

1. Store batteries in a cool, dry place, away from direct sunlight and heat sources.
2. If storing for an extended period, keep the battery at a 40-60% charge level. Avoid storing it fully charged or fully depleted.
3. Check the charge level every few months and recharge to the recommended storage level if necessary.
4. Use a fireproof bag or container designed for LiPo battery storage.

4.8.3 Transporting the Battery:

1. When transporting, ensure the battery terminals are protected and cannot come into contact with metal objects.
2. Carry batteries in a dedicated, fireproof battery case.

4.8.4 Battery Disposal:

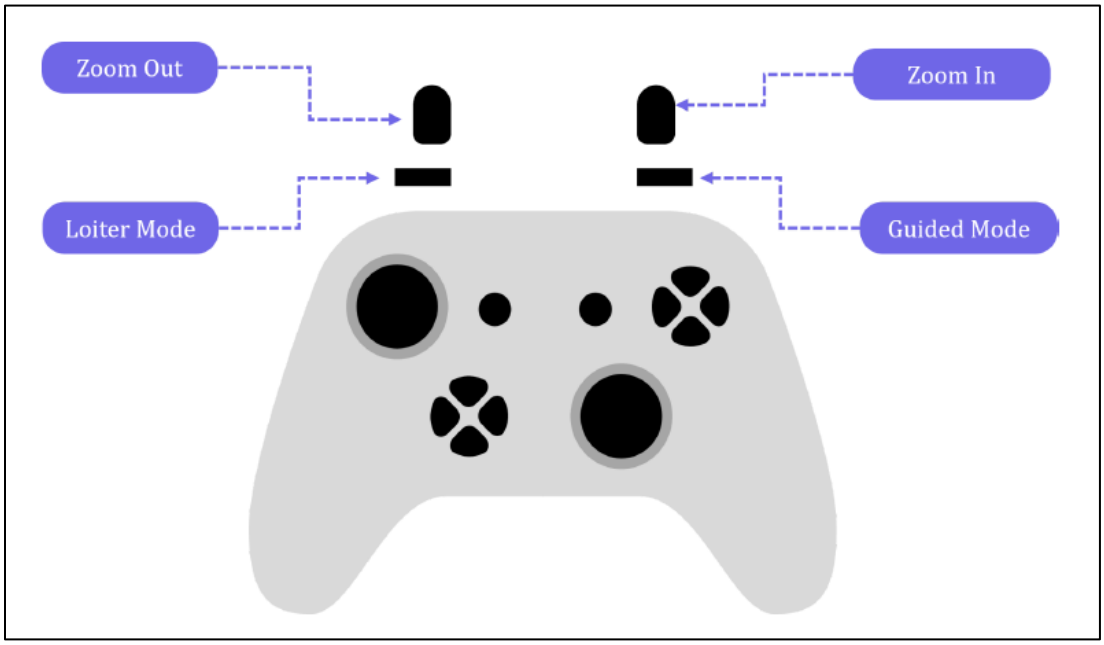
1. Do not dispose of batteries in regular trash. Batteries should be recycled according to local regulations.
2. If the battery is damaged, follow local guidelines for hazardous waste disposal.

4.8.5 General Precautions:

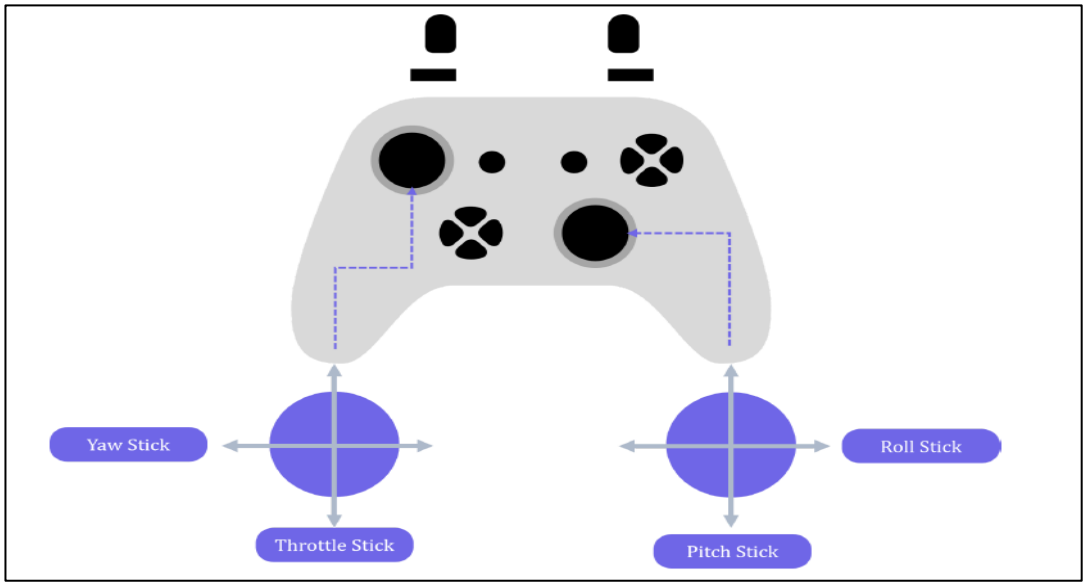
1. Never use a battery that is not specifically designed for your drone model.
2. Keep batteries out of reach of children.
3. Regularly inspect the battery for signs of wear or damage.

4.9 Flight And Companion Controller -

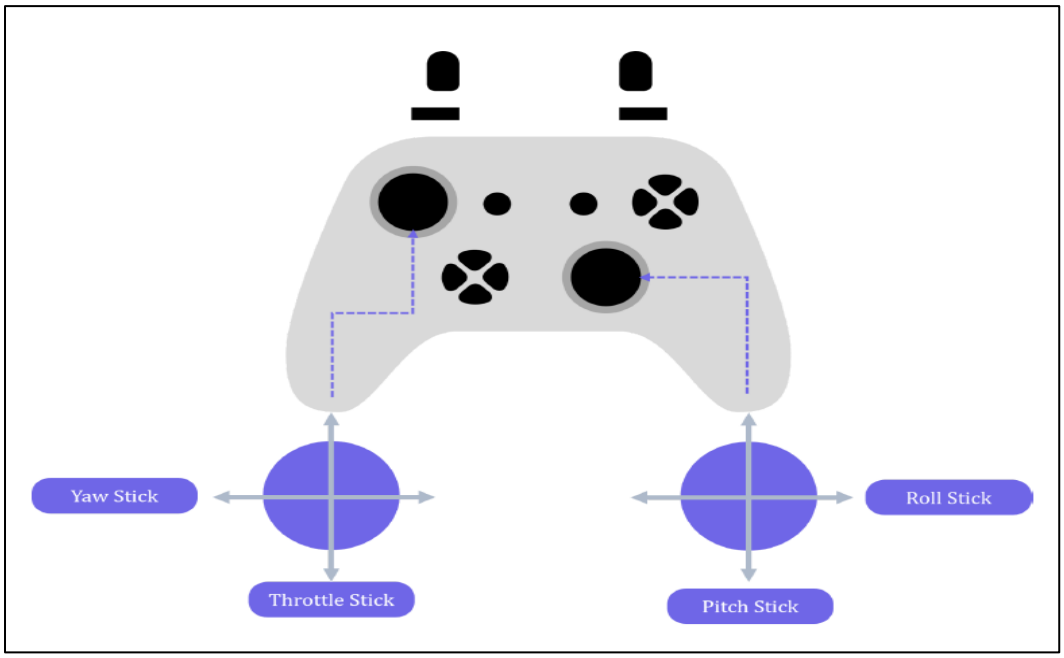
4.9.1 Joystick - Modes and Zoom



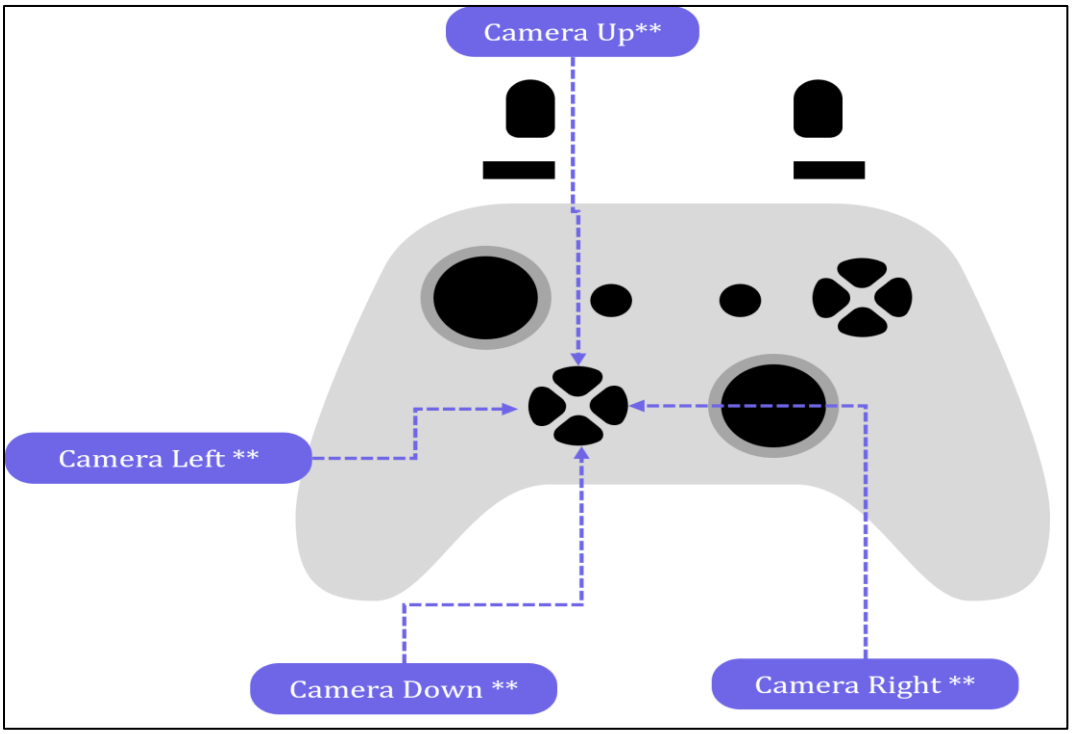
4.9.2 Joystick - Sticks and Control



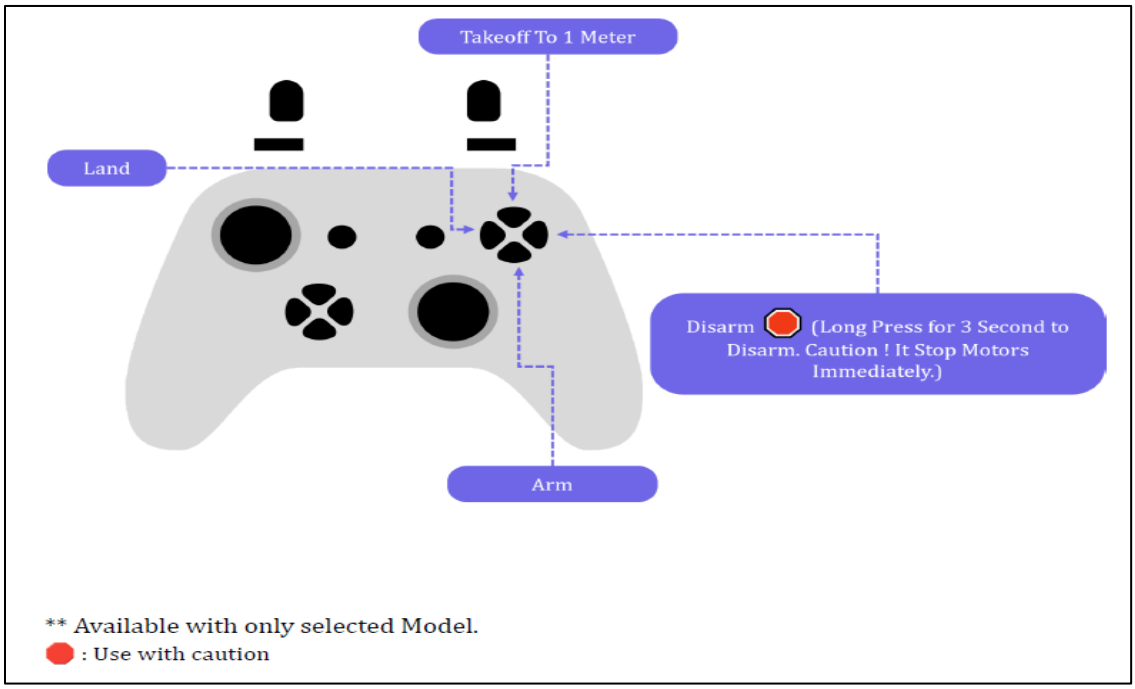
4.9.3 Joystick - Sticks and Control



4.9.4 Joystick - Camera Control



4.9.5 Joystick - Command and Special Modes



4.10 DATA AND CONTROL FLOW ARCHITECTURE

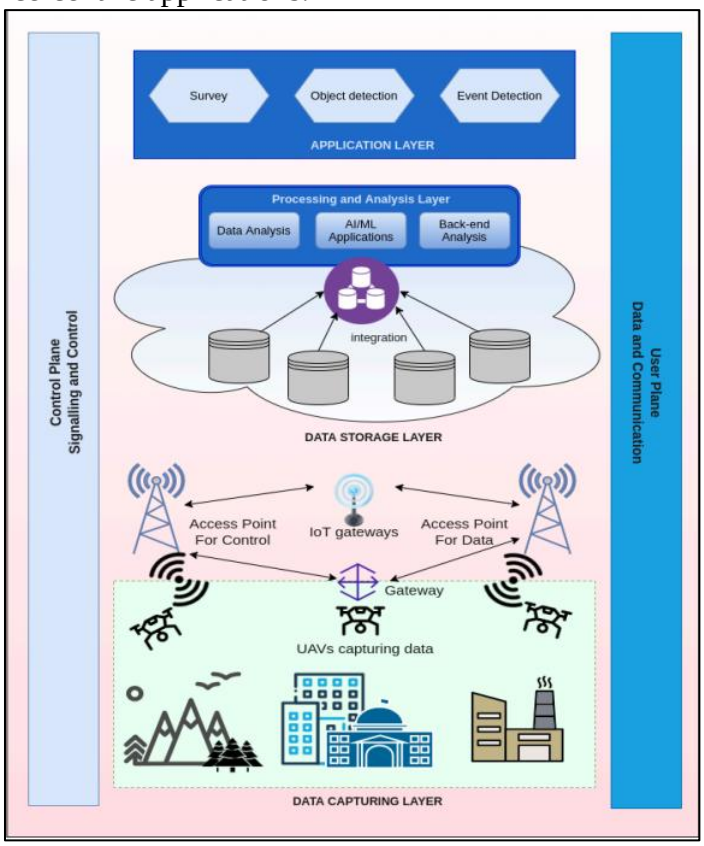
Figure below describes the proposed multilayered architecture of the system. It consists of four layers for the integration of diverse technologies and providing abstraction.

Data Capturing Layer:
This is the most important step in the whole design. The proposed system tends to offer a variety of methods like UAVs, standalone cameras, and cameras on UAVs, microphones, sensors, IoT sensors, etc. to capture data. The data capturing layer will facilitate data capturing across multiple devices with minimum complexities to end-users.

Interaction with Data Storage Layer:
The data capturing layer will provide seamless connectivity to the data storage layer.

Data Storage Layer:
This layer will accept raw data from the data storage layer and store it in the agreed format. The layer may provide facilities for data annotations and similar tasks. The major challenge here will be designing schema for the multi-domain data. The layer shall be responsible for enforcement of security policies, framing data access guidelines, and shall offer access to the data in real-time. Provisions will be made to offer data in the format as desired by the Processing and Data Analytics layer.

Processing and Data Analytics Layer:
The aim of this layer is to offer a variety of data analytics services to different applications. The layer will offer facilities for designing and developing machine learning models and data analysis models for monitoring and surveillance-centric applications.



Application Layer:
This layer is concerned with user applications. Different end-users using the system will be citizens, industry, government agencies, etc.

User interface:
Different interfaces may be offered to different users and the type of interface will be governed by the applications being offered. The data in the processed form will be accepted by this layer from the data storage layer and will be offered to end-users.

Communication pillars:

The pillars consist of the Control Plane and User Plane for providing seamless end-to-end communication between devices and layers of the system.

4.11 ON-BOARDING PROCESSING

On-board Computer Specifications

SOC Name	Broadcom BCM2711
CPU Name	ARM Cortex-A72 (ARM v8)
Core Count	4 (Quad-Core)
Architecture	64 bit
Processing Speed	1.5 GHz
RAM	4 GB LPDDR4 @ 3200 MHz
Storage	32GB

4.12 MISSION PROTOCOL

The mission sub-protocol allows a GCS or developer API to exchange mission (flight plan), geofence and safe point information with a drone/component.

The protocol covers:
Operations to upload, download and clear missions, set/get the current mission item number, and get notification when the current mission item has changed.

Message type(s) and enumerations for exchanging mission items.

Mission Items ("MAVLink commands") that are common to most systems.

The protocol supports re-request of messages that have not arrived, which allows missions to be reliably transferred over a lossy link.

Mission Types

MAVLink 2 supports three types of "missions": flight plans, geofences and rally/safe points. The protocol uses the same sequence of operations for all types (albeit with different types of Mission Items). The mission types must be stored and handled separately/independently.

Mission protocol messages include the type of associated mission in the mission_type field (a MAVLink 2 message extension). The field takes one of the MAV_MISSION_TYPE enum values: MAV_MISSION_TYPE_MISSION, MAV_MISSION_TYPE_FENCE, MAV_MISSION_TYPE_RALLY.

Mission Items (MAVLink Commands)
Mission items for all the mission types are defined in the MAV_CMD enum.

MAV_CMD is used to define commands that can be used in missions ("mission items") and commands that can be sent outside of a mission context (using the Command Protocol). Some MAV_CMD can be used with both mission and command protocols. Not all commands/mission items are supported on all systems (or for all flight modes).

The items for the different types of mission are identified using a simple name prefix convention:

4.12.1 Flight plans:

NAV commands (MAV_CMD_NAV_*) for navigation/movement (e.g. MAV_CMD_NAV_WAYPOINT, MAV_CMD_NAV_LAND)

DO commands (MAV_CMD_DO_*) for immediate actions like changing speed or activating a servo (e.g. MAV_CMD_DO_CHANGE_SPEED).

CONDITION commands (MAV_CMD_CONDITION_*) for changing the execution of the mission based on a condition - e.g. pausing the mission for a time before executing next command (MAV_CMD_CONDITION_DELAY).

Geofence mission items:

Prefixed with MAV_CMD_NAV_FENCE_ (e.g. MAV_CMD_NAV_FENCE_RETURN_POINT).

Rally point mission items:

There is just one rally point MAV_CMD: MAV_CMD_NAV_RALLY_POINT.

The commands are transmitted/encoded in MISSION_ITEM or MISSION_ITEM_INT messages. These messages include fields to identify the particular mission item (command id) and up to 7 command-specific optional parameters.

Field Name	Type	Values	Description
command	uint16_t	MAV_CMD	Command id, as defined in MAV_CMD.
param1	float		Param #1.
param2	float		Param #2.
param3	float		Param #3.
param4	float		Param #4.
param5 (x)	float / int32_t		X coordinate (local frame) or latitude (global frame) for navigation commands (otherwise Param #5).
param6 (y)	float / int32_t		Y coordinate (local frame) or longitude (global frame) for navigation commands (otherwise Param #6).
param7 (z)	float		Z coordinate (local frame) or altitude (global - relative or absolute, depending on frame) (otherwise Param #7).

The first four parameters (shown above) can be used for any purpose - this depends on the particular command. The last three parameters (x, y, z) are used for positional information in MAV_CMD_NAV_* commands, but can be used for any purpose in other commands.

The remaining message fields are used for addressing, defining the mission type, specifying the reference frame used for x, y, z in MAV_CMD_NAV_* messages, etc.:

4.12.2 MISSION_ITEM_INT vs MISSION_ITEM

MISSION_ITEM and MISSION_ITEM_INT are used to exchange individual mission items between systems. MISSION_ITEM messages encode all mission item parameters into float parameters fields (single precision IEEE754) for transmission. MISSION_ITEM_INT is exactly the same except that param5 and param6 are Int32 fields.

Protocol implementations must allow both message types in supported operations (along with the corresponding MISSION_REQUEST and MISSION_REQUEST_INT message types).

MAVLink users should always prefer MISSION_ITEM_INT because it allows latitude/longitude to be encoded without the loss of precision that can come from using MISSION_ITEM.

Message/Enum Summary

The following messages and enums are used by the service.

Message Description

MISSION_REQUEST_LIST Initiate mission download from a system by requesting the list of mission items.

MISSION_COUNT Send the number of items in a mission. This is used to initiate mission upload or as a response to MISSION_REQUEST_LIST when downloading a mission.

MISSION_REQUEST_INT Request mission item data for a specific sequence number be sent by the recipient using a MISSION_ITEM_INT message. Used for mission upload and download.

MISSION_REQUEST Request mission item data for a specific sequence number be sent by the recipient using a MISSION_ITEM message. Used for mission upload and download.

MISSION_ITEM_INT Message encoding a mission item/command (defined in a MAV_CMD). The message encodes positional information in integer parameters for greater precision than MISSION_ITEM. Used for mission upload and download.

MISSION_ITEM Message encoding a mission item/command (defined in a MAV_CMD). The message encodes positional information in float parameters. Used for mission upload and download.

MISSION_ACK Acknowledgment message when a system completes a mission operation (e.g. sent by autopilot after it has uploaded all mission items). The message includes a MAV_MISSION_RESULT indicating either success or the type of failure.

MISSION_CURRENT Message containing the current mission item sequence number. This is emitted when the current mission item is set/changed.

MISSION_SET_CURRENT Set the current mission item by sequence number (continue to this item on the shortest path).

STATUSTEXT Sent to notify systems when a request to set the current mission item fails.

MISSION_CLEAR_ALL Message sent to clear/delete all mission items stored on a system.

MISSION_ITEM_REACHED Message emitted by system whenever it reaches a new waypoint. Used to monitor progress.

Enum Description

MAV_MISSION_TYPE Mission type for message (mission, geofence, rallypoints).

MAV_MISSION_RESULT Used to indicate the success or failure reason for an operation (e.g. to upload or download a mission). This is carried in a MISSION_ACK.

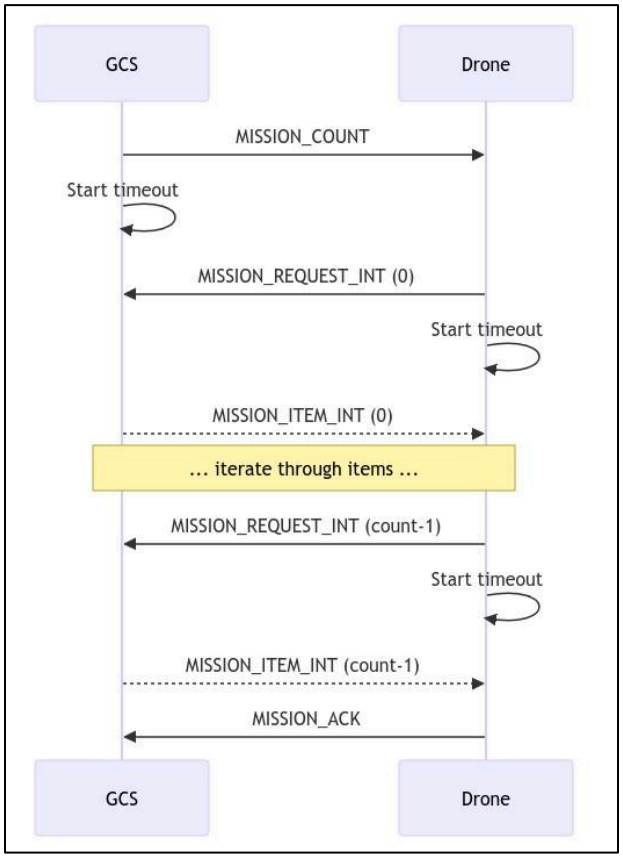
MAV_FRAME Co-ordinate frame for position/velocity/acceleration data in the message.

MAV_CMD Mission Items (and MAVLink commands). These can be sent in MISSION_ITEM or MISSION_ITEM_INT.

Operations This section defines all the protocol operations.

4.12.3 Upload a Mission to the Vehicle

The diagram below shows the communication sequence to upload a mission to a drone (assuming all operations succeed).



Mission update must be robust! A new mission should be fully uploaded and accepted before the old mission is replaced/removed.

4.12.4 Mission Upload Sequence

In more detail, the sequence of operations is:

GCS sends MISSION_COUNT including the number of mission items to be uploaded (count).

A timeout must be started for the GCS to wait on the response from Drone (MISSION_REQUEST_INT).

