Rapidise integrates its access control, video management, and AI capabilities into a cohesive system that uses smart edge devices to communicate actionable intelligence to a centralized, multi-tenant cloud platform. This unified structure ensures seamless **remote management**, supports diverse **multi-device** deployments, and delivers critical **AI-based event insights**.

Here is a detailed breakdown of how these components are connected and the benefits they provide:

1. Connection Architecture: Edge-to-Cloud Unification

The core connection strategy involves smart edge hardware reporting security data and video streams to a unified cloud platform.

A. Access Control & Smart Gateway Controllers

- **Smart Gateway Controllers** and Access Control Systems (such as the **Multi-Tenant Access Control System** and the **Smart Gateway For Access Controller**) act as the physical intelligence points.
- These devices leverage various communication protocols, including **Cellular, Ethernet**, **LoRaWAN**, and **WiFi-6 and BLE-5.4**, to connect to the network.
- Security and video data are transmitted using the **MQTT Communication Protocol** (or similar IoT dataflow architectures) to the cloud.

B. Video Management Platform (VMS Portal)

- Rapidise developed a **Multi-Tenant Custom Cloud Video Management Software (VMS)** designed to replace existing third-party portals.
- The VMS serves as the central hub, operating on **Amazon Web Services (AWS)**.
- The VMS uses a **Multi-Tenant architecture strategy**, managed using **Docker**, which provides **completely isolated tenants** while reducing server infrastructure costs.
- The portal supports **video encoding** using **FFmpeg** and handles **Live Streaming** using **WebRTC** technology.

2. Functions and Benefits: Remote Management & Multi-Device Support

The unified platform enables comprehensive control and monitoring across multiple security assets.

A. Remote Management and Control

- The cloud platform provides businesses with **full control over their access systems with minimal setup**.
- The VMS enables users to **manage and distribute video content seamlessly**, offering a user-friendly interface for video playback, customization, and analytics.
- The Access Control Systems themselves support enhanced functionality and **remote control**, allowing management of building security without bulky traditional hardware.
- The **Embedded Software** capabilities support **FOTA (Firmware Over the Air)** updates, allowing devices (cameras and access controllers) to be remotely maintained and updated with new features and security patches.

B. Multi-Device and Multi-Source Support

- The architecture supports various interfaces for both video and access control devices, including the **Wiegand Interface** for traditional HID card readers and camera integration.
- The Access Control System is designed with **external camera integration** that provides **multiple photo views of visitors and live streaming video at the gate**, effectively merging video and access logs.
- The system supports remote user interaction via **Mobile App** (Android and iOS) and **Custom Web dashboards** (Member, Admin, Users), allowing multiple stakeholders to monitor security and video simultaneously.

3. AI Integration and Event Insights

AI processing is distributed between the edge and the cloud to generate actionable insights and enhance security measures.

A. AI on Edge for Real-Time Insights

- High-performance edge devices, such as the **Surveillance AI Camera** and **Edge AI Box** powered by the **Qualcomm QCS 6490 SOC (12 TOPS NPU)**, perform real-time processing directly at the source (**AI on Edge**).
- This local processing provides **AI-based event insights** immediately for applications like:
    - **Safety/Security: Intrusion detection, Gun Detection, Violence Detection**, and **Activity Tracking**.
    - **Road & Traffic Monitoring: License Plate Recognition, Overspeed Detection**, and **Red Light Violation Detection**.
- In access control, edge AI enables advanced security features like **2.5D face recognition** (using camera and Time-of-Flight sensors) for superior accuracy and **robust protection against spoofing attempts**.

B. Cloud Analytics for Searchable Metadata

- Events detected at the edge, or video streams sent to the cloud, are processed further using the **Event Detection Architecture on Cloud**.
- This workflow can integrate cloud services like **Amazon Rekognition Video** to **automatically identify objects, scenes, and activities**.
- This process generates **rich metadata** for detected labels, resulting in **Video with Event Annotations along Timeline**. This is crucial as it makes the content **searchable within a file and even across files**, providing actionable insights based on specific event types (e.g., "motion detection" or "loitering detection").

The system operates like a digital security fortress: The cameras and access controllers are the vigilant sentries (Edge AI), immediately recognizing threats and events locally. They communicate these vital alerts and video footage over robust protocols (MQTT/Cellular) to the central command center (Cloud VMS Portal), which acts as the unified, analytical dashboard, organizing all security streams and access logs for comprehensive remote management.