Drone receives message and responds with MISSION_REQUEST_INT requesting the first mission item (seq==0).

A timeout must be started for the Drone to wait on the MISSION_ITEM_INT response from GCS.

GCS receives MISSION_REQUEST_INT and responds with the requested mission item in a MISSION_ITEM_INT message.

Drone and GCS repeat the MISSION_REQUEST_INT/MISSION_ITEM_INT cycle, iterating seq until all items are uploaded (seq==count-1).

After receiving the last mission item the drone responds with MISSION_ACK with the type of MAV_MISSION_ACCEPTED indicating mission upload completion/success.

The drone should set the new mission to be the current mission, discarding the original data.

The drone considers the upload complete.

GCS receives MISSION_ACK containing MAV_MISSION_ACCEPTED to indicate the operation is complete.

Note:

A timeout is set for every message that requires a response (e.g. MISSION_REQUEST_INT). If the timeout expires without a response being received then the request must be resent.

Mission items must be received in order. If an item is received out-of-sequence the expected item should be re-requested by the vehicle (the out-of-sequence item is dropped).

An error can be signaled in response to any request using a MISSION_ACK message containing an error code. This must cancel the operation and restore the mission to its previous state. For example, the drone might respond to the MISSION_COUNT request with a MAV_MISSION_NO_SPACE if there isn't enough space to upload the mission.

The sequence above shows the mission items packaged in MISSION_ITEM_INT messages. Protocol implementations must also support MISSION_ITEM and MISSION_REQUEST in the same way.

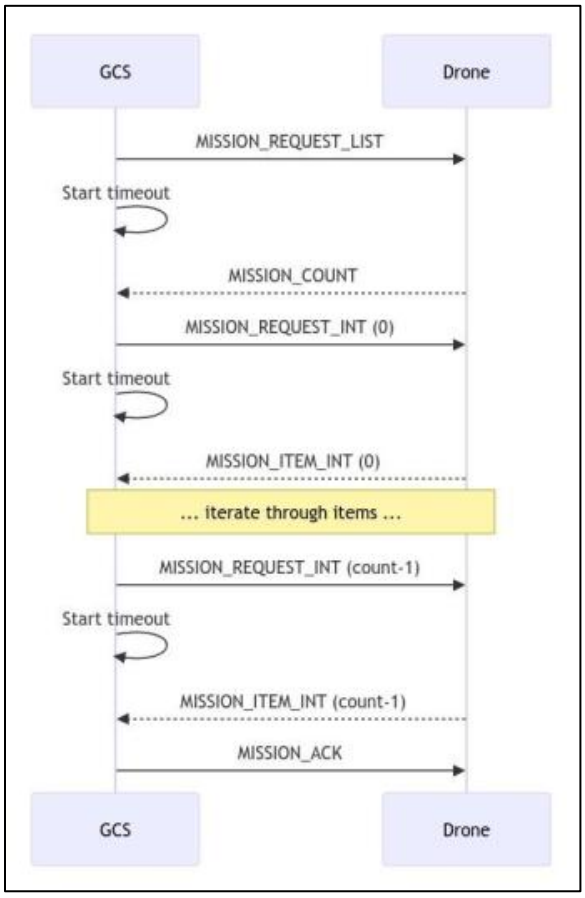
Uploading an empty mission (MISSION_COUNT is 0) has the same effect as clearing the mission.

Download a Mission from the Vehicle

The diagram below shows the communication sequence to download a mission from a drone (assuming all operations succeed).

4.12.5 Sequence: Download mission

The sequence is similar to that for uploading a mission. The main difference is that the client (e.g. GCS) sends MISSION_REQUEST_LIST, which triggers the autopilot to respond with the current count of items. This starts a cycle where the GCS requests mission items, and the drone supplies them.



Note:A timeout is set for every message that requires a response (e.g. MISSION_REQUEST_INT). If the timeout expires without a response being received then the request must be resent.

Mission items must be received in order. If an item is received out-of-sequence the expected item should be re-requested by the GCS (the out-of-sequence item is dropped).

An error can be signaled in response to any request using a MISSION_ACK message containing an error code. This must cancel the operation.

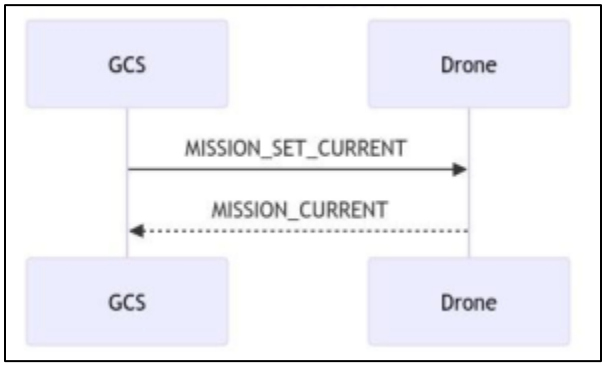
The sequence above shows the mission items packaged in MISSION_ITEM_INT messages.

Protocol implementations must also support MISSION_ITEM and MISSION_REQUEST in the same way. Set Current Mission Item

The diagram below shows the communication sequence to set the current mission item.

4.12.6 Set mission item

In more detail, the sequence of operations is:



GCS/App sends MISSION_SET_CURRENT, specifying the new sequence number (seq). Drone receives message and attempts to update the current mission sequence number. On success, the Drone must broadcast a MISSION_CURRENT message containing the current sequence number (seq).

On failure, the Drone must broadcast a STATUSTEXT with a MAV_SEVERITY and a string stating the problem. This may be displayed in the UI of receiving systems.

Notes:

There is no specific timeout on the MISSION_SET_CURRENT message.The acknowledgment of the message is via broadcast of mission/system status, which is not associated with the original message. This differs from error handling in other operations.

This approach is used because the success/failure is relevant to all mission-handling clients.

Monitor Mission Progress

GCS/developer API can monitor progress by handling the appropriate messages sent by the drone:

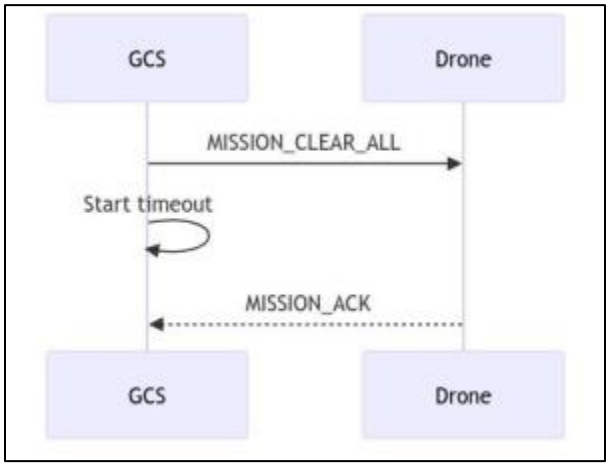
The vehicle must broadcast a MISSION_ITEM_REACHED message whenever a new mission item is reached. The message contains the seq number of the current mission item.

The vehicle must also broadcast a MISSION_CURRENT message if the current mission item is changed.

Clear Missions

The diagram below shows the communication sequence to clear the mission from a drone (assuming all operations succeed).

4.12.7 Clear Missions



In more detail, the sequence of operations is:

GCS/API sends MISSION_CLEAR_ALL

A timeout is started for the GCS to wait on MISSION_ACK from Drone.

Drone receives the message, and clears the mission from storage.

Drone responds with MISSION_ACK MAV_MISSION_ACCEPTEDMAV_MISSION_RESULT. with result type of GCS receives MISSION_ACK and clears its own stored information about the mission. The operation is now complete.

Note:

A timeout is set for every message that requires a response (e.g. MISSION_CLEAR_ALL). If the timeout expires without a response being received then the request must be resent.

An error can be signaled in response to any request (in this case, just MISSION_CLEAR_ALL) using a MISSION_ACK message containing an error code. This must cancel the operation. The GCS record of the mission (if any) should be retained.

Canceling Operations

The above mission operations may be canceled by responding to any request (e.g.MISSION_REQUEST_INT) with a MISSION_ACK message containing the MAV_MISSION_OPERATION_CANCELLED error.

Both systems should then return themselves to the idle state (if the system does not receive the cancellation message it will resend the request; the recipient will then be in the idle state and may respond with an appropriate error for that state).

4.13 GEO-FENCING

It is a feature that allows operators to define virtual boundaries within which the drone is permitted to operate. When enabled, geo-fencing ensures that the drone does not fly outside the designated area, helping to enhance safety and prevent the drone from entering restricted or dangerous zones.

4.13.1 Key Features of GEO-FENCING:

-

4.14 AUTONOMY ARCHITECTURE

4.14.1 Visual Inertial Odometry (VIO)

It is a key technology for providing precise real-time navigation and positioning. The drone would use a combination of visual data from cameras (to track features and estimate movement) and inertial data from sensors (accelerometers and gyroscopes in the IMU) to accurately determine its position and orientation, even in GPS-denied or challenging environments.

4.14.2 Path Planning

It involves calculating the most efficient route from the starting point to the destination while avoiding obstacles.
the drone can autonomously navigate through complex environments in 3D, adjusting its path in real time. It leverages data from sensors like **VIO** (Visual Inertial Odometry) for precise positioning and obstacle detection, ensuring smooth, safe, and efficient flight even in dynamic environments.

4.14.3 PX4

It is an open-source flight control software used in drones, including the Menthosa Suparna drone. It provides the essential control systems for flight, including stabilization, navigation, and autonomous flight capabilities. PX4 supports a wide range of sensors (like GPS, IMU, and cameras), and is highly customizable, allowing for integration with various sensors and payloads. It enables advanced flight modes such as autonomous missions, path planning, and real-time control, making it ideal for use in both research and commercial drone.

4.14.4 GPS-denied navigation

It allows to fly and navigate accurately without relying on GPS signals. This is achieved through the integration of sensors like Visual Inertial Odometry (VIO), IMUs (Inertial Measurement Units), and sometimes LiDAR or cameras.

4.14.5 BVLOS (Beyond Visual Line of Sight)

This allows the drone to operate beyond the pilot's direct visual range, relying on sensors, GPS, and communication systems for navigation. This is particularly useful for long-range missions, inspections, or surveys in remote areas where the drone needs to travel far from the operator.

4.14.6 Follow Me

This mode enables the drone to autonomously track and follow a moving target, such as a person or vehicle. The drone uses GPS or visual tracking to keep the target in sight, making it ideal for activities like filming, sports, or personal tracking in outdoor environments.

4.15 360 OBSTRACLE AVOIDANCE ARCHITECTURE

The **360-degree Obstacle Avoidance** is designed to ensure that the drone can detect, avoid, and navigate around obstacles in all directions during flight, enhancing its safety, autonomy, and ability to operate in complex environments. This architecture typically involves a combination of multiple sensors, algorithms, and systems to provide comprehensive environmental awareness and real-time decision-making. Below is a detailed breakdown of how such an architecture might work.

4.15.1 Depth estimation

It is a key component in autonomous navigation for drones . It refers to the process of determining the distance between the drone and objects in its environment.

4.15.2 Object detection

It is a critical task in autonomous drone operations for drones. It enables the drone to identify and classify objects within its environment, which is essential for tasks such as obstacle avoidance, target tracking, environment mapping, and autonomous navigation.

4.16 Mapping and Visual Odometry (VOA)

In autonomous drone navigation, Mapping and Visual Odometry (VOA) are critical components for reliable and precise operation. These technologies work together to enable the drone to understand its environment, localize itself, and navigate without the reliance on GPS. Here's an overview of both concepts,

4.17 Wireless Access Option

4.17.1 Connection Modes

Suparna has 3 Connection Modes by which the C2 (Command and Control) link can be established between the drone and Ground Control Station (GCS). Suparna can be flown in both outdoor (GPS available) as well as indoor (GPS denied) environments. But due to the nature of data being transmitted in both environments the bandwidth requirements change.

● For **Indoor Environment**, drone is constantly mapping the environment and using the Vision systems for localization. The bandwidth required is in the range of - 30 Mbps and some peaks of up to 50 Mbps.

● For **Outdoor Environment**, the drone has GPS for its localization and no mapping is being done. So bandwidth reduces to 2 Mbps with peaks up to 5 Mbps.

A. 5G Mode

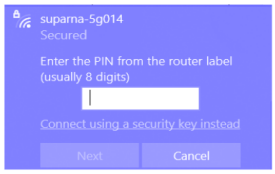
On board the drone there is a 5G module, which supports all the sub 6 Ghz 5G bands available in India. The module supports 5G nano sim which is inserted into the drone via the insertion slot present at the back of the drone.
Connecting to the drone -
1. Before powering on the drone, insert the 5G nano sim card into the drone.
2. Power ON the drone.
3. For public 5G use -
a. Log into 'idronam.com' now you can connect to your drone via selecting the drone alias at Dashboard.
4. For private 5G use -
a. Open the ''iDronam Enterprise' software. If you have previously added the drone you can simply select the connect button on the device dashboard.
b. If you are using the drone for the 1st time. Please add the drone to the database and then continue.
5. Upon successful connection you will be able to see the drone telemetry data and live feed.

Hurray! Your drone is now connected via a 5G network. Enjoy Flying.

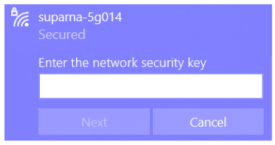
B. Hotspot Mode

The drone has a 2.4/5Ghz wifi module onboard for quick and easy connections. This can also be used to connect to the drone. By default, the drone is in Hotspot or AP (Access Point) mode and broadcasting in 2.4Ghz band.

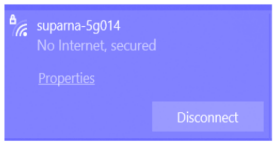
Connecting to the drone -
1. Power ON the drone.
2. Connect to the Hotspot. The SSID of the drone's hotspot is unique. It is the drone's serial no. - 'suparna-5gXXX'. Password for the hotspot is - 'Suparna5Gdrone'.
3. Open the 'iDronam Enterprise' software. Go to the dashboard.
4. If the drone is added, connect to the drone.



In **Windows 10/11** the Hotspot is shown as in image and if a password is entered here the connection will not be established. So, in order to connect, select the link below the text box called - **'Connect using a security key instead'.**



After selecting the link, this input box will open. Now, enter the password mentioned above here.



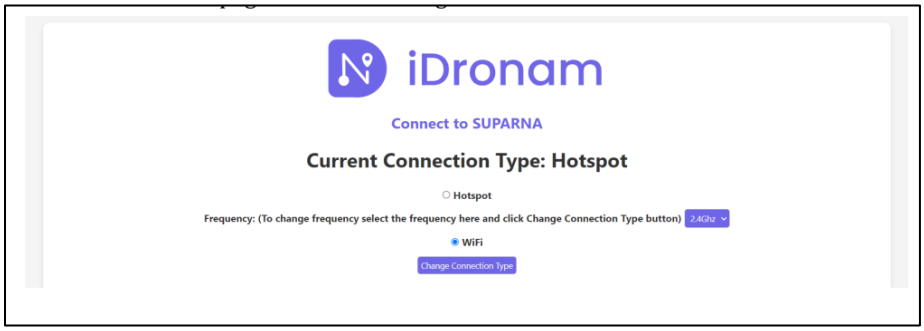
Windows shows loading even when connection is done. Just click somewhere else and then check wifi connections, if successful the connection will be established and it can be seen as shown in the image.

C. WiFi Mode

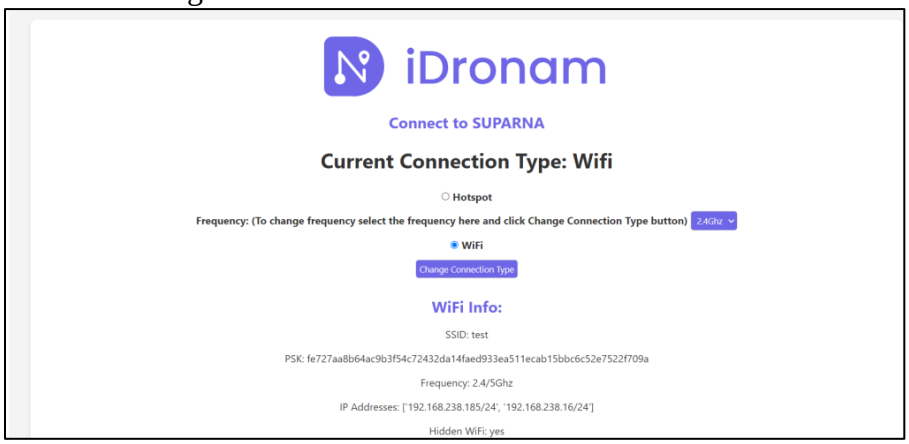
When in wifi mode, the drone can be connected to any 2.4/5Ghz wifi network. As the drone comes in Hotspot mode by default, we need to switch it to wifi mode, which can be done by the network mode switch webpage hosted inside the drone. The steps for connecting to the webpage are -
1. Connect to the hotspot of the drone.
2. Open any browser and enter the link of the webpage - 'suparna-5gXXX.local', where suparna-5gXXX is the ID of the drone and can be checked from the SSID of the hotspot.
If you are facing issues you can also navigate to the webpage by entering the drone's IP - '10.42.0.1'. This is the same for all the drones.
3. Upon successful connection a webpage will be opened as shown in the image below-

4. This will be the first time for a drone's wifi mode connection. Navigate to the bottom of the page where the ‘Add New WiFi’ section is present. Here, enter the wifi details - ‘SSID’ and ‘password’. Please enter the password carefully, you can view password text by clicking the Show button.

5. After entering the details and verifying the password. Click on the 'Connect' button. A warning will pop up; click ok. Now the page will refresh. This means that the wifi details are added into the drone.
6. Now to connect to the WiFi navigate to the top of the webpage, here select the ‘WiFi’ radio button and click on ‘Change connection type’. A warning message will come, click on ok and the page will start loading.



7. Now, the drone’s Hotspot will be disabled and the drone will connect to the entered WiFi.
8. In order to connect to the drone via the WiFi, connect the GCS system to the same WiFi as the drone.
9. Now you will need the IP address assigned to the drone. This can be obtained via your WiFi router where you will be able to see the drone’s ID connected to the WiFi.
10. If your router does not have this functionality or you are unable to retrieve the IP address. You can open the network mode switch web page by going to the link - ‘suparna-5gXXX.local’. Here you will be able to see the IP addresses assigned to the drone.



11. Now, add this IP in the ‘iDronam Enterprise’ via the ‘Add devices’ and you can connect to the drone.

D. Network Mode Switch

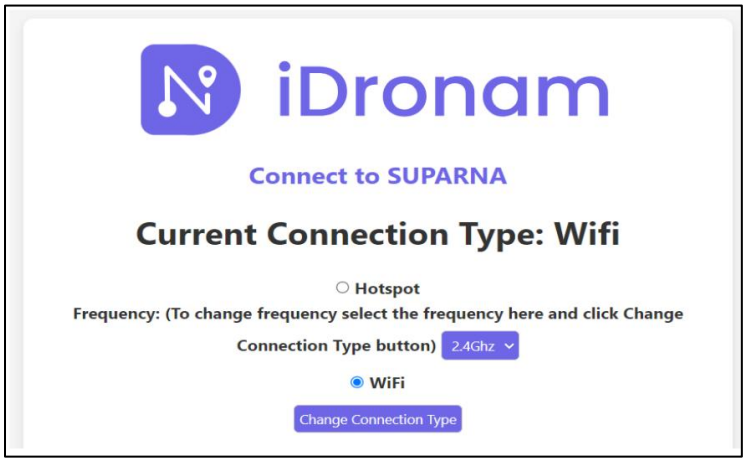
The drone has a single wifi module on board. Hence, at a time the drone can be in either hotspot mode or wifi mode. So, how to switch from one mode to another, this can be done by a webpage hosted in the drone itself.

E. Network mode switch webpage

This is a central webpage for Switching and Monitoring the Networks of the Drone.
Currently, Wifi and Hotspot modes can be configured from this page.
There are 3 sections to the webpage -

i. Current Connection Type :

It shows in what connection mode the drone currently is in. There are 2 radio buttons showing the connection modes, and the current mode is already selected. Along With these there is a frequency selection list. This is used when a drone is to be used in Hotspot mode. There are 2 options - 2.4 and 5Ghz.



ii. WiFi / Hotspot Info :

This section changes with respect to the drone’s network mode.

a. WiFi Info -

This displays the current SSID, Password(PSK), Frequency, IP Addresses and Hidden WiFi Status of the wifi to which the drone is connected.

b. Hotspot Info -

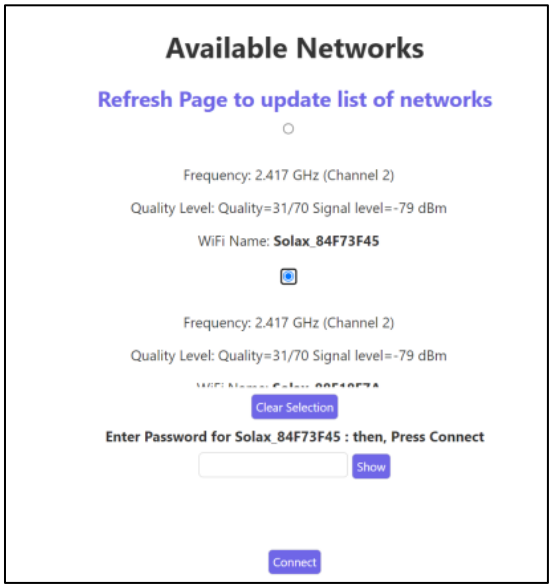
This displays the SSID, Password and Frequency of the drone's Hotspot.

c. Add New WiFi :

This section is used when you are switching to the WiFi mode for the first time. Also, it can be used when you want the drone to connect to hidden wifi.

d. Available Networks :

This section only shows in Wifi mode and is used to change the wifi network of the drone. Once you select the wifi network from the list, the password text will show up. Once entered click on connect to change drone WiFi.



4.18 Flight Controller

1. Overview

Suparna control stack runs on autopilot hardware to control drones, UAVs, and other unmanned vehicles. It offers robust capabilities for controlling a wide range of vehicles like multi-copters, fixed-wing, VTOLs, and ground vehicles. Here a quadcopter with autonomous capabilities is presented

2. System Components

The system is composed of several key components that work together to ensure smooth flight operations and management of the vehicle. These components include the Flight Stack, Middleware, Hardware Abstraction, and the Operating System.

3. Flight Stack

The Flight Stack includes the navigation, position estimation, and attitude controllers. It is responsible for ensuring the vehicle follows flight paths, maintains stability, and reaches its intended destination.

4. Middleware PX4's

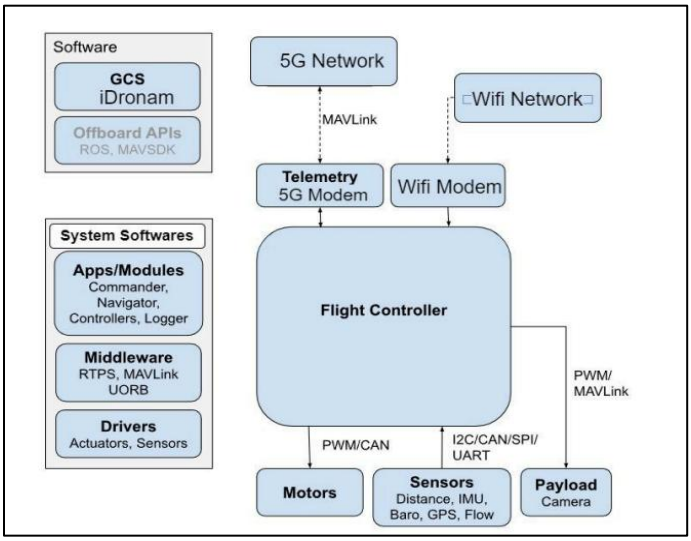
Middleware facilitates communication between different parts of the system, such as the flight control and sensors. It provides standard interfaces for vehicle components, making the system more modular and extensible.

5. Hardware Abstraction Layer (HAL)

The Hardware Abstraction Layer separates the operating system and hardware-specific implementations from the higher-level flight logic. This ensures that PX4 can run on various autopilot hardware with minimal changes to the software.

6. Operating System

The controller is designed to run on top of a real-time operating system, providing low-latency, predictable scheduling required for flight control applications.

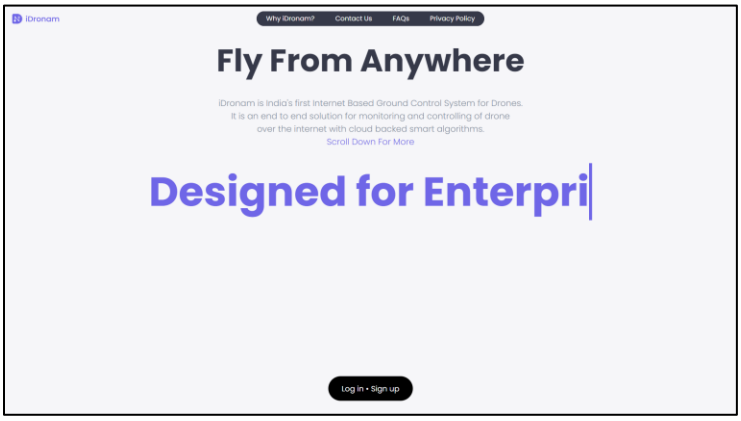


4.19 Software Installation

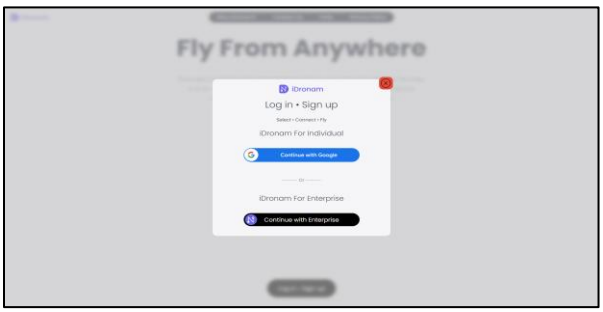
Organization Registration and Verification As drone operation is a crucial task and to know who is flying the Aircraft we have onboard the user with valid details. We are aggressively working to digitalise the process and improve system delivery.

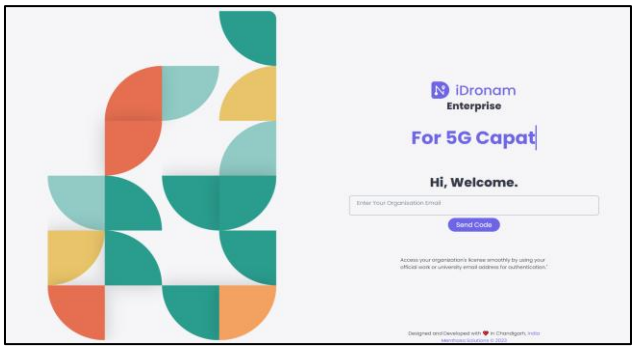
This section brief You about the Registration and Verification of Organisation :

- **Open iDronam**



Click on "Login/Signup"



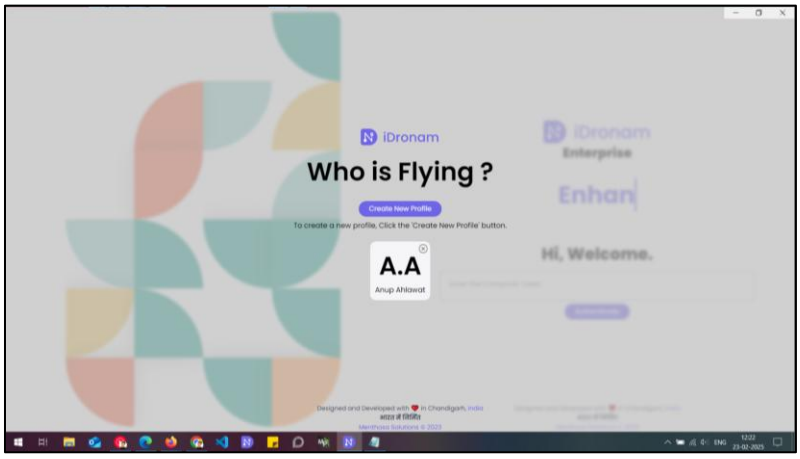


Click on “iDronam for Enterprise” and enter your Enterprise mail.

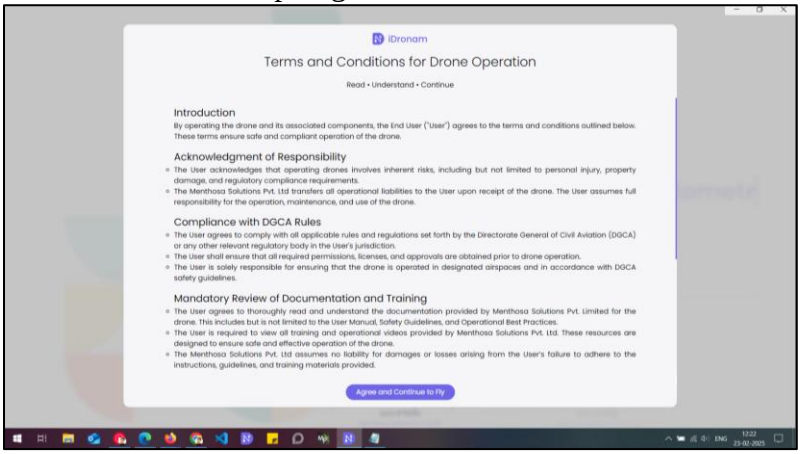
4.20.1 Software Setup

A. Indoor Mode

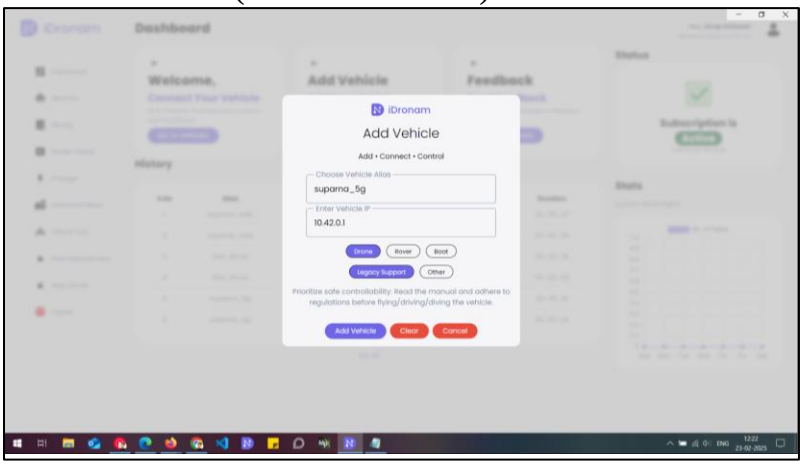
Select Profile



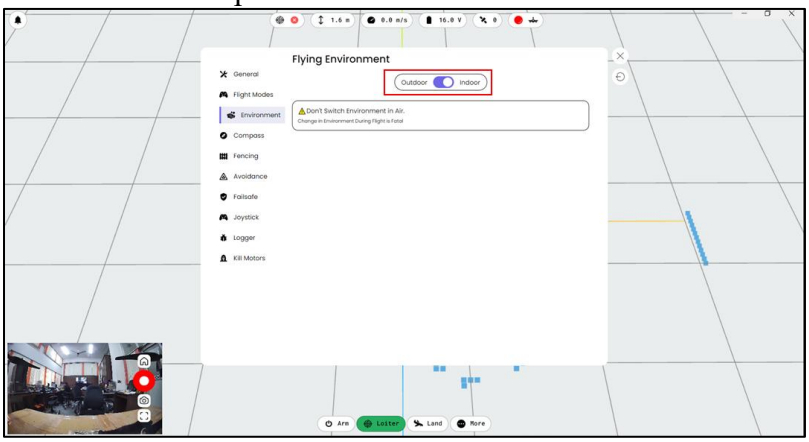
Accept Agreement



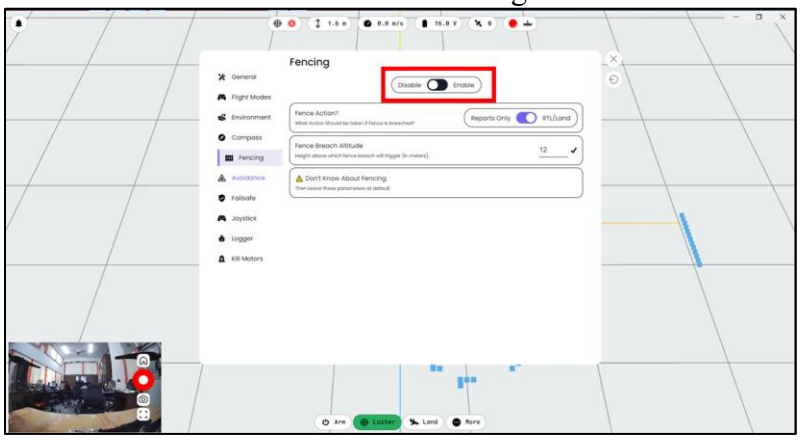
Add Drone (Over WiFi Or 5G) and connect to it.



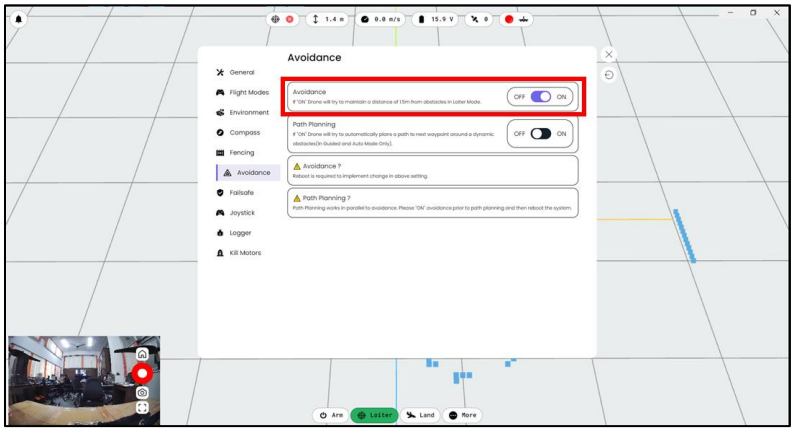
Click More Options and Set Environment to “Indoor”.



Disable “Geo Fencing”

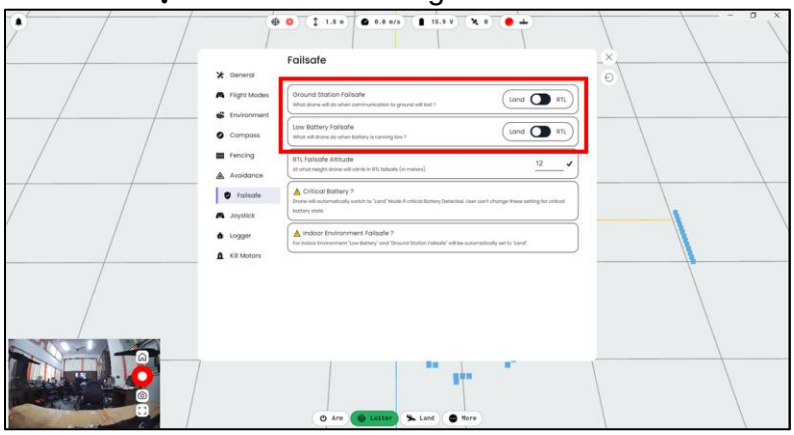


Enable “Avoidance”

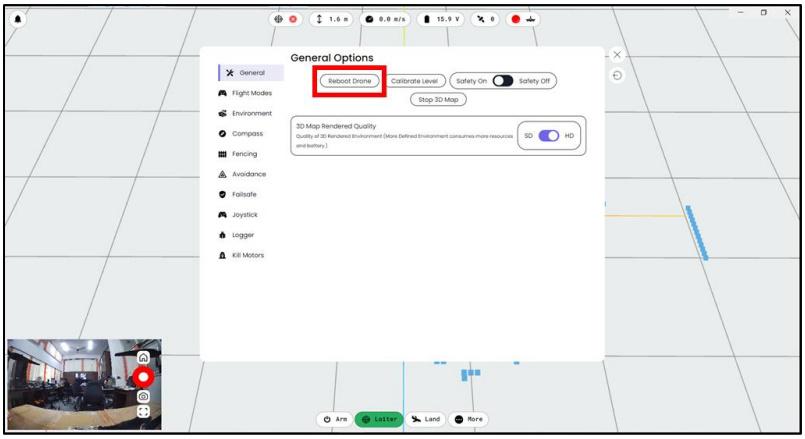


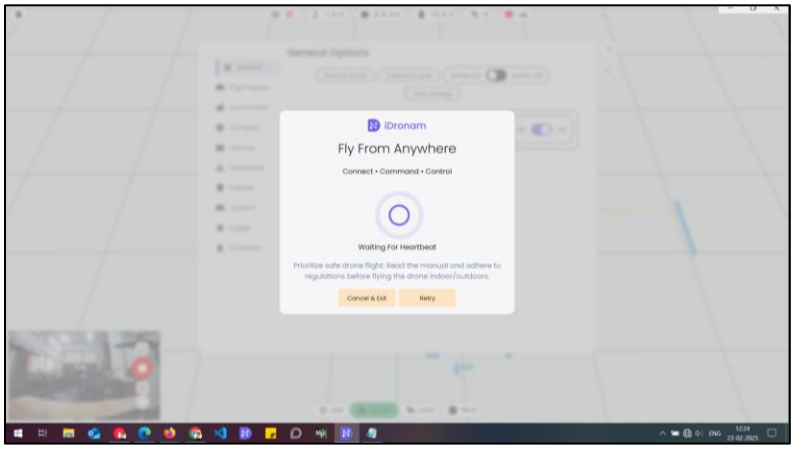
Configure Failsafe

! For Indoor Configure it to “Land”

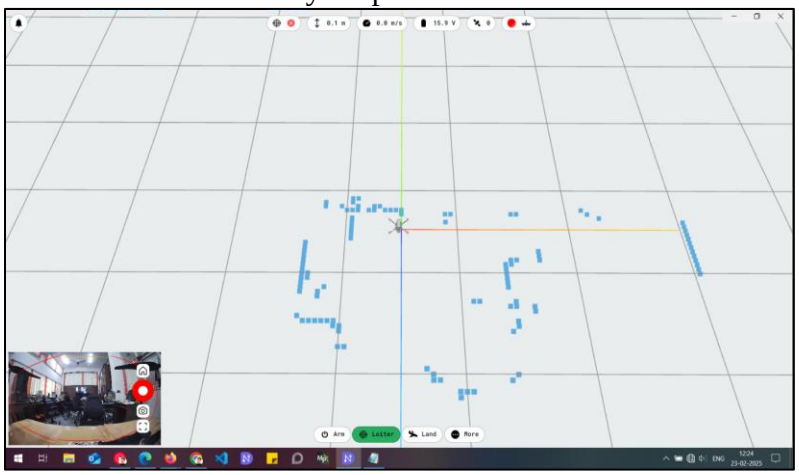


Reboot The Drone and Retry





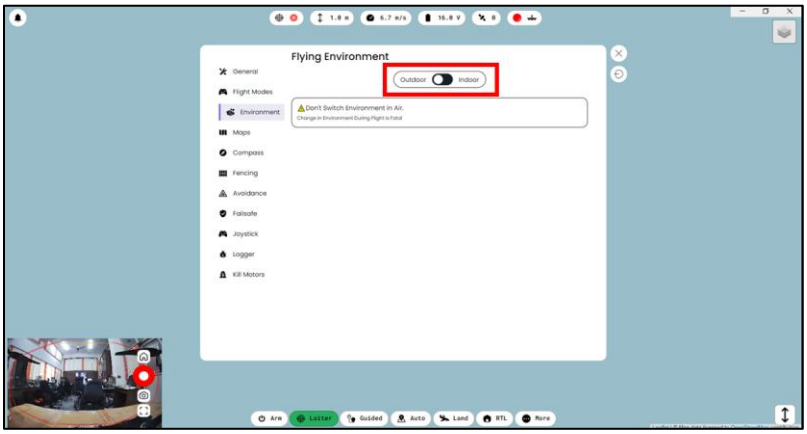
Verify Map and Obstacle



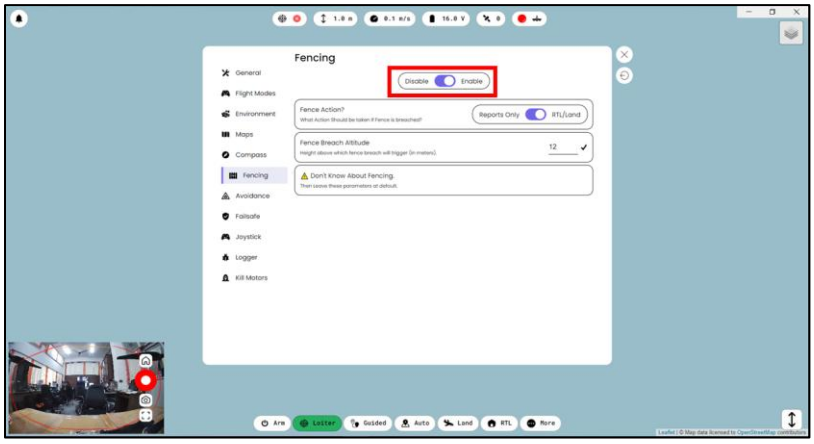
B. Outdoor Mode-

Outdoor flight requires some more parameters to set up before flight.
Follow the steps below before taking the flight to ensure safe outdoor flight.

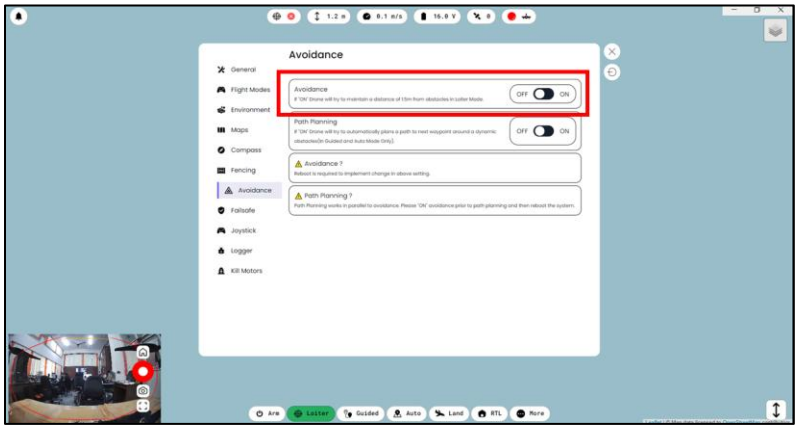
Switch to Outdoor Mode



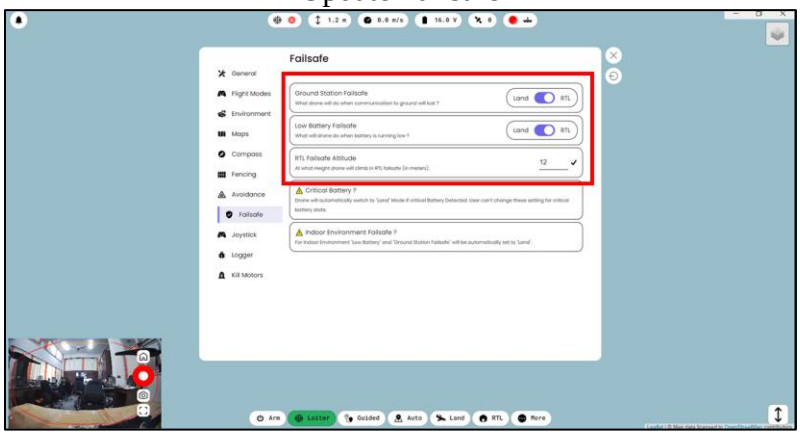
Turn ON Geo Fencing



Turn OFF Obstacle Avoidance

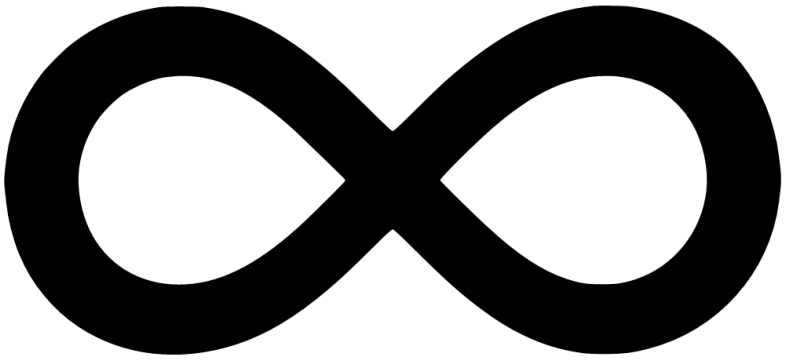


Update Failsafe

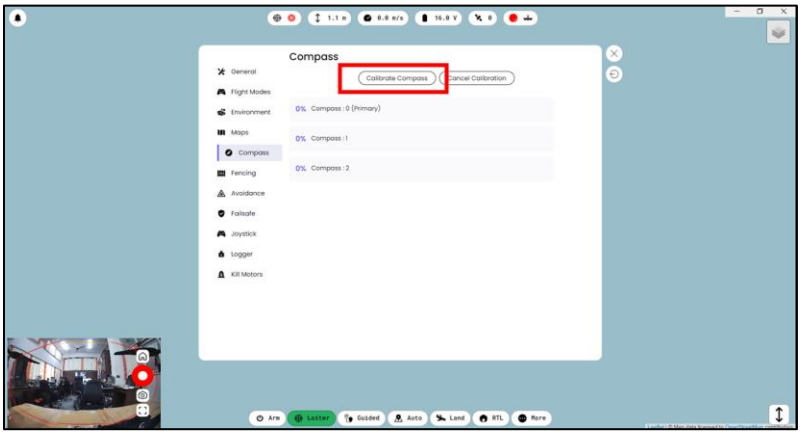


RTL (Return to Launch) Mode:
RTL Altitude is the height the drone ascends to before returning to the launch site. It must be higher than any obstacles in the line of sight along the RTL path and lower than the Fence Breach Altitude.

Calibrate Compass



After pressing the “Calibrate Button”. Pick up the aircraft and move in the infinity shape and see calibration progress.



Compass calibration must be performed before flight or when changing location, as it is affected by nearby magnetic interference. During calibration, the progress percentage increases. Upon successful completion, the drone reboots. If calibration fails, the percentage resets to 0, requiring users to retry.

4.21 AI/ML Use Case-

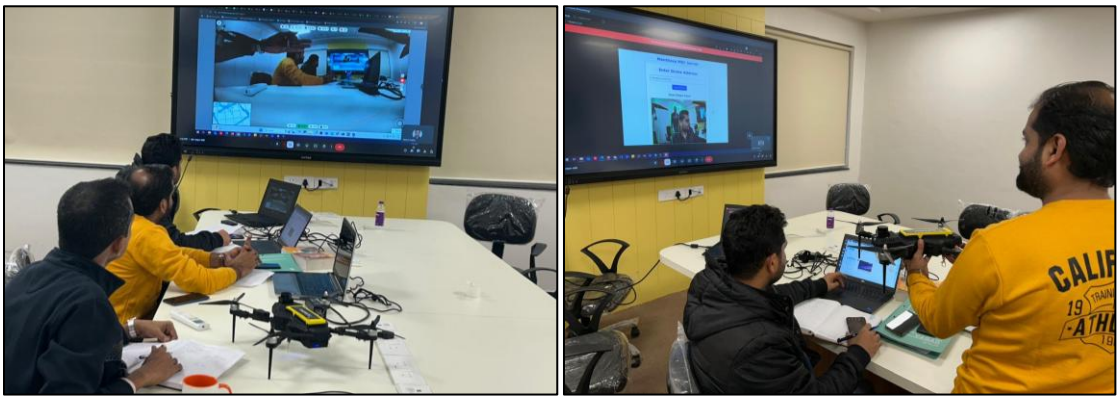


Fig- showing API of Drone Integrated with MEC VM

4.22 Sim Insertion And 5g Registration-

4.22.1 SIM Insert

A. SIM Slot:

The drone would have a designated SIM card slot on its onboard communication system, typically integrated into its communication module.

- **Insert SIM**: The SIM card is inserted into the slot, similar to inserting a SIM card into a phone. Ensure that the SIM card is inserted correctly.
- **Power On the Drone**: Once the SIM card is securely inserted, power on the drone. The onboard system will attempt to connect to the mobile network.

B. SIM REGISTRATION

Registration will be carried out by the RAN (Radio Access Network) of the system, which will handle the process automatically to ensure seamless integration of devices or users into the network.

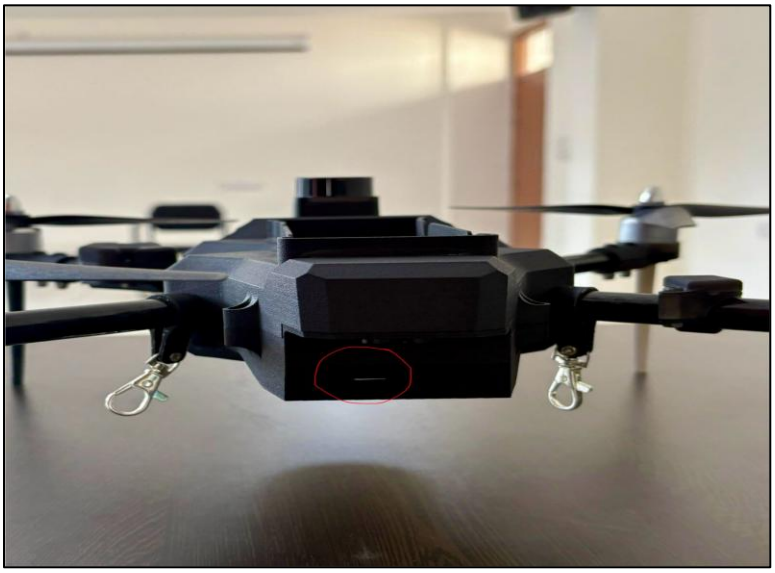


Fig- showing the slot space in 5G Drone

4.23 Installing The Drone Camera Applicatiom At Mec:

4.23.1 Steps for installation -

1. 1. Download and unzip the files
2. 2. Install docker - https://docs.docker.com/engine/install/ubuntu/
3. 3. import the image file - sudo docker import dronemecserveraiml_v1.1.tar.gz dronemecserveraiml_v1.1:latest
4. 4. run the docker image via compose - sudo docker compose up -d
5. 5. view the webpage on - http://(mecip):5000
6. 6. for viewing drone stream enter link - rtsp://(drone ip):10000/drone_cam.

4.24 TROUBLESHOOTING

The drone is equipped with an automated troubleshooting system that continuously monitors its performance during operation. In the event of any malfunctions or errors, the system immediately detects the issue and alerts the user via the iDronam app. The app provides real-time notifications and detailed error messages, allowing the user to identify the nature of the problem. Until the issue is diagnosed and resolved, the drone will not be ready for flight. This built-in self-diagnosis ensures that the drone remains in optimal condition, minimizing the risk of failure during operation and ensuring safety.

4.25 Take off and General Flight precautions-

After successful pre-arm checks, the drone is ready for take-off. There are 2 methods of arming the drone-

- Using GCS software : The arm button in the control panel can be clicked for a 1 tap takeoff. Here the drone will take-off to an altitude of 1 meter and will switch to Guided Mode. The pilot can switch to loiter mode between the takeoff to control the drone.
- Manual : Pilot can manually take off the drone using the joystick-
- Switch to Loiter mode.
- Bring the left stick (throttle) of the controller to the bottom right position and hold it there.
- Drone will give an aural signal and all the propellers will start moving.
- Move the stick to extreme bottom position and slowly raise it to middle position and slightly nudge the stick to upward position.
- Drone will take off and hover in its position.
- For increasing altitude nudge the stick upwards. The drone will maintain its position vertically wherever the pilot leaves the stick.
- To decrease the altitude, nudge the stick downwards.
- The drone will hover in its position if no command is given.

4.25.1 Before taking off there a few things that pilot must observe:

1. When in an indoor environment, observe the 3D map data coming onto the GCS software central screen. If the map is skewed or is not in a regular shape of the drone's surroundings. Then, it means the drone has lost its local position and will show unintentional behavior. The drone must be restarted by removing and reinserting the battery(power cycle).
2. Another parameter is the Ground velocity of the drone, shown in the central dashboard of GCS software. The GCS will not arm the drone if it is greater than 0.3 m/s. But if somehow it is skipped. The pilot must always check this parameter if it shows any value above the threshold of 0.3 m/s.
3. Stop the takeoff sequence and use the Reboot drone button to reboot the flight controller of the drone. The reasons for ground velocity misbehaving are -

- Low Light conditions, the vision system does not have enough light to function optimally. Move to a better lit area.
- Optical Flow sensor blocked. There is a downward facing vision sensor under the belly of the drone. If it is blocked/hindered it might report wrong values.

1. Dynamic Obstacles around the drone during takeoff. The drone's obstacle avoidance starts once an altitude of 50 cm is detected; if any object breaches the 1.5m cut-off during takeoff the drone might not takeoff in a smooth manner. So to avoid this pilot must make sure no dynamic obstacles move around the drone before takeoff.
2. When in an outdoor environment, the pilot must observe for any GPS/Compass glitch that may happen during takeoff. If the position on map (central screen of GCS) shifts randomly that may indicate GPS/Compass glitch, immediately abort takeoff sequence. Reboot the flight controller via the Reboot Drone button.

4.25.2 Pre-Arm Checks-

After the preflight checks are performed and all the conditions are satisfied the pilot must move forward to pre-arm checks.

These are a list of flight critical conditions which are necessary to arm the drone. Failing any one of the conditions will result in a Pre-arm check failure which will be displayed by the GCS.

The checks are as follows-

GPS (Outdoor) - If the GPS is not able to get a good lock it will result in the GPSfailure, please move the drone to an open location.

Compass - The compass is affected by high Electromagnetic fields, if the drone is in a high EMF region it will cause compass failure. Move the drone to a low EMF region.

Proximity - The drone's obstacle avoidance system checks for any obstacle which is in 60cm of proximity. This check will fail if any obstacle is detected within the 60cm radius of the drone. Please remove the obstacles.

GCS - The Ground control station has a good C2 link with drones via the GCS software. If it fails, the pilot will lose all communication with the drone.Check the drone and GCS networks.

Battery - The voltage level is further checked by the drone. If the battery is less than 11.5 Volts this check will fail. Please charge the battery.

Visual Odometry (Indoor) - The drone uses a vision system to navigate in indoor mode or GPS-denied areas. If the vision system is unable to function properly this check will fail. Please refer to the full manual for the complete vision system operation range.

Safety Switch - If all of the above checks are passed, the final check is of the Safety switch. It is a safety mechanism to avoid unintentional arming of drones. For passing this check the pilot needs to press the safety off switch in the GCS software. After which an aural tone is heard and a Ready to Arm message will be displayed on GCS.

4.26 PRE FLIGHT CHECKS

4.26.1 Battery Checks

Drone is powered by a 4 cell (4S) 4500mah Li-ion battery.

It is recommended that the battery is fully charged up to 16.80 Volts, before each flight for optimal performance and charge only using the charger provided in the box.

If battery is not fully charged then,

❗ If the voltage is below 11.5 Volts, the drone will not arm because of Battery Failsafe.

🔘 If voltage is above maximum rating of 16.8 Volts, do not proceed any further, remove the battery and contact Menthosa Solutions as the battery may damaged. In any other case the drone will be able to fly.

4.26.2 Structure Checks

1. Drone has several moving parts which are held together by a rigid and lightweight carbon fiber chassis so before flight it is mandatory to see if any moving part is loose or not.
2. Motor mounts - The BLDC motors placed on these mounts are fastened using 4 Nuts. There are 4 of these on each drone.
3. It is to be ensured that the motors are not loose and the nuts are fastened.
4. The mounts do not have any cracks on them which may cause structural integrity problems.

4.26.3 Landing Gears -

Drone has 4 landing gears which give it a stable place to land, ground clearance to the payload and keeps it horizontally stable.

It is to be checked if there are cracks, chipping or any other kind of damage.

4.26.4 Propellers - Drone use the propellers to fly

1. Are properly fastened on the motors.
2. No chipping on the surface of the props.
3. Direction of the propellers is correct.

Payload - The drone has a 1 axis gimbal camera as its primary payload and optionally a 500g secondary payload can be mounted under the drone. Make sure all the payloads are mounted properly.

Drone Cover - The drone has a lightweight cover on its chassis which is fastened using 6 nuts. Make sure the cover is not damaged.

4.27 Flight Area Checks

The drone is equipped with a 360 degree obstacle avoidance and has a tolerance of 2m. At 1.5m distance from the obstacle drone will try to move away from the obstacle. Drone has GPS for outdoor operations, it has an accuracy of 2.5m.

There are 2 scenarios for this check -

1. Indoor : Drone requires at least 4m x 4m clearance for optimal indoor operation.
2. Outdoor : Drone requires open area where there are no buildings close by of heights ~25m and above as this will hinder GPS accuracy of the drone.

4.28 GCS Software, C2 Link and Controller Check-

The Ground Control Station (GCS) Software is the application which is used to command and control the drone. Before each flight, it should be updated to the latest version.

- C2 link is the command and control link between the GCS and the drone. Drone has 3 modes for communication - 5G, WiFi and Hotspot.
- **5G Mode** - Drone is using an on board 5G dongle to connect to the private network.
- **WiFi Mode** - Drone will be connected to the wifi, using the web interface .
- **Hotspot Mode** - Drone will be creating its own network and Pilot can connect to it.
- Make sure the GCS and drone are on the same network for C2 link to get established.
- A joystick controller is provided which can be used to fly the drone manually.
- It is to be connected before each flight to the GCS.

5. META QUEST XR/VR

5.1 Introduction

Oculus Quest 2 is most advanced all-in-one VR system

Developed by Meta Platform (facebook.inc)

Released on October 13, 2020

The standard Oculus Quest system consists of a VR headset (head-mounted display) and 2 controllers to be held in hands:

5.2 What Include In The Box

5.3 Key Features-

5.3.1 Standalone VR System:

- **No PC Required**: Unlike many VR headsets, the Meta Quest 2 is completely standalone, meaning it doesn't require a PC or external sensors to operate.
- **Integrated Processor**: Powered by a Qualcomm Snapdragon XR2 processor, providing strong performance for VR applications.

5.3.2 Display and Visuals:

- **Resolution**: The Quest 2 has a 1832 x 1920 resolution per eye, providing a sharp and immersive visual experience.
- **Refresh Rate**: The Meta Quest 2 supports up to 120Hz , offering smoother experiences during fast-moving VR applications.

5.3.3 Tracking:

- **Inside-Out Tracking**: The Quest 2 uses built-in cameras to track your movement, meaning you don't need external tracking sensors. This makes it easy to set up and use in various environments.
- **Hand Tracking**: The device supports hand tracking, allowing you to interact with the virtual world without controllers, though it works best in certain applications.

5.3.4 Controllers:

- The Meta Quest 2 comes with two wireless controllers equipped with tracking sensors, enabling natural interaction with VR environments.

5.3.5 Software and Content:

- The Quest 2 supports a large variety of VR content, including games, productivity tools, educational apps, and VR training simulations. The content is available via the **Meta Quest Store**.
- It also supports Oculus Link, which allows you to connect the Quest 2 to a PC to access PC VR content through SteamVR and Oculus PC software.

5.3.6 Audio:

- Built-in speakers provide spatial audio, The sound is emitted from the side of the headset, delivering audio without requiring additional accessories.

5.3.7 Comfort and Design:

- The Meta Quest 2 is lighter and more compact than its predecessor, making it more comfortable for extended sessions.
- It comes with adjustable straps and a customizable fit for various head sizes.

5.3.8 Storage Options:

- The Meta Quest 2 offers 128GB Storage.

5.3.9 Battery Life:

- The battery life typically lasts around 2-3 hours, depending on the type of activity. Games or applications with more demanding graphics can consume battery faster.

5.3.10 Social Features:

- You can connect with friends, share content, and interact in virtual spaces via Meta's social platforms.
- The **Horizon Worlds** platform is a popular VR social experience available on the Quest 2, where users can create, interact, and play in virtual worlds.

5.4 WHAT IS META QUEST 2?

Meta Quest 2 is an excellent tool for various training applications because of its portability, ease of use, and immersive experience. Here are some potential uses:

- **Employee Training**: machinery operation, safety training, emergency protocols
- **Medical Training**: practice surgery or diagnosis without real-world consequences
- **Education**:enabling students to explore history, science, and art in new and engaging ways
- **Soft Skills Training**:practice soft skills like public speaking, customer service, or negotiation through role-playing scenarios
- **Virtual Classrooms**: you can use tools like Horizon Workrooms for remote learning and collaboration.

5.3.1 Employee Training:

Meta Quest 2 can simulate a realistic working environment where employees can learn to operate complex machinery without the risk of causing damage to equipment or injuring themselves.

This Training can include:

Simulated Environments: Employees can interact with virtual machines, learning the controls, sequences, and operations.

Hands-on Practice: VR allows for tactile feedback, allowing workers to practice in a fully immersive setting that mirrors the real-world experience.

Error Correction: Instant feedback can be provided on mistakes or improper handling, helping employees correct their actions before working with actual equipment.

Repetitive Practice: Workers can repeatedly practice scenarios in a controlled, virtual environment until they master the skills, without using up valuable machine time.

5.3.2 Medical Training:

XR/VR in medical training offers immersive, hands-on experiences for students and professionals to practice critical skills safely and effectively:

Surgical Training:

Simulate various surgeries, from basic to complex, in a realistic virtual environment and gain real-time feedback on technique and accuracy, allowing for repeated practice and improvement.

Diagnosis & Clinical Skills:

Engage in virtual patient interactions, practicing medical history taking, physical exams, and diagnosis of different conditions.

Anatomy Education:

Visualize interactive models of human anatomy, offering deeper understanding of structures and systems. Perform virtual dissections to study organs and tissues without physical cadavers.

Procedure Training:

Practice common medical procedures and handle virtual complications in a risk-free setting.

5.3.3 Education:

XR/VR creates virtual spaces where students can learn by actively engaging with content. Rather than passively reading or listening, they can experience history, science, art, and more firsthand.

Exploring Complex Concepts:

- **Science:** Students can explore complex concepts like the human body, space, or chemical reactions in 3D, making abstract ideas easier to grasp.
- **History:** Travel through time and witness historical events or explore ancient civilizations, providing a deeper understanding of past cultures and significant moments.
- **Art:** Walk through virtual galleries, observe sculptures from all angles, and even create art in a 3D environment, offering a hands-on approach to learning about artistic techniques.

Interactive Learning:

XR/VR encourages active participation. Students don't just read about a topic—they explore it, experiment with it, and even make decisions in simulated environments that help reinforce learning.

Personalized Learning:

Virtual experiences can be tailored to individual learning paces and preferences, allowing students to revisit complex material, practice as much as needed, and engage with content in ways that best suit their needs.

5.3.4 Soft Skills Training:

Soft skills training through XR/VR offers immersive experiences to enhance key interpersonal and professional skills:

Communication Skills: Practice public speaking, active listening, and cross-cultural communication in virtual environments.

Leadership & Management: Simulate leadership roles, team management, and conflict resolution scenarios.

Emotional Intelligence (EQ): Develop empathy, self-awareness, and emotional regulation through realistic simulations.

Teamwork & Collaboration: Strengthen collaboration, problem-solving, and decision-making in virtual team settings.

Negotiation & Persuasion: Role-play negotiations and practice persuasion tactics in interactive scenarios

5.3.5 Virtual Classrooms:

Virtual classrooms using XR/VR provide interactive learning experiences where students and teachers interact in a 3D virtual space.

Key benefits include:

Immersive Learning: Students engage with lessons and simulations, making learning dynamic.

Global Access: Students can attend classes from anywhere, breaking geographical barriers.

Interactive Features: Virtual tools like whiteboards and 3D models enhance lessons.

Real-time Collaboration: Students collaborate on projects and participate in discussions through avatars.

Personalized Learning: Adaptive tools offer customized learning experiences for each student.

5.4 AR (Augmented Reality), VR (Virtual Reality), and MR (Mixed Reality)

5.4.1 Augmented Reality (AR)

AR technology overlays digital content (such as images, videos, or 3D models) on the real world, typically viewed through a screen, like a smartphone, tablet, or AR glasses. Unlike VR, AR does not replace the physical world; instead, it enhances it.

Key Features:

- **Overlay Digital Content**: AR adds virtual elements (graphics, sounds, etc.) to the real world.
- **Real-Time Interaction**: It interacts with the real world in real time, responding to the user's environment and movements.

Common Uses:

- **Mobile Apps**: Pokémon GO, IKEA Place (for furniture placement).
- **Retail**: Try-on features for clothes or makeup in stores.
- **Industrial Applications**: Repair manuals or assembly instructions overlaid on machinery.
- **Navigation**: Directions overlaid on a real-time map.

Devices: Smartphones, tablets, AR glasses (e.g., Microsoft HoloLens, Magic Leap), smart lenses.

5.4.2 Virtual Reality (VR)

VR is a fully immersive technology that replaces the real world with a completely virtual one. Users typically wear a headset that blocks out the real world and displays a digital environment, allowing them to interact with the virtual world.

Key Features:

- **Complete Immersion**: VR users are fully immersed in a virtual environment, often with 360-degree visuals and spatial sound.
- **User Interaction**: Users can interact with virtual objects using controllers, gloves, or body movements.

Common Uses:

- **Gaming**: Fully immersive games (e.g., Beat Saber, Half-Life: Alyx).
- **Training & Simulation**: For aviation, medicine, military, or other industries requiring hands-on training in a controlled, virtual space.
- **Virtual Tourism**: Explore virtual representations of places like museums, historic sites, or natural wonders.
- **Entertainment & Films**: VR movies or experiences where users feel like they're part of the story.

Devices: VR headsets (e.g., Oculus Rift, HTC Vive, PlayStation VR), haptic gloves, motion sensors.

5.4.3 Mixed Reality (MR)

MR combines elements of both AR and VR. It blends the virtual and real worlds in such a way that physical and digital objects coexist and interact in real time. It's often more immersive than AR but doesn't fully replace reality like VR.

Key Features:

- **Interaction Between Real and Virtual Worlds**: MR allows real-world and virtual elements to interact. For example, a digital object might be placed on a physical table and react as if it were really there.
- **Hybrid Environment**: MR creates a more integrated environment than AR, where users can interact with both real and digital objects.

Common Uses:

- **Industrial Applications**: In design, users can interact with CAD models and adjust them in real-time, while also working with physical parts.
- **Training**: MR can be used for realistic training scenarios where users engage with both physical tools and virtual training materials.
- **Entertainment**: MR can be used for immersive storytelling, where virtual characters can interact with real-world surroundings.
- **Education**: Learning experiences where students can engage with both digital and real-world elements (like historical reenactments in a classroom).

Devices: MR headsets (e.g., Microsoft HoloLens, Magic Leap), smartphones/tablets with MR apps.

5.5 XR Foundation Features for Design and Development

The **XR (Extended Reality) Foundation** plays a crucial role in creating and advancing immersive experiences, which combine **Virtual Reality (VR)**, **Augmented Reality (AR)**, and **Mixed Reality (MR)** into a unified framework. The XR Foundation supports a variety of features and technologies that are integral to designing and developing XR applications. These features are intended to ensure **compatibility, performance, interoperability**, and **scalability** across a wide range of devices and use cases.

To set up a development environment for the **XR/VR,** you'll need to install and configure several software tools to get started with VR development. Below is a step-by-step guide to help you get your Meta Quest 2 development environment up and running.

5.5.1 Steps to Install Required Hardware and Software

A. Hardware Requirements

- **Meta Quest 2** headset.
- **USB-C Cable** (to connect your Meta Quest 2 to your PC).
- A computer with **Windows 10/11** (recommended) or macOS for development.
- **Controllers**: Meta Quest 2 controllers for interaction with virtual environments.

B. Software Requirements

- **Unity3D** or **Unreal Engine** for creating your VR applications.
- **Oculus App** on your PC (for managing the Meta Quest 2).
- **Oculus Integration for Unity** (if using Unity).
- **Android Studio** (for building and deploying the app to Meta Quest 2).

5.6 Install and Build application usage

There are numerous applications available in the Meta Quest 2 app store, catering to a wide variety of interests and skills. To get started, the first app you should explore is called **First Steps**.

This app is specifically designed for new users and offers a guided experience to help you become familiar with the VR environment. Through interactive animations and clear instructions, **First Steps** teaches you how to properly control the virtual reality interface and operate the controllers effectively. This will give you the foundational knowledge needed to navigate the virtual world safely and confidently.

Once you're comfortable with the basic controls, you'll discover a wide range of applications in the Meta Quest 2 store that focus on skill development across different areas. These include fitness apps, language learning programs, art and design tools, meditation guides, and many others. Each app provides an immersive experience that helps you develop new abilities, improve cognitive skills, or even learn a new language, all within a virtual environment.

1. **Language Learning**: Mondly VR, Engage (language courses).
2. **Cognitive Skills**: Peak, Oculus Quest Mind Lab.
3. **Public Speaking**: VirtualSpeech, Speech Center VR.
4. **Fitness**: FitXR, OhShape, BoxVR.
5. **Music**: Virtuoso (piano), Incredibox (beats).
6. **Art & Design**: Tilt Brush, Kingspray Graffiti, SculptrVR.
7. **Business/Productivity**: Spatial, Immersed.
8. **Coding**: VIRTUAL CODE, Cospaces Edu.
9. **Design & Architecture**: ShapeLab VR, SketchUp Viewer.
10. **Meditation**: Tripp, Guided Meditation VR.
11. **Physics & Engineering**: Physics Playground, The Lab.
12. **Cooking**: **Kitchen VR**, **Cook-Out:** A Sandwich Tale.
13. **Cultural Learning**: Wander, National Geographic VR

5.7 TROUBLESHOOTING

5.7.1 VR Headset Not Turning On

- **Check Battery**: Ensure the headset is charged. Plug it into the charger and let it charge for at least 30 minutes.
- **Hard Reset**: Press and hold the power button for about 10 seconds to force a restart.
- **Try Different Charger**: If charging doesn't work, try a different USB-C charger or cable.

5.7.2 No Display / Black Screen

- **Adjust the Headset Fit**: Make sure the lenses are properly aligned with your eyes. Adjust the head straps for a comfortable fit.
- **Check the Power**: If the headset is on but the display remains black, try restarting it by holding down the power button for 10 seconds.
- **Reboot**: Try to reboot the device by pressing and holding the power button for 10 seconds.

5.7.3 Controllers Not Working

- **Battery Check**: Ensure the controllers have working batteries (replace them if necessary).
- **Re-pair the Controllers**: Go to the **Meta Quest 2 settings** > **Devices** > **Controllers** > **Pair New Controller**.
- **Restart the Headset**: Turn off the headset and restart it, then try pairing the controllers again.

5.7.4 Tracking Issues

- **Clear the Play Area**: Ensure your play area is well-lit, and free from obstructions. The cameras on the headset need a clear view of the environment for proper tracking.
- **Reset the Guardian System**: Go to **Settings** > **Guardian** and select **Reset Guardian** to redefine your play area.
- **Clean the Sensors**: Check if the sensors or cameras on the headset are clean. Use a soft, lint-free cloth to gently clean them.

5.7.5 Wi-Fi Connectivity Issues

- **Check Your Network**: Ensure that your Wi-Fi network is working properly and that the headset is within range of the router.
- **Forget and Reconnect**: Go to **Settings** > **Wi-Fi**, forget the network, and reconnect by entering your password again.
- **Restart the Router**: If the Wi-Fi connection is unstable, restarting the router can help.

5.7.6 App Not Launching or Freezing

- **Restart the Headset**: Hold down the power button for 10 seconds and then turn the headset back on.
- **Check for Updates**: Go to **Settings** > **About** > **Software Updates** and ensure your software is up to date.
- **Reinstall the App**: If an app is constantly freezing, try uninstalling it and reinstalling it from the **Meta Quest Store**.

5.7.7 Audio Problems (No Sound or Low Sound)

- **Volume Controls**: Make sure the volume is turned up using the volume buttons on the side of the headset.
- **Reboot the Headset**: If sound isn't working, reboot the headset to reset the audio system.
- **Check Headphones**: If using external headphones, ensure they're properly connected and the audio is set to output to them.
- **Adjust the Fit**: Make sure the earphones or speakers are positioned correctly.

5.7.8 Performance Lag or Low Frame Rate

- **Close Unnecessary Apps**: If the performance is slow, close background apps that may be using resources.
- **Reboot the Device**: Restart the headset to clear any background processes that might be slowing it down.
- **Check for Updates**: Go to **Settings** > **About** > **Software Updates** to ensure your headset is running the latest firmware.
- **Reduce Graphics Settings**: In certain games, reducing the graphics settings might help improve performance.

5.7.9 Overheating

- **Allow for Cooling**: If the device is getting too hot, take breaks and allow the headset to cool down.
- **Use in a Cooler Area**: Ensure the environment you're using the headset in isn't too hot. Avoid using it in direct sunlight or in hot rooms.

5.7.10 Pairing with the Meta Quest App

- **Ensure Bluetooth is On**: Make sure Bluetooth is enabled on your phone for the pairing process.
- **Re-pair the Device**: In the **Meta Quest App**, go to **Devices** > **Pair New Headset**, and follow the instructions.
- **Restart Your Phone**: If pairing issues persist, try restarting your phone and the headset, then attempt pairing again.

5.7.11 Factory Reset

- **Warning**: A factory reset will erase all your data and settings.

To Perform a Factory Reset:

1. Turn off your Meta Quest 2.
2. Hold the **volume down** button and the **power** button until the boot menu appears.
3. Use the volume buttons to select **Factory Reset** and confirm with the power button.
4. Wait for the reset to complete.

5.8 Benefits of Using XR/VR :

Cost-effective: Reduces the need for physical equipment and on-site trainers.

Safe Environment: Allows for risky situations to be simulated safely.

Engagement: Immersive learning keeps employees engaged, enhancing retention and reducing knowledge gaps.

Scalability: Can be rolled out to employees in different locations without the need for additional physical infrastructure.

Customizable: Training modules can be tailored to specific machinery, safety protocols, or emergencies that employees need to familiarize themselves with.

5.9 WHAT YOU HAVE TO DO ?

Research : Understand how immersive environments improve learning and design experiences that engage different learning styles.

Develop Software: Create interactive VR/XR platforms, 3D models, and simulations for subjects like science, history, and art.

User Testing: Prototype, test, and refine VR learning experiences with real students and educators to gather feedback.

Collaborate: Work with educators and researchers to ensure your VR/XR solutions align with curriculum and educational goals.

Explore New Technologies: Integrate AI, gesture recognition, and haptic feedback to enhance interactivity and personalization.

Ensure Accessibility: Focus on making experiences inclusive, with attention to disabilities and device accessibility.

Address Ethics & Privacy: Prioritize student data privacy and ethical considerations in immersive environments.

6. EVALUATION BOARD

6.1 Overview

5G EVB can be used to develop applications based on Quectel 5G modules.
This EVB can be used to test basic functionalities of these modules.

6.2 Specifications

Temperature Range	
1. Operating Temperature	-30 °C to +75 °C
2. Extended Temperature	-40 °C to +85 °C
Audio	
Voice	Digital Audio and VoNR/ VoLTE (Optional)
Frequency Bands	
5G NR	3GPP Rel-16 NSA/SA operation, Sub-6 GHz
5G NR NSA	n1/ 3/ 5/ 7/ 8/ 20/ 28/ 38/ 40/ 41/ 71/ 75/ 76/ 77 / 78
5G NR SA	n1/ 3/ 5/ 7/ 8/ 20/ 28/ 38/ 40/ 41/ 71/ 75/ 76/ 77 / 78
DL 4 × 4 MIMO(5G)	n1/ 3/ 7/ 38/ 40/ 41/ 71/ 77/ 78
LTE Category	DL Cat 20/ UL Cat 18
LTE-FDD	B1/ 3/ 5/ 7/ 8/ 20/ 28/ 32 /71
LTE-TDD	B38/ 40/ 41/ 42/ 43
DL 4 × 4 MIMO (LTE)	B1/ 3/ 7/ 38/ 40/ 41/ 42/ 43
WCDMA	B1/ 5/ 8
GNSS	GPS/ GLONASS/ BDS/ Galileo/ QZSS
Processor	Qualcomm X65
Data Rates (Max.)	
5G SA Sub-6	4.0 Gbps (DL)/ 900 Mbps (UL)
5G NSA Sub-6	4.0 Gbps (DL)/ 550 Mbps (UL)
LTE	2.0 Gbps (DL)/ 200 Mbps (UL)
WCDMA	42 Mbps (DL)/ 5.76 Mbps (UL)
Interfaces	
(U)SIM	× 2
UART	× 3
SDIO	× 1
USB 2.0/ 3.0/ 3.1	× 1
PCIe 3.0	Gen3, Lane × 2
PCM	× 1
SPI	× 1
Antennas	Cellular: × 4; GNSS: × 1
eSIM	Optional
Electrical Features	
Supply Voltage Range	3.3–4.4 V, typ. 3.8 V
Transmitting Power	
	WCDMA: Class 3 (23 dBm ±2 dB) LTE- FDD: Class 3 (23 dBm ±2 dB) LTE- TDD: Class 3 (23 dBm ±2 dB) 5G NR: Class 3 (23 dBm ±2 dB) 5G NR n38/n41/n77/n78: Class 2 (26 dBm ±2 dB)
Modulations	
5G	Supports UL 256 QAM and DL 256 QAM
LTE	UL & DL QPSK, 16 QAM, 64 QAM, 256 QAM

Wi-Fi 6	FC60E
Dimensions	25.5 mm × 22.0 mm × 2.25 mm
Weight (g)	Approx. 2.58 g
WLAN Protocol	IEEE 802.11a/b/g/n/ac/ax
Wi-Fi Frequency Band	2.4 GHz/ 5 GHz
Wi-Fi Antenna	2
Wi-Fi Modulation Mode	DBPSK/DQPSK/CCK/BPSK/QPSK/QAM
2.4 GHz Channel Bandwidth	20 MHz/ 40 MHz
5 GHz Channel Bandwidth	20 MHz/ 40 MHz/ 80 MHz
Encryption Mode	WPA3
Temperature Range	
Operating Temperature Range	-30 °C to +75 °C
Data Rate (Max.)	
802.11a	54 Mbps
802.11b	11 Mbps
802.11g	54 Mbps
802.11n	600 Mbps
802.11ac	866 Mbps
802.11ax	1774.5 Mbps
Interfaces	
PCIe	× 1
PCM	× 1
UART	× 1
Antenna Interfaces	12
Electrical Features	
I/O Power Supply Voltage	1.8 V
Power Supply Voltage	VDD_CORE_VL: 0.95 V VDD_CORE_VM: 1.35 V

6.3 Interface Application

This chapter describes the hardware interfaces of the 5G EVB, as listed below:

- Power supply
- Module TE-A interface
- PHY TE-A interface
- USB interface
- Audio interfaces
- Digital Audio Codec Board Connector
- Analog Audio Interfaces
- Earphone Interface
- (U)SIM interfaces
- UART interfaces
- SD card interface
- PCIe to USB interface
- Switches and buttons
- Status indicators
- Wi-Fi interface

- Antenna Interfaces
- It also provides information about the buttons, switches, status indication LEDs and test points to help
- developers use the EVB.

6.3.1 Power Supply

The 5G EVB can be powered by an external power adapter through the power jack (J0303).

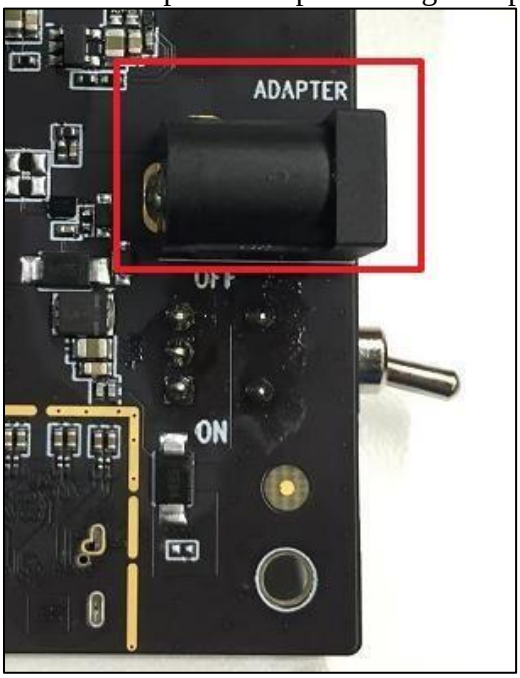


Figure : EVB Power Supply Interface

6.3.2 Module TE-A Interface (J0101/J0102)

Module TE-A interface is designed to accommodate the TE-A of the modules. The TE-A is mounted onto and connected to the EVB via BTB connectors J0101 and J0102. The developer will be able to test the functionalities of the modules easily (insert as indicated by the arrow to prevent reverse insertion).

The following figure displays the connection between the module TE-A and the EVB.

Figure : Connection Between the Module TE-A and the EVB

6.3.3 USB Interface (J1101)

A USB Type C connector, which complies with USB 3.0/3.1 and USB 2.0 standard, is provided. This USB interface is used for AT command communication, data transmission and firmware upgrade.

Figure : USB Interface Connection

6.3.4 Audio Interface (J0802/J0901/J0801)

EVB provides one digital audio codec board interface (I2S) J0802 and two analog audio interfaces J0901 and J0801.

6.3.5 Digital Audio Codec Board Connector (J0802)

The 5G EVB supports two different kinds of external digital audio codec TE-As named ALC5616 and TLV320AIC3104. The codec circuit is assembled on an independent small board which can be interconnected with the EVB by the BTB connector J0802.

Codecs can be selected according to specific application demands, the following figures show the connection between digital audio codec TE-A and the EVB.

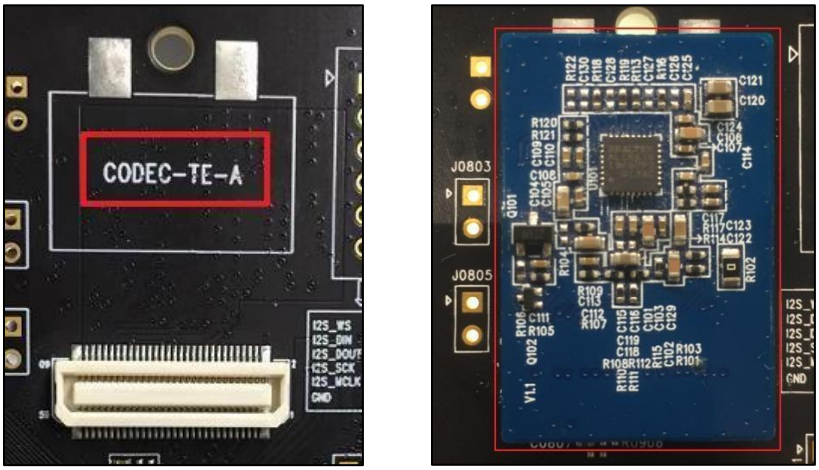


Figure : Connection Between Codec TE-A and the EVB

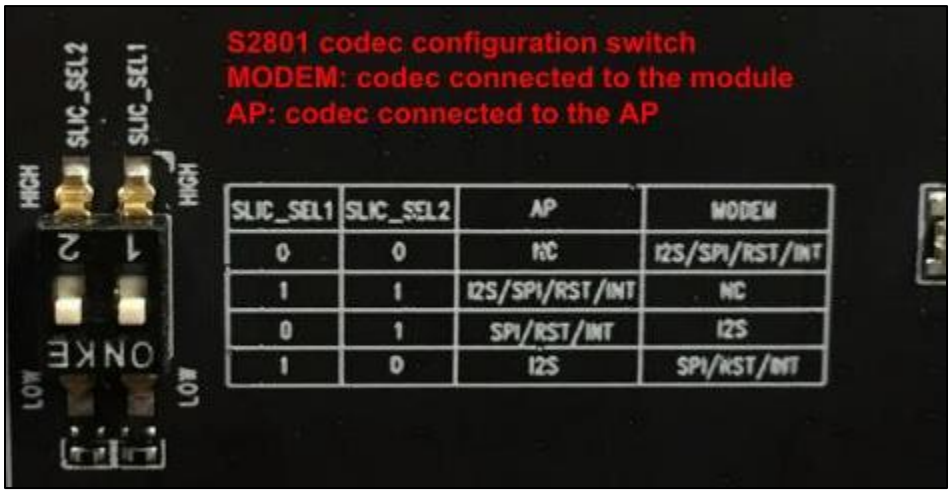


Figure : S2801 Switch

The figure and table below illustrates the pin assignment and pin definition of earphone connector J0901.

Figure : Pin Assignment of J0901

6.3.6 Table : Pin Definition of J0901

PIN NO.	PIN NAME	DESCRIPTION
1	MIC	Microphone input
2	AGND	Dedicated GND for audio
3	SPK R	Right channel of stereo audio output
4	SPK L	Left channel of stereo audio output
5,6	NC	Not Connected

The following figure shows a schematic of an audio plug which suits the audio jack on 5G EVB.

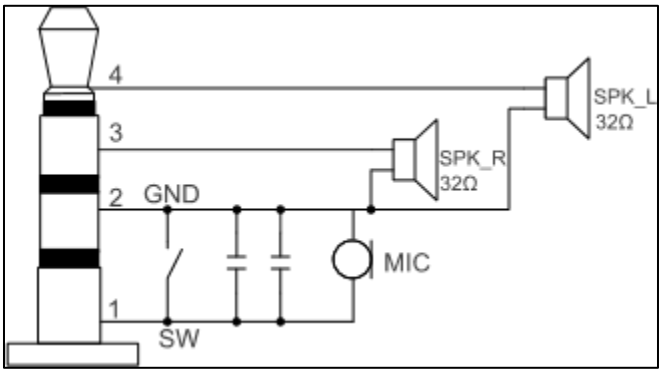


Figure : Schematic of Audio Plug

6.3.7 (U)SIM Card Interfaces (J1401/J1402)

The 5G EVB has two 8-pin push-push type (U)SIM card (1.8/2.95 V) connectors J1401 and J1402. The following figure shows a simplified connector schematic for J1401 and J1402.

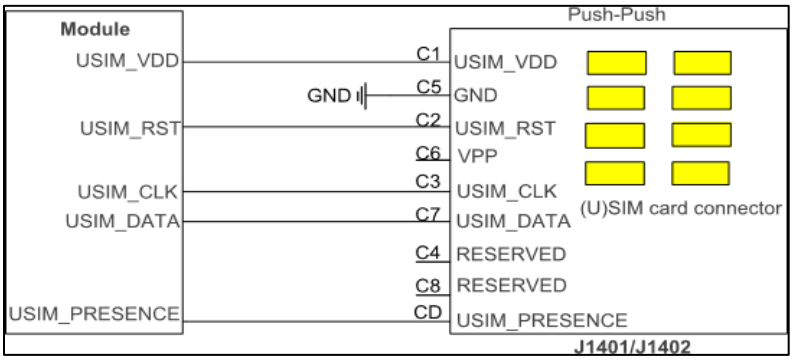


Figure: Simplified Connector Schematic for U(SIM) Card Connector

The figure and table below illustrate the pin assignment and definition of (U)SIM card connector J1401. J1402 is similar to J1401.

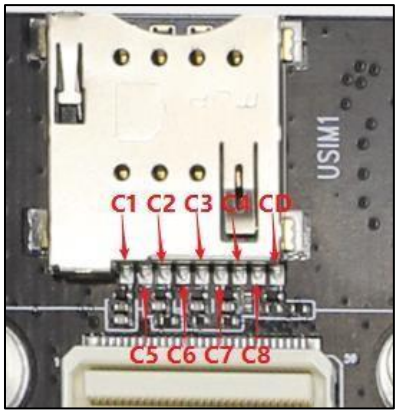


Figure : Pin Assignment of (U)SIM Card Connector J1401

6.3.8 Table : Pin Definition of J1401

C1	**USIM VDD**	**PO**	**U(SIM) card power supply , provided by module**
C2	**USIM RST**	**DO**	**U(SIM) card reset**
C3	**USIM CLK**	**DO**	**U(SIM) card clock**
C4	**RESERVED**	**-**	**Not Connected**
C5	**GND**	**-**	**Ground**
C6	**VPP**	**-**	**Not Connected**
C7	**USIM DATA**	**I/O**	**Data line, bi directional**
C8	**RESERVED**	**-**	**Not Connected**
CD	**USIM PRESENCE**	**DI**	**U(SIM) card insertion detected**

6.3.9 D Card Interface (J1301)

The 5G EVB provides an SDIO interface, which can be used for connecting SD card. The following figure shows the simplified interface schematic for J1301.

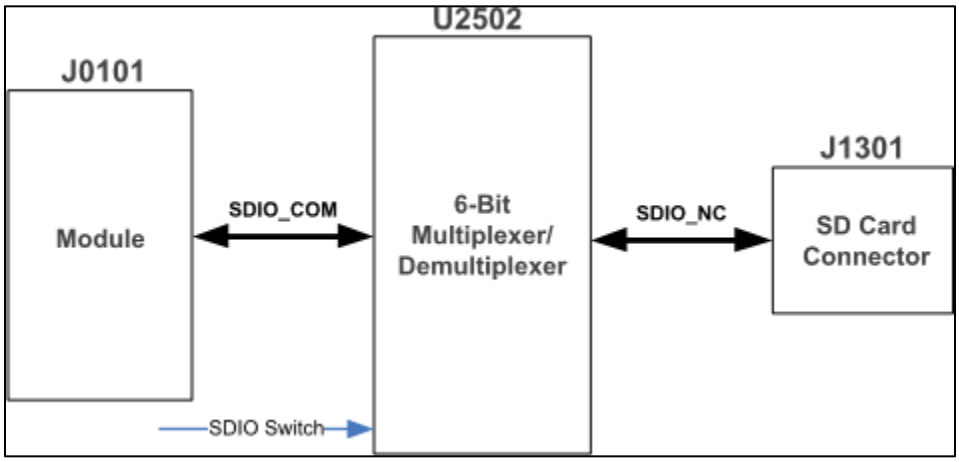


Figure : Simplified Interface Schematic for J1301

If SD card function is intended to be used, please switch the SDIO Switch to low level illustrated in the figure and table below, a standard SD card can be inserted into J1301. Which supports micro SD card of maximal 32 GB. With the SD card interface, customers can easily enhance the memory capacity of modules.

Figure : S2501 Switch

6.3.10 Table: SDIO Switch Function

SDIO SWITCH	FUNCTION
Low	Enable SD card Function
High	Enable emmc Function

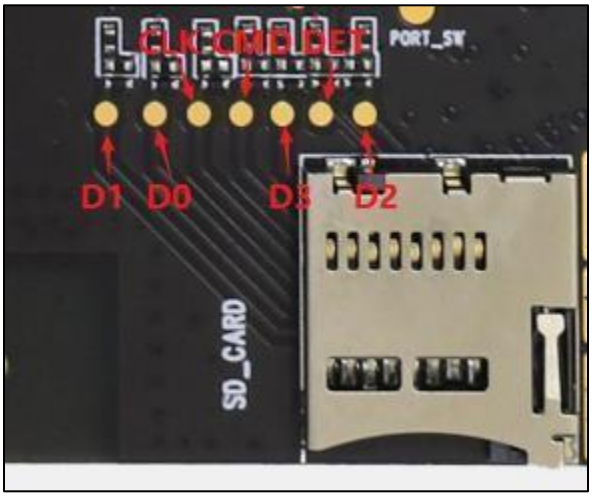


Figure : Pin Assignment of SD Card Connector J1301

6.4 UART Interfaces (J2002/J2003)

The 5G EVB supports two UART interfaces: main UART J2002 and debug UART J2003, supporting baud rate of 115200 bps by default.

The main UART interface is used for communication between the module and the host application. The debug UART interface is used for Linux console and log output.

The following figure shows a block diagram of UART interfaces of the EVB.

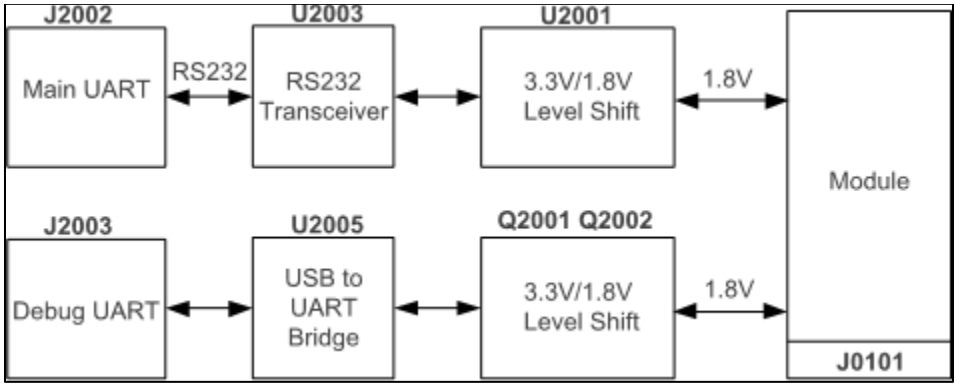


Figure : UART Block Diagram

6.4.1 PCIe to USB Interface (J1601)

The 5G EVB reserves a PCIe 3.0 signal over USB interface for developers' testing, and this function is not enabled by default. Please refer to the following block diagram.

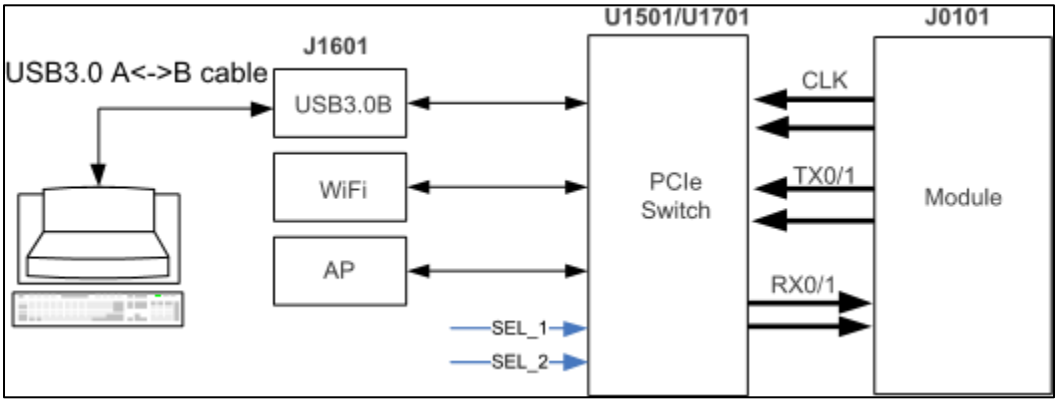


Figure : PCIe Block Diagram

Figure : S1501 Switch

6.4.2 Table : PCIe Connection Truth Table

PCIE SEL1	PCIE SEL2	FUNCTION
0	1	MODULE->PC
1	0	MODULE->AP
1	1	MODULE->WIFI

6.4.3 Switches and Buttons

The 5G EVB includes six switches (S0301, S1501, S1801, S1802, S2501 and S2801) and three buttons (S0201, S0202 and S0203), as shown in the following figures.

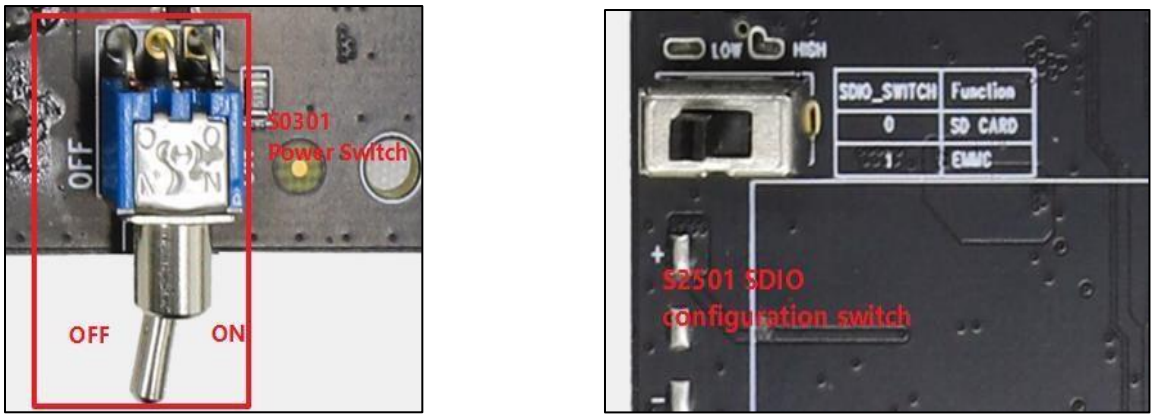


Figure : Power Switch and S2501 Switch

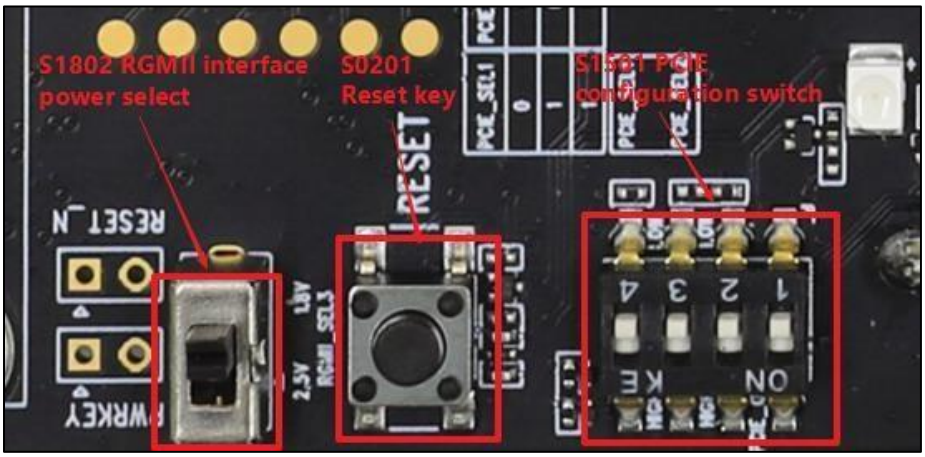


Figure : S1802/S1501 Switch and S0201 Button

Figure : S0202/S0203 Button

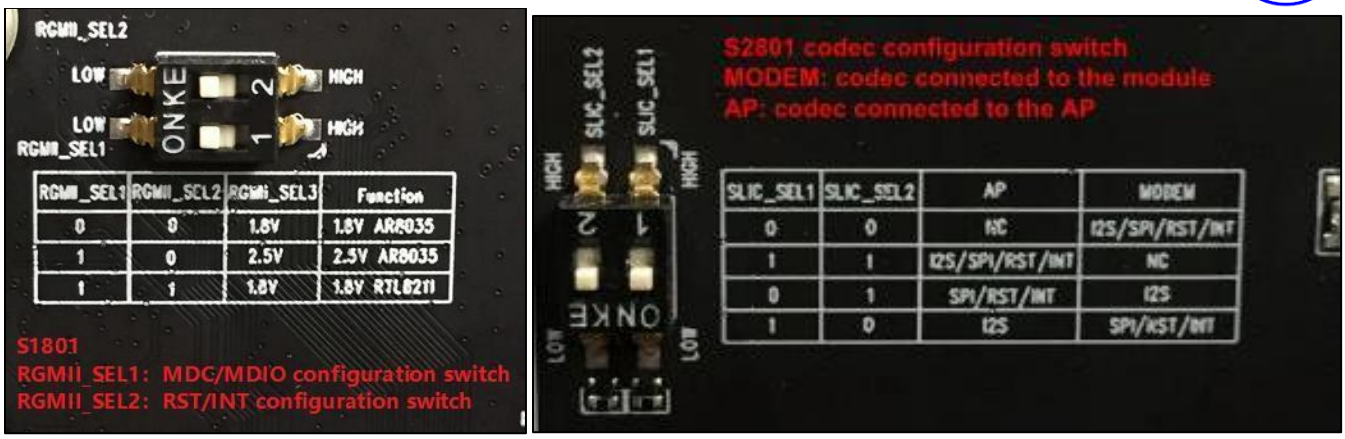


Figure : S1801/S2801 Switch

6.4.4 Table : Description of Switches and Buttons

Interface	Reference Designator	Description
Power Switch	S0301	VBAT ON/OFF control
PWRKEY	S0202	Power key used to turn on/off the module
PCIe Configuration	S1501	PCIe configuration switch. Refer to Chapter 3.9
RESET	S0201	Reset button used to reset the module
USB_BOOT	S0203	Emergency download control
RHMII Configuration	S1801, S1802	RGMII configuration switch Refer to Chapter 3.3
SDIO Configuration	S2501	SDIO configuration switch Refer to Chapter 3.7
Codec Configuration	S2801	Codec configuration switch Refer to Chapter 3.5

6.4.5 Status Indicators (D0201/D0202/D0203/D0204/D0205)

There are five status indication LEDs on the EVB. The following figure manifests the positions of these LED indicators.

Figure : Status Indicator

Table : Description of Status Indication LEDs

Reference	Description
D0201	Indicates whether the power supply for module is ready On: VBAT ON Off: VBAT OFF
D0202	Indicates the operation of the module. On: the module is power on Off: the module is power off
D0203	Indicates the module's NET_MODE status.
D0204	Indicates the module's NET_STATUS status.
D0205	Indicates the module's SLEEP status.

6.4.6 Wi-Fi Interfaces (J0701/J0702)

The Wi-Fi TE-A interface is designed to accommodate the TE-A of Wi-Fi modules (paired with FG50V). The TE-A is connected to the EVB via BTB connectors J0701 and J0702. The interface allows customers to test the Wi-Fi function of the module or to develop applications with Wi-Fi function easily.

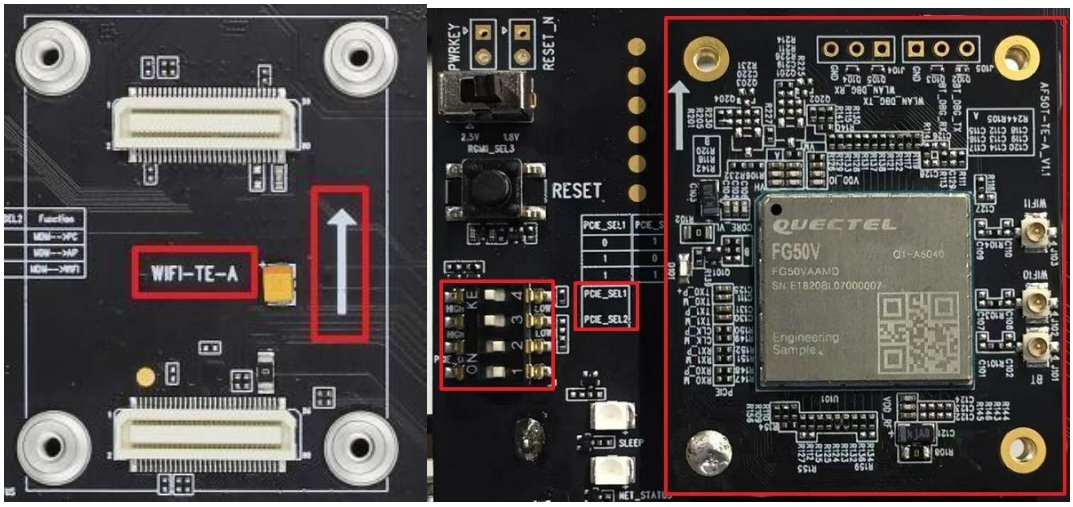


Figure : Connection Between FG50V-TE-A and the EVB

6.4.7 Antenna Interfaces

The 5G EVB includes twelve antenna interfaces. The following figure shows the assembly of these antenna interfaces.

Figure : Antenna Interfaces

6.5 Evaluation Board Operation Procedures

This chapter introduces how to use the 5G EVB for testing and evaluation.

6.5.1 Turn on the Module

1. Connect the module TE-A to the EVB via connectors J0101 and J0102.
2. Insert a (U)SIM card into the USIM1 card connector on EVB.
3. Use RF cable to connect the module TE-A to the EVB, and connect antennas to the EVB.
4. Connect the EVB to a 5 V/ 3 A power, then switch S0301 to ON. Then D0201 (ON/OFF indicator of the module's power supply) will light up.
5. Press the S0202 (PWRKEY) for at least 500ms, then the module will be powered on and D0202 (operation indicator of the module) will light up.

6.5.2 Communication via USB

1. Power on the module according to the procedure in *Chapter 1*.
2. Connect the EVB and a PC with USB cable through USB Type-C interface, and then run the driver disk on the PC to install the USB driver. The USB port numbers can be viewed in Device Manager of the PC when the USB driver is installed, as shown below.

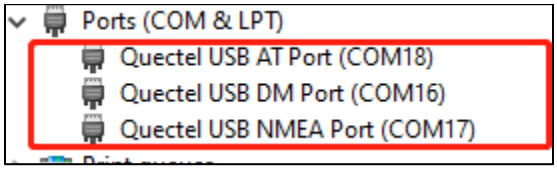


Figure : USB Ports

EVALUATION BOARD ANUBHAV (CORAL TELECOM)
WIFI Name – QsoftAP ; PASSWORD – 1234567890

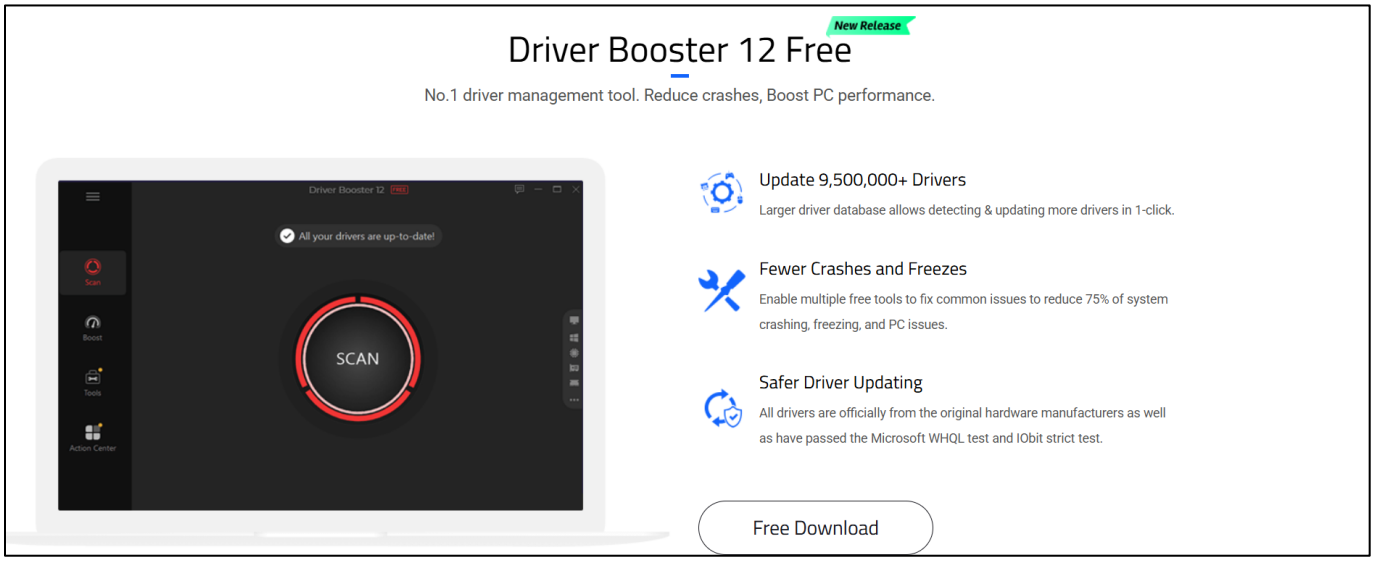
6.6 SETUP

6.6.1 ABBREVIATION:-

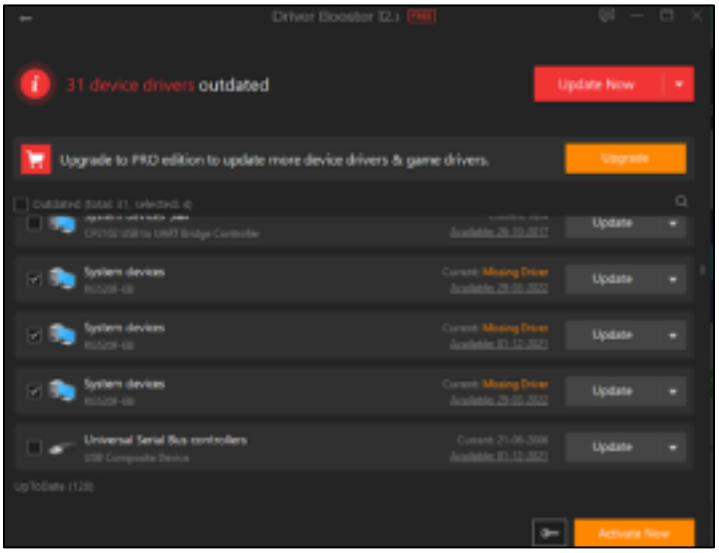
AT- TO INITIATE ---BASIC COMMAND REQUIRED FOR EACH ACTIVITY. ATA- FOR ANSWER/ACCEPT THE CALL
ATH- FOR HANG/CUT THE CALL.
ATD- TO DIAL A NO.

NOTE - Download a IOT DRIVER

1. Go to iobit.com
2. Click on free Download.

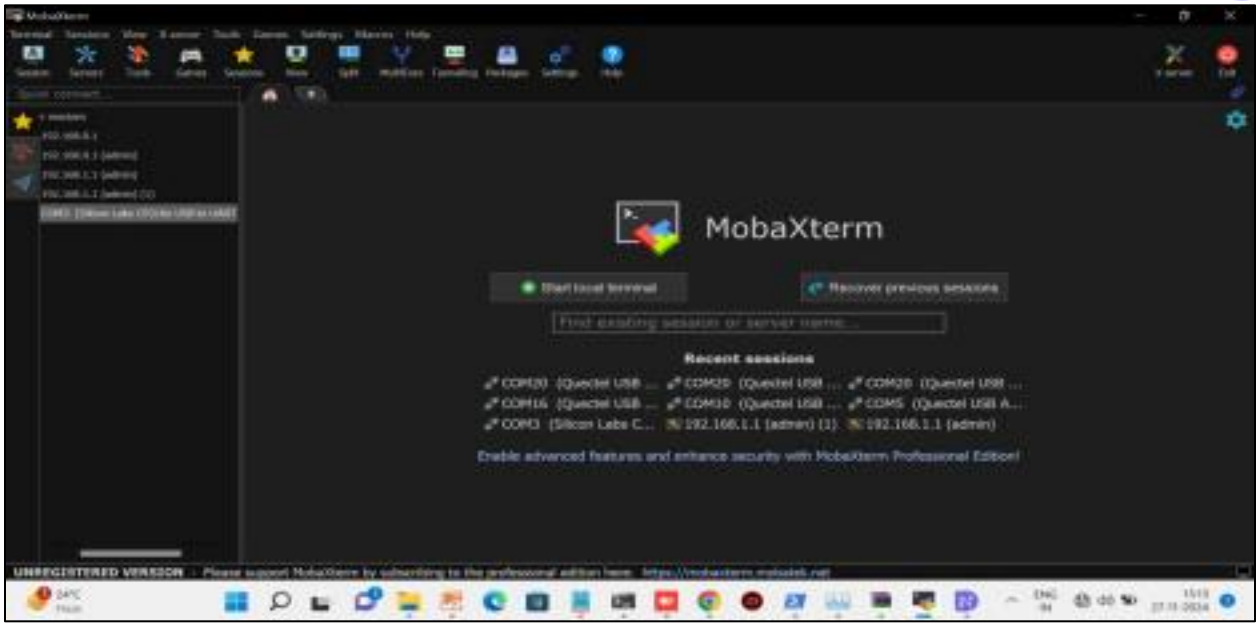


3. driver_booster_setup.exe file will download .
4. Open the file
5. Click on install button .
6. Decline the optional offer
7. Click on **NO THANKS**
8. Click on Scan
9. Untick Outdated all at the starting tab .
10. Select the System device RG520 F-EB , CP2102 USB to UART Bridge controller
11. Click on update now

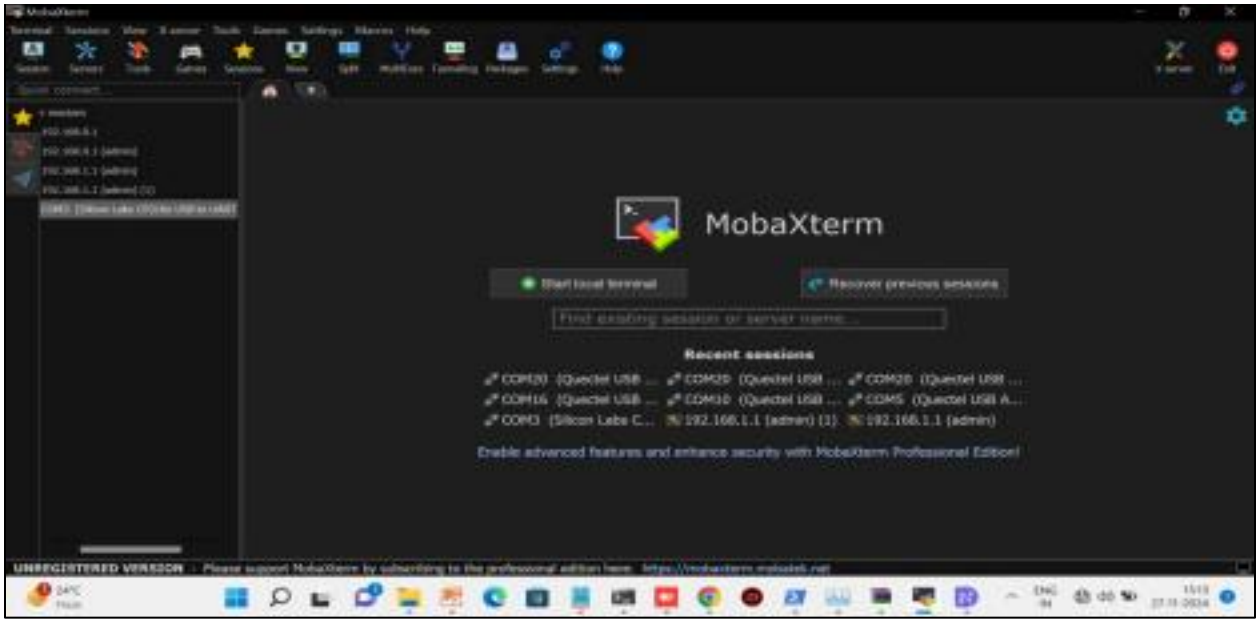


6.6.2 Steps to Run Evaluation Board

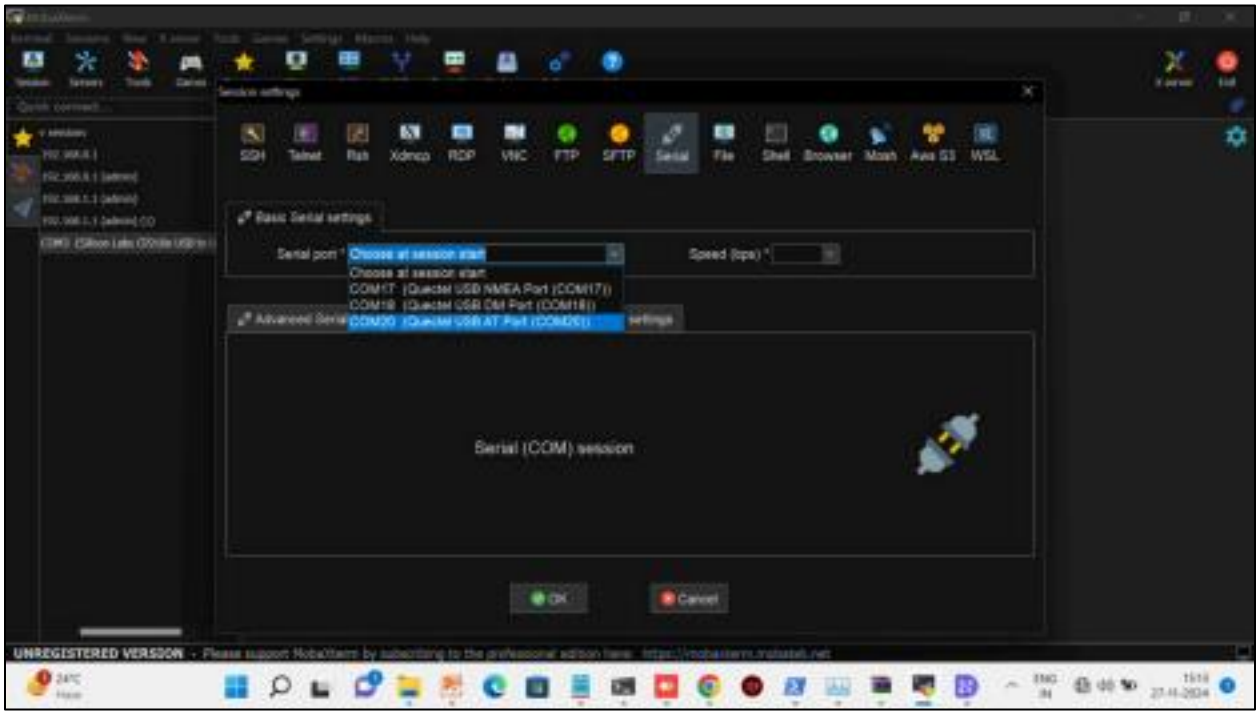
STEP-1-> OPEN MobaXterm Application on your WINDOWS PC.



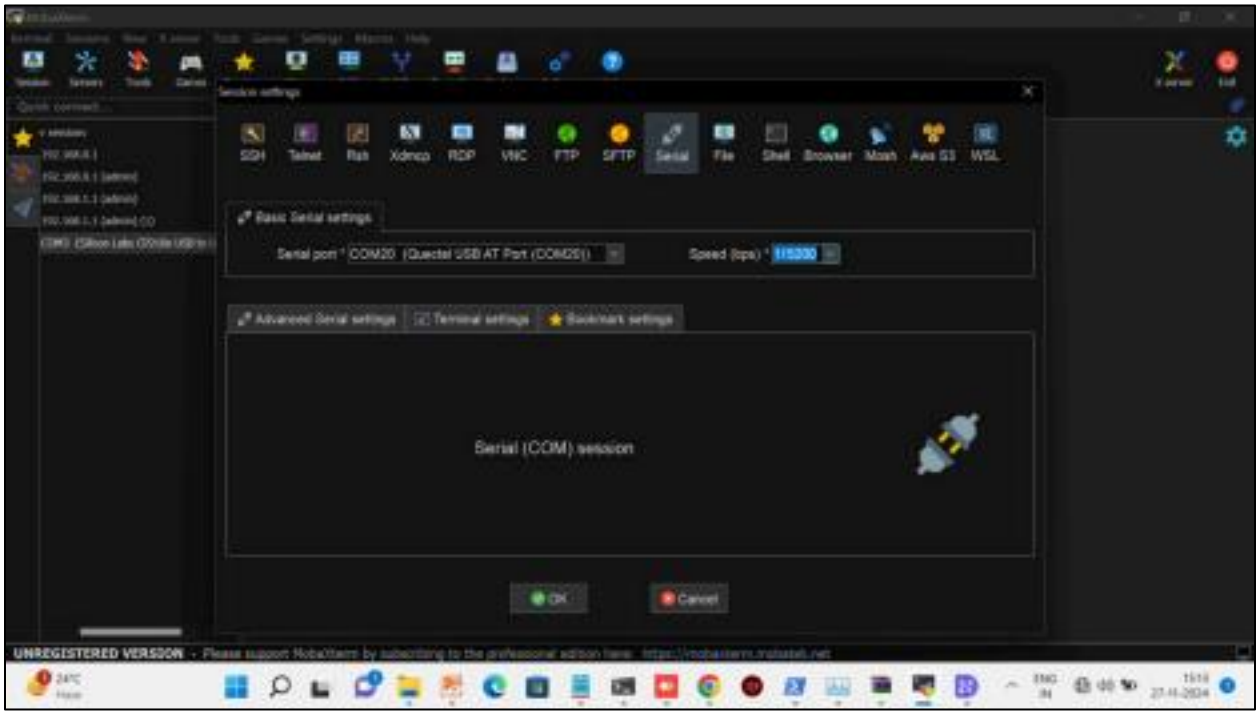
STEP 2-> Click on the session tab and go to serial .



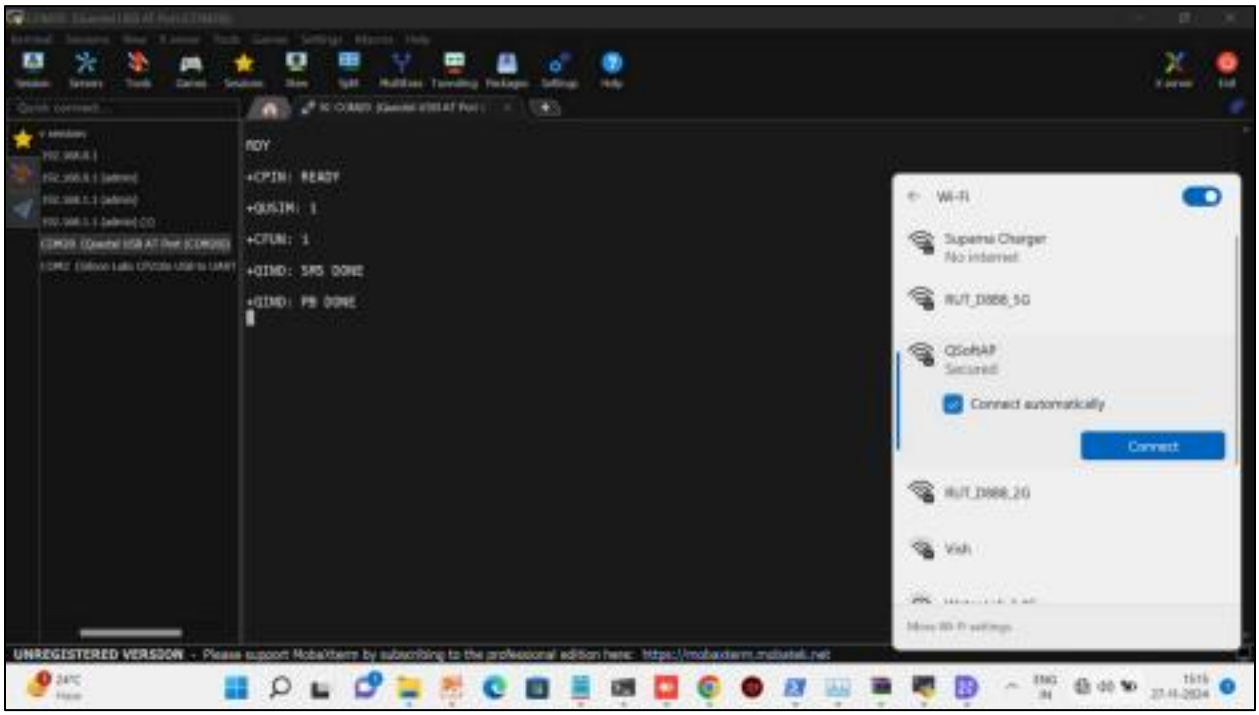
STEP3-> SELECT “USB AT” PORT (HIGHLIGHTED IN BLUE).



STEP4-> CHOOSE THE SPEED-- 115200 bps.



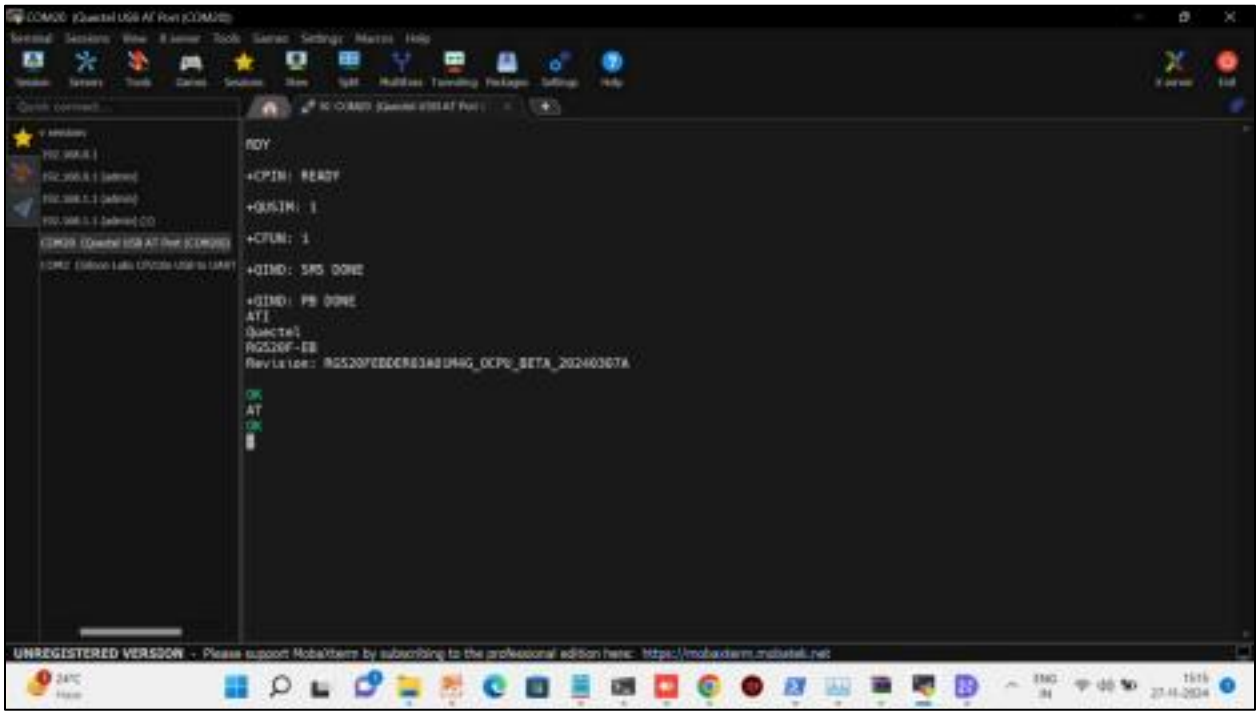
STEP 5-> CONNECT THE WIFI OF THE ANUBHAV NAME “QSoftAP” ; PASSWORD IS “1234567890”



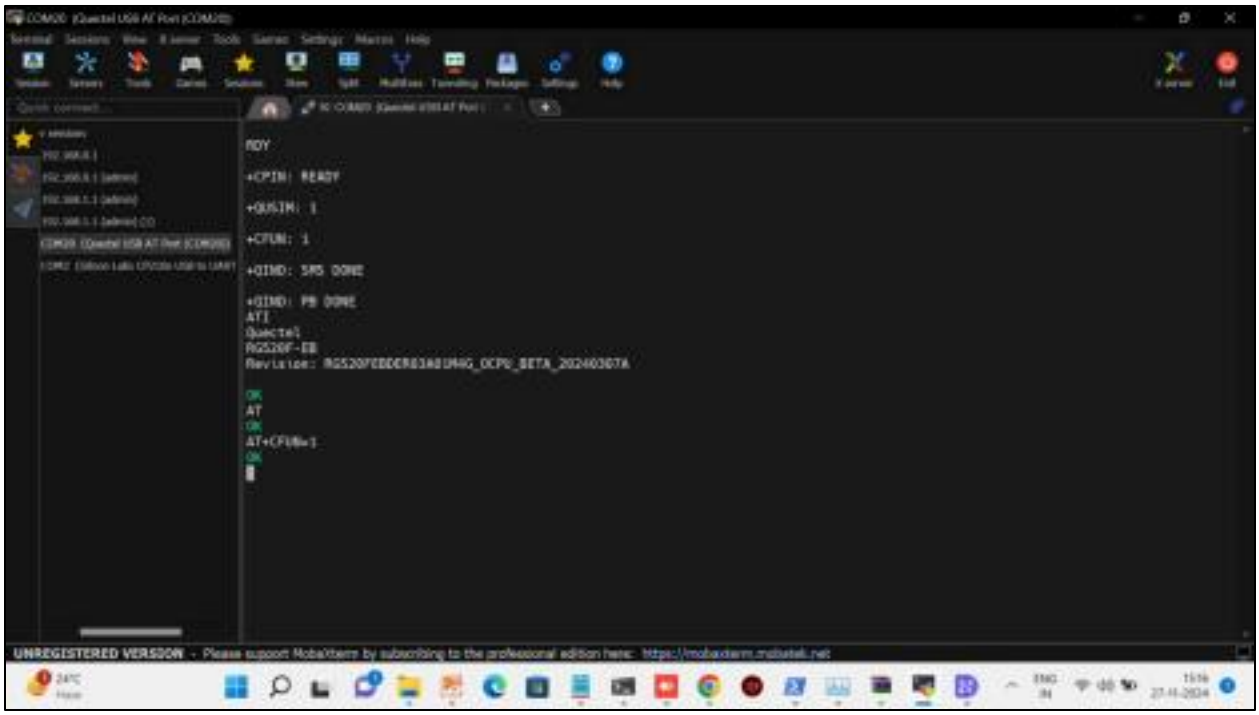
STEP 6-> 1. “AT” COMMAND

2. COMMAND IS “ATI”

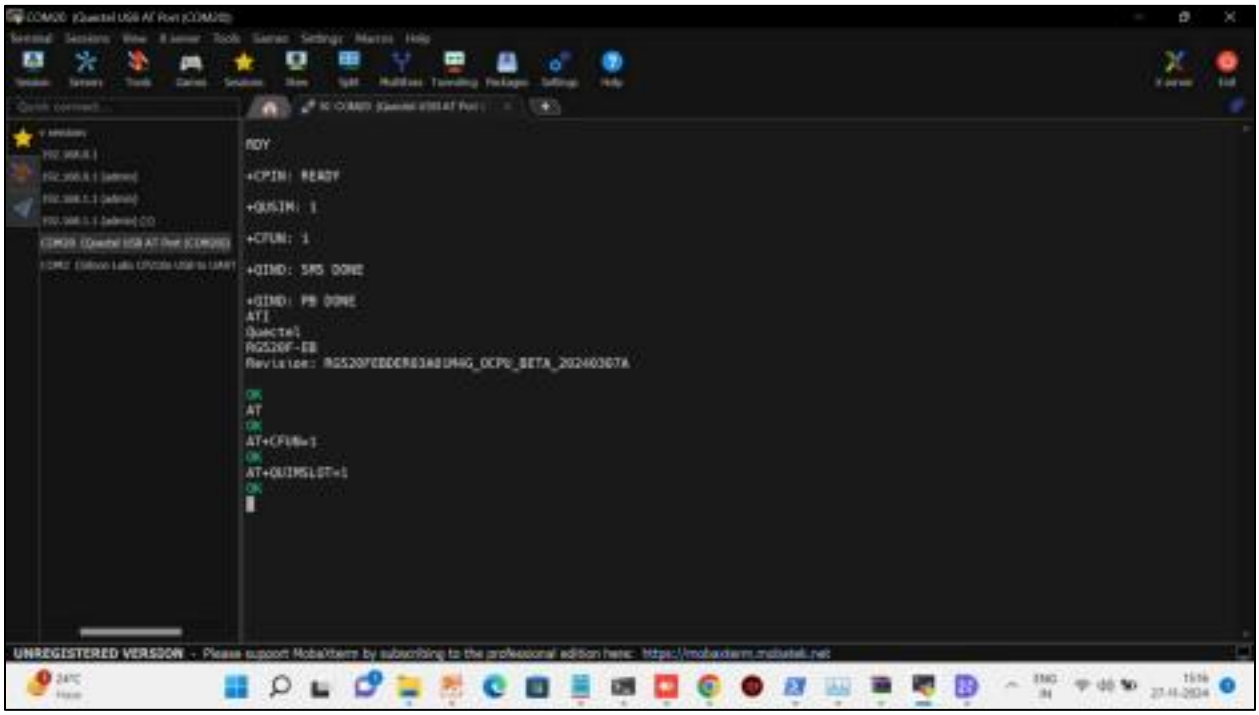
NOTE- TO INITIATE



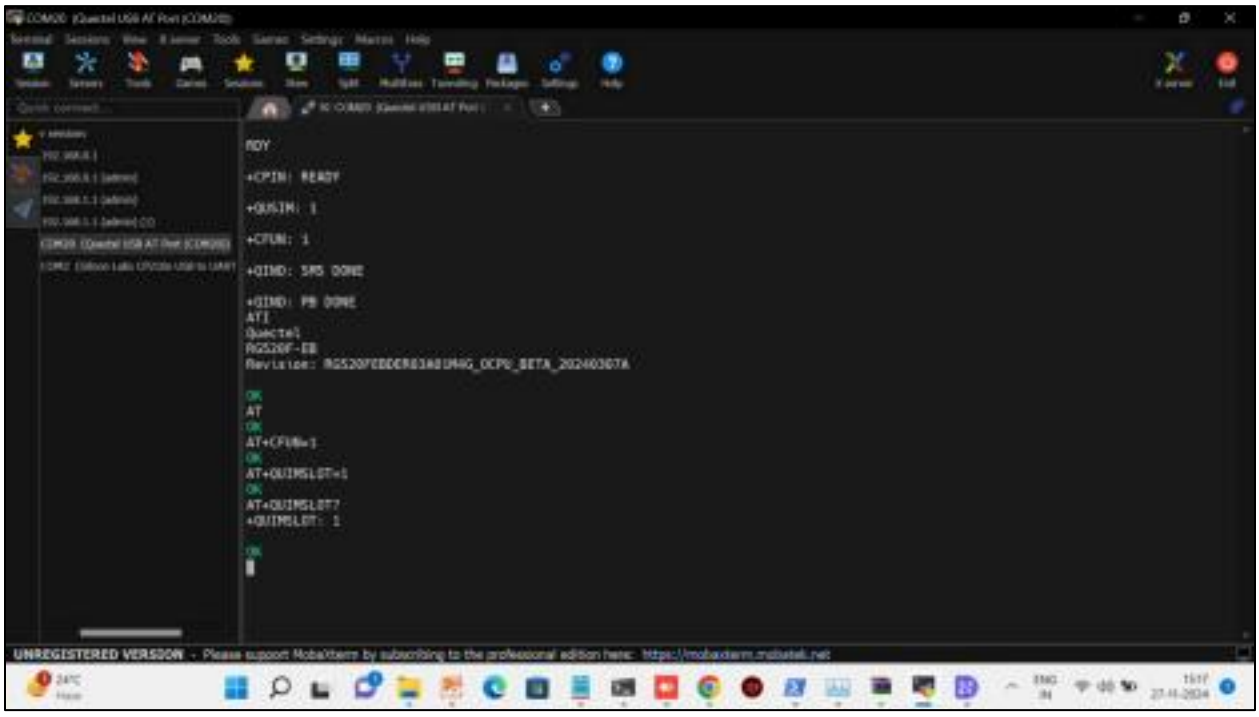
STEP 7-> START THE MODEM BY THE COMMAND “AT+CFUN=1”



STEP 8-> SELECT SIM SLOT 1 BY USING COMMAND “AT+QUIMSLOT=1”.
NOTE – MAKE SURE SIM IS IN SLOT 1.

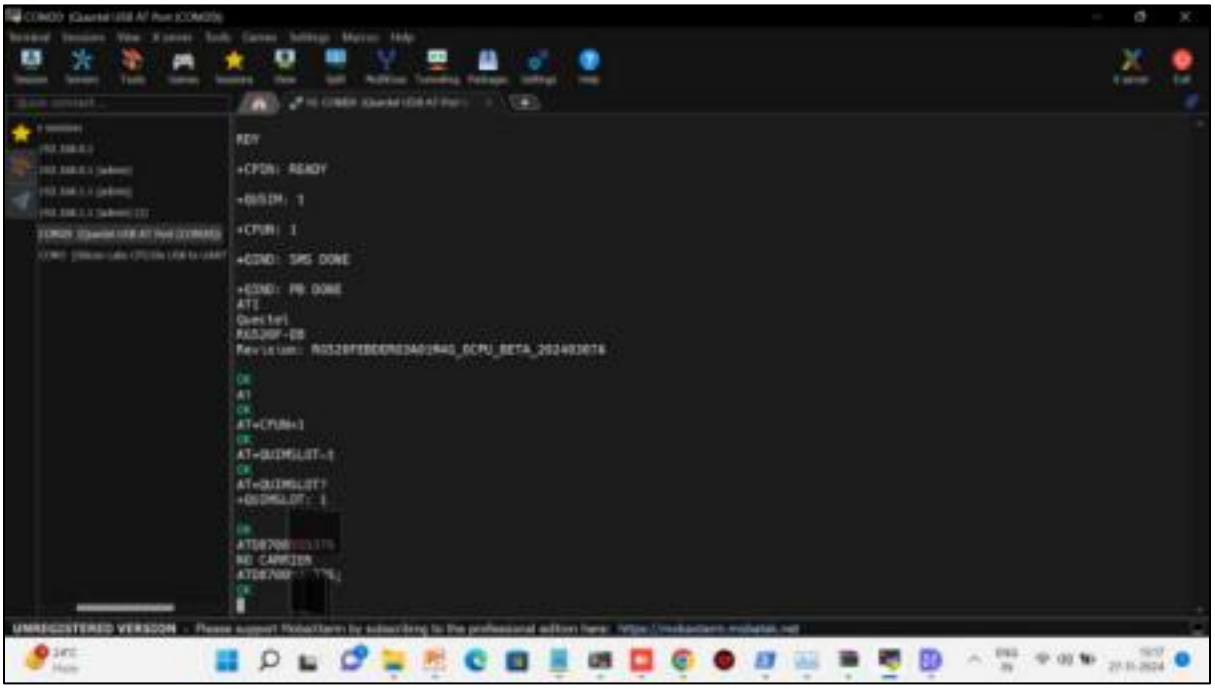


STEP 9-> CHECK THE WORKING SIM SLOT IN THE EVALUATION BOARD ;
COMMAND – “AT+QUIMSLOT?”
NOTE-“IF SIM IS INSERTED IN SLOT 2 THEN CHANGE IT TO SLOT 1”



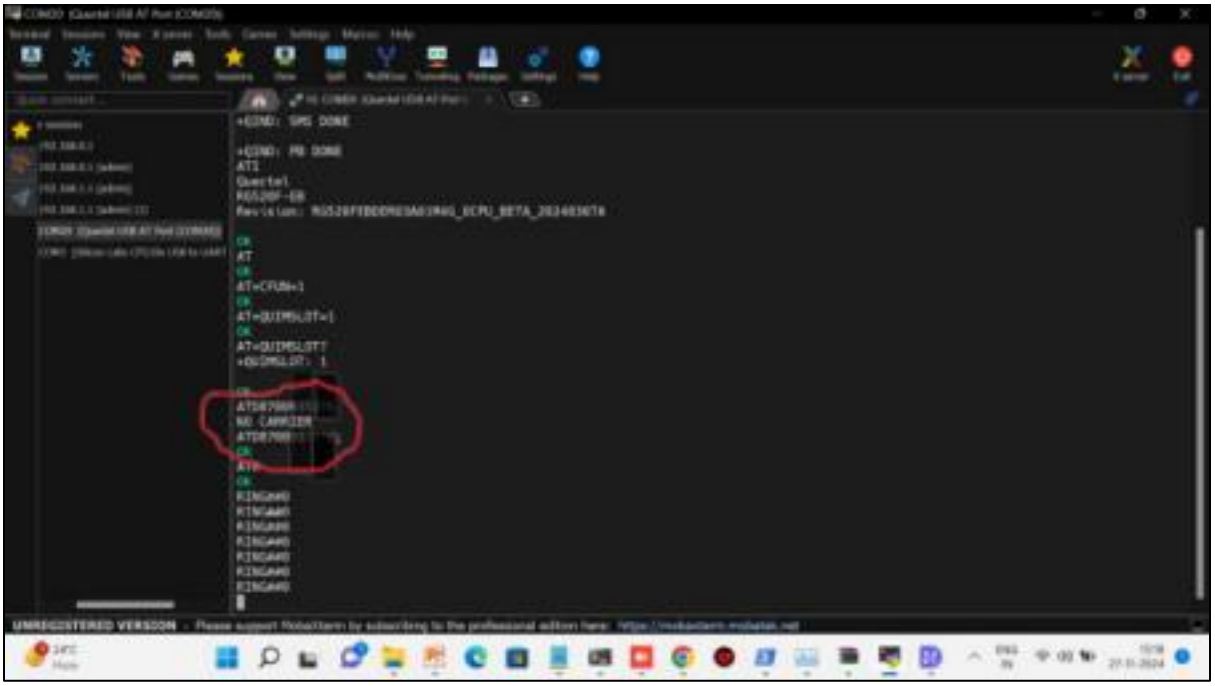
STEP 10-> DIAL A NUMBER WITH COMMAND “ATD8700######;”

NOTE- ##### - DENOTES PHONE NUMBER

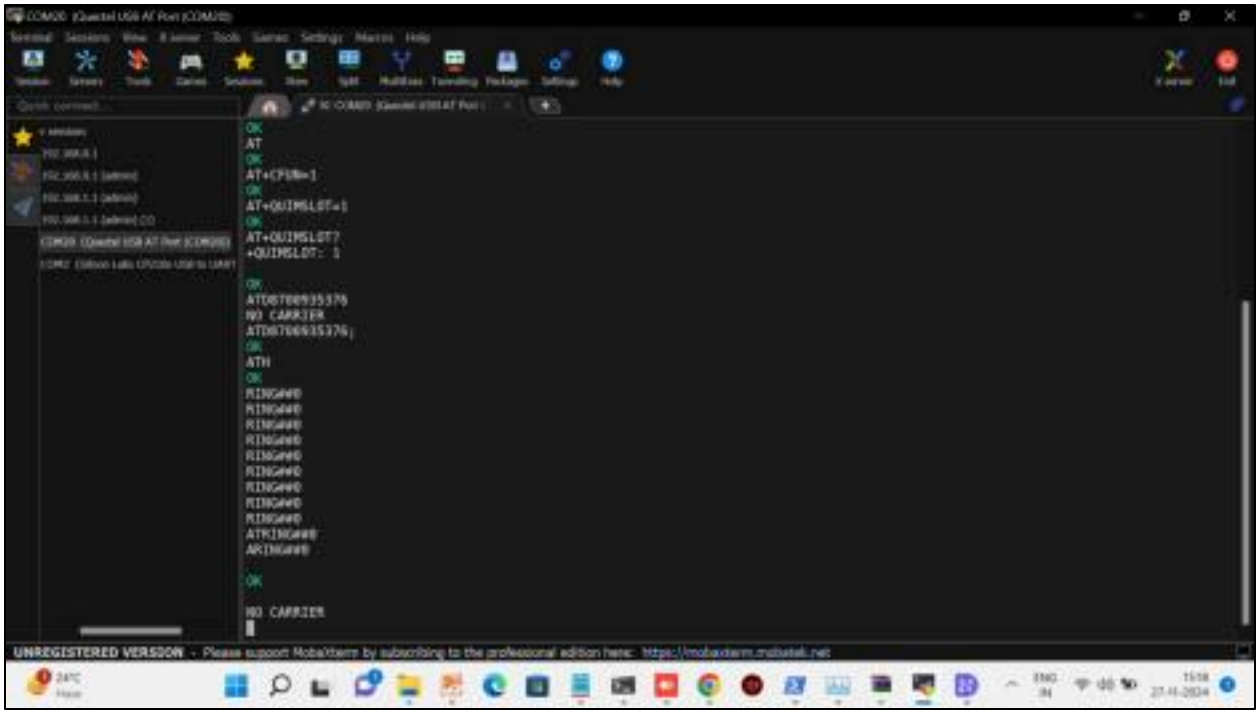


STEP 11->AFTER CALL INITIATE WE GOT THAT OUTPUT “OK”

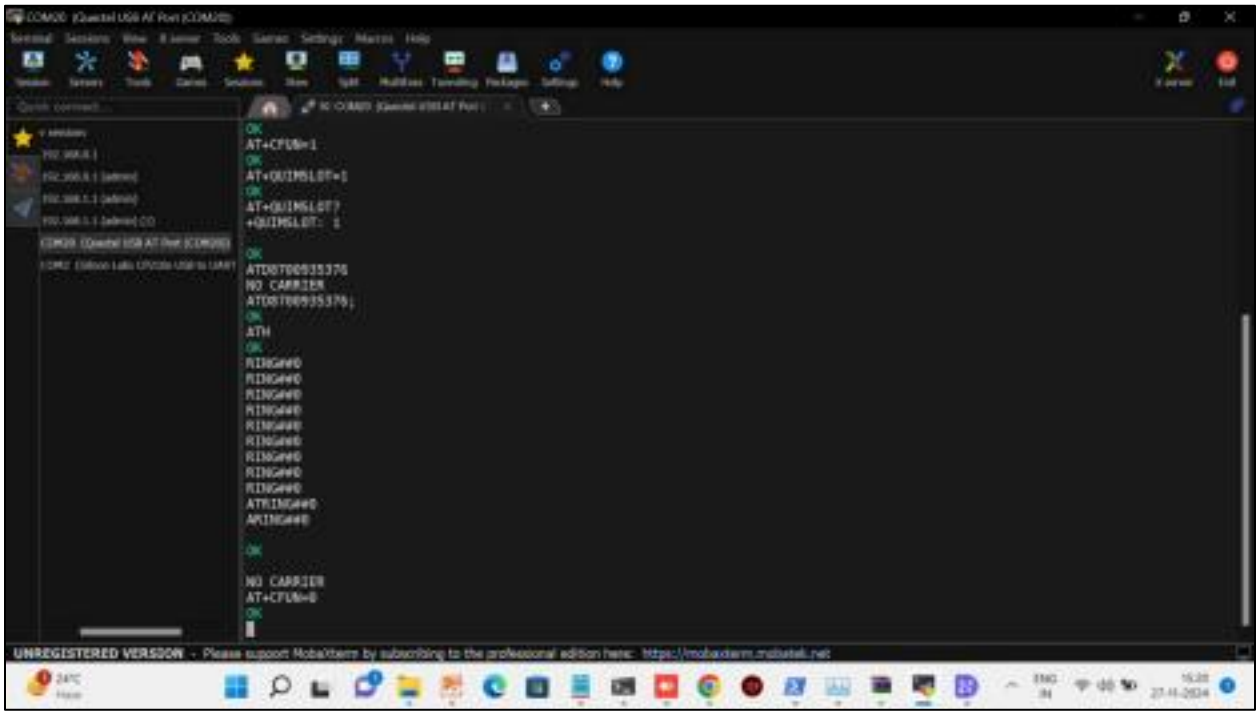
NOTE:- THIS TIME CALL IS INITIATED FROM THE BOARD “ANUBHAV”---- (HIGHLIGHTED IN RED CIRCLE)



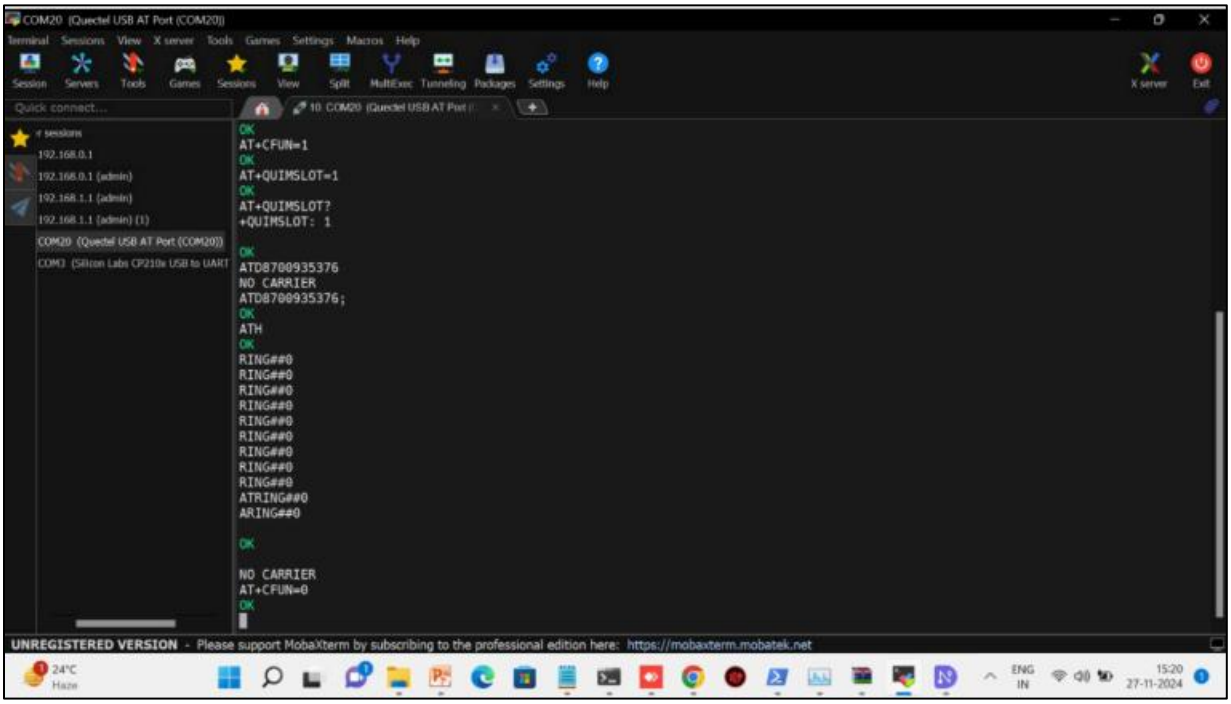
STEP:-12->> IF WE WANT TO HANG UP THE CALL FROM BOARD THEN WE HAVE TO GIVE THE COMMAND “ATH”AFTER SUCCESSFUL HANG UP WE GOT THE OUTPUT “OK”



STEP:-13->> IF WE WANT TO HANG UP THE CALL FROM CELL PHONE THEN NO COMMAND IS REQUIRED BUT WE GOT THE OUTPUT “NO CARRIER”.



STEP:-14->> IF WE WANT TO PICK UP THE CALL FROM BOARD THEN WE HAVE TO GIVE THE COMMAND “ATA”.



TO EXIT:-

1. FIRST COMMAND:- AT+CFUN=0 --- TO TURN OFF THE MODEM.
2. REMOVE THE SIM GENTLY.

Some Other Commands-
AT+CPIN - To know the details during receiving call.

6.6.3 Integrating With Raspberry Pi

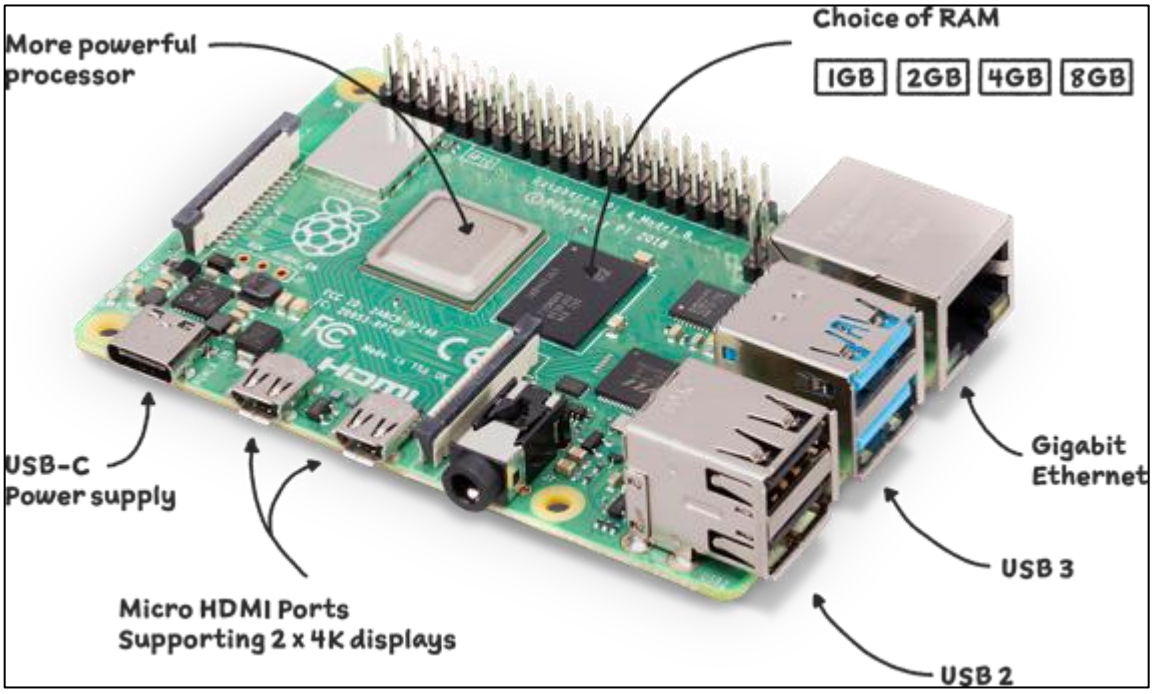


Fig - Showing the Diagram and interfaces of Raspberry Pi

6.7 SPECIFICATION

- Broadcom BCM2712 2.4GHz quad-core 64-bit Arm Cortex-A76 CPU, with cryptography extensions, 512KB per-core L2 caches and a 2MB shared L3 cache
- VideoCore VII GPU, supporting OpenGL ES 3.1, Vulkan 1.2
- Dual 4Kp60 HDMI® display output with HDR support
- 4Kp60 HEVC decoder
- LPDDR4X-4267 SDRAM (2GB, 4GB, 8GB, and 16GB)
- Dual-band 802.11ac Wi-Fi®
- Bluetooth 5.0 / Bluetooth Low Energy (BLE)
- microSD card slot, with support for high-speed SDR104 mode
- 2 × USB 3.0 ports, supporting simultaneous 5Gbps operation
- 2 × USB 2.0 ports
- Gigabit Ethernet, with PoE+ support (requires separate PoE+ HAT)
- 2 × 4-lane MIPI camera/display transceivers

- PCIe 2.0 x1 interface for fast peripherals (requires separate M.2 HAT or other adapter)
- 5V/5A DC power via USB-C, with Power Delivery support
- Raspberry Pi standard 40-pin header
- Real-time clock (RTC), powered from external battery
- Power button

Steps to Connect Evaluation Board with Raspberry Pi:

Power Off Both Devices

Ensure that both the Raspberry Pi and the evaluation board are powered off before making physical connections.

Connect via USB

Connect your evaluation board and Raspberry Pi using a USB to Type-C cable.

Power On Evaluation Board
Power on the evaluation board and press the reset button for 5-6 seconds until a green light appears.

Connect the Raspberry Pi to a Monitor
Connect the Raspberry Pi to a monitor using an HDMI cable.

Using a Monitor and Keyboard
Plug in a keyboard and mouse to the Raspberry Pi.
Power up the Raspberry Pi by connecting it to a power source.
Once booted, the Raspberry Pi will show the desktop interface.
To open the terminal, you can either:

- Click on the **Terminal** icon in the top-left corner (it looks like a black screen).
- Or press **Ctrl + Alt + T** to open the terminal.

Update the System
Run the following commands in the terminal:
sudo apt-get update
sudo apt-get upgrade

Install Minicom

Run the command:
sudo apt-get install minicom

Set Up Minicom
Run the following command:
sudo minicom -D /dev/ttyUSB2 -b 115200

Now the terminal is ready to use with the evaluation board.

Once inside minicom, try sending basic AT commands to the GSM module:

AT

If you see OK, it means the GSM module is responding properly.

Check the Network Registration

Before making a call, you should ensure the module is registered to a network. Use the following command:

AT+CREG?

This will return the network registration status. Look for CREG: 0,1 (home network) or CREG: 0,5 (roaming).

Make a Call

Now you can make a call using the ATD command. Replace <PHONE_NUMBER> with the number you wish to call (include the international code if necessary).

ATD<PHONE_NUMBER>;

- The” **;** “ at the end is necessary to initiate the call.

If everything is set up correctly, the GSM module will dial the number, and you should hear a ringing tone or the call will be initiated.

Answer a Call

If your GSM module is set up to receive calls, you can answer an incoming call with the following command:

ATA

Hang Up a Call

To hang up a call, you can use the following command:

ATH

Handling Errors and Troubleshooting

No network: Make sure the SIM card has a network signal. You can check the signal strength with the command:

AT+CSQ

7. IOT SENSOR

In this project, we're leveraging the power of 5G connectivity alongside a variety of IoT sensors to revolutionize environmental testing. With the help of our cutting-edge technology we have enhanced the accuracy and efficiency of our testing processes. By integrating IoT sensors into the labs and utilizing the high-speed, low-latency capabilities of 5G networks, we aim to elevate the quality of environmental testing across air, water, and soil domains. This innovative approach not only ensures compliance with industrial standards but also facilitates real-time monitoring and analysis for proactive environmental management.

7.1 TECHNOLOGY USED

MQTT (Message Queuing Telemetry Transport)

7.2 SENSOR USED IN THIS PROJECT

NPK Soil Sensor
TDS Sensor
Temperature & Humidity Sensor
Light Intensity Sensor

It facilitates efficient communication between IoT devices and the central monitoring system.
It enables real-time data exchange, critical for accurate environmental sensing.

7.3 SENSOR SPECIFICATION

7.3.1 LIGHT INTENSITY SENSOR

Chip: BH1750FVI Power Supply: 3.3V - 5V Light

Range：0 – 65535 lx(Lux) Sensor

Built-in: 16 bit AD converter Direct digital output, bypassing the complex calculation, bypassing the calibration Close to the spectral characteristics of visual Widely used to 1-lux high precision measurement Standard NXP IIC communication

7.3.2 TDS SENSOR

Input Voltage	3 ~ 6mA
Output Voltage	0 ~ 2.3V
Working Current	PH2.0-3P
Module Interface	3.3 ~ 5.5V
Electrode Interface	XH2.54-2P
TDS Measurement Range	0 ~ 1000ppm
TDS Measurement Accuracy	± 10% F.S. (25 ℃)

7.3.3 NPK SOIL SENSOR

Power supply: 5V Only
Maximum power consumption: ≤0.15W
Operating temperature: -40~80℃
NPK parameters: Range: 0-1999 mg/kg(mg/L)
Resolution: 1 mg/kg(mg/L)
Precision:±2%FS
Response time: ≤1S
Protection grade: IP68
Probe material: 316 stainless steel

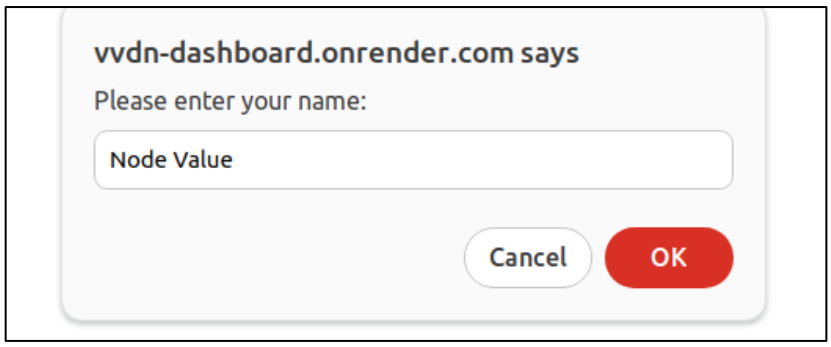
7.3.4 TEMPERATURE & HUMIDITY SENSOR

Operating Voltage: 5V
Temperature Range: -40 to 125 C
Humidity Range: 0~100%rh
Probe Material: Plastic + Metal Typ.
Temperature Accuracy: 0.3C Typ. Relative
Humidity Accuracy:3 %RH

7.5 DASHBOARD

STEP 1

Open url: https://vvdn-dashboard.onrender.com Enter the node of the sensor mentioned on sensors
Keep same node at same site example: All sensor should have same node mentioned on there box



7.6 How to Access Sensor Data

Setting Up MQTT client

Install Python on Windows or linux

Install Mqtt library -pip3 install paho-mqtt

MQTT Broker Details:

Server: broker.emqx.io

TCP Port: 1883

WebSocket Port: 8083

SSL/TLS Port: 8883

Secure WebSocket Port: 8084

Example Python Script to Listen Temperature Sensor

```
f# python 3.11

import random

from paho.mqtt import client as mqtt_client

broker = 'broker.emqx.io'

port = 1883

topic = "iot/Node-20/temp" # Replace node with current node of sensor

# Generate a Client ID with the subscribe prefix.

client_id = f'subscribe-{random.randint(0, 100)}'

username = 'vvdn'

password = 'vvdn'

def connect_mqtt() -> mqtt_client:

def on_connect(client, userdata, flags, rc):

if rc == 0:

print("Connected to MQTT Broker!")

else:

print("Failed to connect, return code %d\n", rc)

client = mqtt_client.Client(client_id)

# client.username_pw_set(username, password)

client.on_connect = on_connect

client.connect(broker, port)

return client
```

```
def subscribe(client: mqtt_client):

def on_message(client, userdata, msg):

print(f"Received `{msg.payload.decode()}` from `{msg.topic}` topic")

client.subscribe(topic)

client.on_message = on_message

def run():

client = connect_mqtt()

subscribe(client)

client.loop_forever()

if __name__ == '__main__':

run()
```

7.6.1 OUTPUT

23.5

23.6

23.7

```python
from paho.mqtt import client as mqtt_client


broker = 'broker.emqx.io'
port = 1883
topic = "iot/Node-22/temp"
# Generate a Client ID with the subscribe prefix.
client_id = f'subscribe-{random.randint(0, 100)}'
username = 'vvdn'
password = 'vvdn'


def connect_mqtt() -> mqtt_client:
    def on_connect(client, userdata, flags, rc):
        if rc == 0:
            print("Connected to MQTT Broker!")
            for i in range(100):
```

```
PS D:\Aman\New folder> & C:/Python312/python.exe "d:/Aman/New folder/Tutorial.py"
Connected to MQTT Broker!
23.5
23.5
23.5
23.5
23.6
23.5
23.5
23.5
23.5
23.5
23.5
23.5
23.5
23.5
23.5
```

7.6.2 5G CPE SETUP:

First, set the Wi-Fi credentials of TELTONIKA 5g Cpe to default SSID: RUT_D8B8_2G Password: Ec72Qsp4 As soon as sensor find the wifi it automatically connect and send data to cloud MQTT broker

7.6.3 DEBUG

Connect sensor to pc and open tera term(window) or minicom (linux) and connect on serial (port. baudrate: 9600 [115200 for tds]) and check the log. If not able to connect to internet it will show connecting to wi-fi else sensor reading will shown.

8. 5G Use-Case Of Evaluation Board

8.1 Steps to Start with Evaluation Board

Step 1: -Insert the Private 5G SIM in the Evaluation Board

Step 2: - Power on the Board using 5V Power Adapter

Step 3: - Press the Reset Button for 3-5 Seconds

Step 4: - Wait for 15 seconds for the Board to Boot Up

Step 5: - Install the appropriate drivers on the computer.

Recommended: Use Driver Booster: Driver Booster .

- Install the RG520F Drivers (Must Needed)
- Install the PORT Driver (Must Needed)

You are now ready to take the access of the evaluation board.

8.2 Basic Configuration Of Evaluation Board

Step 1: - Press Windows + X on your Windows Computer Home screen and navigate to Device Manager

Step 2: - When you will open the Device Manager you see a list of **Ports(COM & LPT)**

Step 3: - After that install MobaXterm from the internet - MobaXterm : - MobaXterm

Step 4: - MobaXterm is an advanced terminal emulator and remote desktop application designed for Windows. It provides a powerful set of tools for developers, system administrators, and IT professionals who work with remote systems.

8.3 Introduction to MobaXterm

MobaXterm is a powerful terminal and remote access tool for Windows. It supports SSH, RDP, FTP, and more, with a built-in X server and Unix commands. Ideal for developers and sysadmins, it simplifies managing remote servers and running Linux applications on Windows.

Before starting with MobaXterm , Follow these steps to establish connection:

1. Use the USB C(3.0) to connect the Evaluation Board with your system. Use the Type C port on the right side of the board.
2. Make sure the board is powered on with the 5V Power Adapter provided and along with that you have used a USB To Type C to make a connection between the system and 5G Evaluation Board.
3. Warning: Don't use the Debug UART for the Type C port as it has different usage.

8.3.1 Steps To Access Coral Anubhav with MobaXterm:

1. Once When You Will Open MobaXterm you will be welcomed with this screen
2. Select the option of Session on the Top-Right Corner of the Screen
3. Once you will click on that you will see another window
4. Once you get to this screen go for serial connection which have the logo of plug connector
5. In This Screen you will Select the AT Port and will enter the BAUD Rate as 115200
6. After all this you will be able to access the Coral Anubhav
7. Type ATI to see the Basic Details :

8.3.2 Introduction To Attention Commands (AT Commands)

AT commands (Attention commands) are used to communicate with modems or modules via serial communication. They help configure settings, retrieve information, or control device functionalities.

A. Types of AT Commands

- **Test Command (=?) -** The command returns the list of parameters and value ranges set by the corresponding Write Command or internal processes.
  - Syntax: AT+COMMAND=?
  - Purpose: Lists all possible values a command supports.
  - Example Response: +CONFIG: (0,1,2,3), indicating valid options.
- **Read Command (?) -** The command returns the currently set value of the parameter or parameters.
  - Syntax: AT+COMMAND?
  - Purpose: Queries the current value of a setting.
  - Example Response: +CONFIG: 2, meaning the current setting is 2.
- **Write Command (=<parameters>) -** The command sets the user-definable parameter values.
  - Syntax: AT+COMMAND=<value>
  - Purpose: Sets a new value for the configuration.
  - Example Response: OK, confirming the update.

AT Command	Functionality
ATI	Returns model number and firmware version.
AT+CIMI	Returns IMSI number.
AT+COPS=?	Displays list of available networks; check if network "00101" is available.
AT+CFUN=0	Switches UE to minimum functionality (returns OK).
AT+CFUN=1	Switches UE to full functionality (returns OK).
AT+CGDCONT?	Displays list of APNs; check APN configuration as per network slice.
AT+CGDCONT=1,"IP","APN-Name"	Set APN to "APN-Name".
AT+QNWPREFCFG="mode_pref",NR5G	Set the Evaluation board to work in NR5G mode only (returns OK).
AT+COPS?	Displays details of the registered network; if only "0" (automatic) or "1" (manual), the board is not registered.
AT+COPS=1,2,"00101"	Manually registered to network "00101".
AT+CGPADDR=1	Checks if an IP address is assigned. If 0.0.0.0, PDU session is not established; try CFUN=0 & CFUN=1.
ATD123456789;	Dials the 123456789 if it is present on the network
AT+QCFG=?	To list available configuration settings:
AT+QCFG="wifi/model", "fc60e"	To set the Wi-Fi module model to "fc60e":
AT+CHLD=1	To retrieve the held call:
AT+CHLD=2	To put a call on hold:

8.4 Configuring 5G Evaluation for 5G Registration

Now, we will look at how to connect your 5G Evaluation board with the radio and establish 5G Registration.

Entire registration part is divided into 4 Steps

Step 1: Set network mode preference to NR5G

- Set Network Preferences: **AT+QNWPREFCFG="mode_pref",NR5G**

Step 2: Set APN to 'APNname' for data connection.

- Set APN: **AT+CGDCONT=1,"IP","APNname"**

Step 3: Set the operator selection on Automatic mode

- Set operator selection on automatic mode: **AT+COPS=0**

Step 4: Reload The 5G Evaluation Board (Set UE Functionality)

- **AT +CFUN=0**
- **AT+CFUN=1**

8.5 Raspberry Pi Use Case With Coral Anubhav

Recommended : - To Access A Raspberry PI you will have to know its:

1. IP Address
2. Username & Password

NOTE: Check if your Raspberry PI has the Wi-Fi module available or otherwise use a wireless dongle to transmit the data

Step 1: Turn on your Raspberry Pi and take the access of it and run the command: -raspi-config

Step 2: You will be see this screen :

- Select System Options

Step 3: After Selecting System Option you will see this screen :

Select wireless LAN from which you want to transmit the data and then enter the name of your Wi-Fi in the option of SSID:

After that enter the password of your Wi-fi through which data needs to be transmit

-Now your Sensor Data will be transferred via Coral Anubhav(Evaluation Board) to the NMS via the 5G network.

8.6 Use Cases of Automating 5G Evaluation Board (Coral Anubhav) Configuration with Bash Scripts on Raspberry Pi

8.6.1 Introduction

This use case explores the practical applications of automating the configuration of the 5G evaluation(Coral Anubhav) using Bash scripts on a Raspberry Pi. By leveraging predefined commands, users can efficiently manage network registration, modem setup, and configuration changes without manual intervention. This automation enhances reliability, speeds up deployment, and reduces human errors in 5G connectivity setups, making it ideal for IoT applications, industrial automation, and research projects. The guide provides a step-by-step approach to executing AT commands via Bash, ensuring seamless interaction between the Raspberry Pi and the 5G modem.

8.6.2 Prerequisites

- Raspberry Pi (any model with USB support)
- 5G Evaluation Board (Coral Anubhav)
- SIM Card
- Minicom or another serial communication tool
- USB-to-Serial driver installed (if necessary)

8.6.3 Setup Instructions

Run as Root:

sudo -i

Check Device Path:

ls /dev/ttyUSB*

Install Required Packages:

sudo apt update && sudo apt install -y socat;

Grant USB Permissions:

sudo chmod 777 /dev/ttyUSB*

8.6.4 Bash Script for Modem Configuration

Create a script `modem_config.sh` to execute AT commands using `socat`.

#!/bin/bash

Check if minicom is installed

if ! command -v socat &> /dev/null; then

```
echo "socat is not installed. Installing..."

sudo apt update

sudo apt install -y socat

else

echo "script is started."

fi

# the command run and output show in file

echo ATI | socat - /dev/ttyUSB2,crnl > /tmp/hello;

echo AT+cimi | socat - /dev/ttyUSB2,crnl > /tmp/hello;

echo AT+QNWCFG=? | socat - /dev/ttyUSB2,crnl >/tmp/hello;

#when you want to append the output

#echo AT+QNWCFG=? | socat - /dev/ttyUSB2,crnl >>/tmp/output.txt;

# for print on file and terminal

#echo ATI | socat - /dev/ttyUSB2,crnl | tee /tmp/hello;

# read command thru file and output both to terminal and file

#cat commands.txt | socat - /dev/ttyUSB2,crnl | tee /tmp/hello
```

8.6.5 Running the Script

Make the script executable and run it:

```
chmod +x modem_config.sh

sudo ./modem_config.sh
```

8.6.6 Creating a System Service for Automation

To automate the execution of the script, create a systemd service.

```
[Unit]
Description=5G Modem Configuration Service
After=network.target
```

[Service]
ExecStart=/bin/bash /path/to/modem_config.sh
Restart=always
User=root

[Install]
WantedBy=multi-user.target

Save the file as `/etc/systemd/system/modem_config.service` and run the following commands to enable it:

sudo systemctl daemon-reload

Reloads systemd to recognize new or modified service files.

sudo systemctl enable modem_config.service

Enables the service to start automatically on boot.

sudo systemctl start modem_config.service

Starts the service immediately without rebooting.

TroubleShooting of Coral Anubhav

8.7 Basic Checks

1. **Power & Hardware Connections**
- Ensure the module is properly powered
- Check if the antennas are connected (for optimal signal reception)
- Verify the SIM card is inserted correctly
2. **Driver & Firmware Verification**
- Check if the necessary drivers are installed (Linux/Windows)
- Ensure firmware is up-to-date
- Default Baud Rate as 115200. Evaluation Board will communicate with devices on this BAUD Rate
3. **AT Command Interface Check** Use AT commands to verify basic functionality
- AT → Check if the module responds
- ATI → Get manufacturer info
- AT+CGMR → Get firmware version

Debugging Logs

- Insert a USB Type-C connection with Debug UART and then switch to the **Silicon Labs CP210x USB-to-UART Bridge**. Set the BAUD Rate as 115200.This will provide access to hardware-level logs and detailed diagnostic information for all modules and features.

Device and Module Info

- Get Firmware and Device Information:

  AT+CGMR - Display firmware version.

- Check 5G MIMO Status:

  AT+QNWCFG="nr5g_mimo" -Check if 5G MIMO is enabled.

- Enable 5G MIMO:

  AT+QNWCFG="nr5g_mimo",1-Enable 5G MIMO.

ADB(Android Debugging Bridge) Access

- To check about the Coral Anubhav services we can access it by taking adb access to the Coral Anubhav Board.
- Take access by adb shell after connecting it via USB 3.0 provided
- Enter the command - **systemctl status *.service**