## Canopy Sight – Functional and Sensor Compatibility Report

### 1. Overview

- **Primary purpose**: Rail safety monitoring platform combining live video, AI detections, alerts, incidents, and analytics into a unified web dashboard backed by edge devices and a central API.
- **Architecture**: Next.js web frontend, Express+tRPC API, Prisma/PostgreSQL database with pgvector, edge agent for on-device processing, MeshConnect integration for resilient networking, and WebSocket channel for real-time events.
- **Deployment mode in this build**: Demo-first configuration with a demo admin login and full feature access, suitable for evaluations, demos, and pilots.

### 2. Core Functional Capabilities

- **Live Video Monitoring**
  - Single-camera focused live view per site.
  - Multi-camera grid live view per site.
  - Ability to select a specific device or camera to focus on.
  - Automatic camera focus selection driven by alerts that reference a specific device.
  - Zone overlays rendered on top of the video using configured polygons (crossing, approach, exclusion, custom).

- **Site Management**
  - Creation and management of monitoring sites with:
    - Name.
    - Description.
    - Address.
    - Latitude and longitude.
  - Association of devices to sites.
  - Association of zones, alerts, detection events, heatmaps, video clips, incident reports, and MeshConnect nodes to sites.

- **Device Management**
  - Device records with:
    - Name.
    - Site association.
    - Serial number.
    - Firmware version.
    - Status (online, offline, maintenance, error).
    - Last heartbeat timestamp.
    - IP address.
    - MAC address.
    - Device type (camera, meshconnect).
    - Organization association.
  - Device list with filters by site and status.
  - Device detail view including:
    - Site relationship.
    - Camera configurations.
    - Recent system health telemetry.
  - Device heartbeat endpoint to update:
    - Last heartbeat time.
    - Operational status.

- **Camera Configuration**
  - Multiple logical cameras per device through camera configuration records with:
    - Device association.
    - Camera index.
    - Camera name.
    - Resolution.
    - Frames per second.
    - Field-of-view mapping.
    - 360-degree camera flag.
    - Active flag.
  - Support for mapping detection zones to specific camera configurations.

- **MeshConnect Network Integration**
  - MeshConnect configuration per meshconnect-type device with:
    - Frequency band (1.35–1.44 GHz, 2.20–2.50 GHz, dual).

    - Throughput indication.
    - Latency indication.
    - Encryption enabled flag.
    - Encryption key placeholder.
    - Mesh node identifier.
    - Parent node identifier.
    - Network topology (neighbor graph).
    - Wi-Fi enabled flag.
    - Wi-Fi SSID.
    - Wi-Fi password placeholder.
    - Number of Ethernet ports.
    - Gateway flag.
    - Gateway address.
    - Node status (connected, disconnected, syncing, error).
    - Last sync time.
    - Signal strength.
    - Neighbor node list.
  - Mesh topology visualization per site showing node relationships and status.

- **Detection Events**
  - Recording of AI detection events with:
    - Device association.
    - Site association.
    - Object type (person, vehicle, animal, unknown, additional types as configured).
    - Confidence score.
    - Timestamp.
    - Bounding box coordinates.
    - Associated zone identifiers.
    - Optional risk score association.
    - Optional video clip association.
    - Embedding vector for similarity and search.
    - Metadata payload.
    - Organization association.
  - Query endpoints with support for:
    - Time ranges using date coercion.
    - Limit and pagination constraints.
    - Filtering by site and other parameters.

- **Risk Scoring**
  - Separate risk score records attached to detection events with:
    - Overall risk score.
    - Speed factor.
    - Direction factor.
    - Dwell time factor.
    - Zone factor.
    - Time-of-day factor.
    - Metadata payload.

- **Alerting**
  - Alert records with:
    - Detection event association.
    - Site association.
    - Device association.
    - Severity (advisory, warning, critical).
    - Status (active, acknowledged, resolved, dismissed).
    - Title.
    - Message.
    - Acknowledged-by identifier.
    - Acknowledged time.
    - Resolved time.
    - Metadata payload.
    - Organization association.
  - WebSocket-driven live alert feed with:
    - Real-time push of new alerts.
    - Severity-dependent visual styling.
    - Animated appearance and removal.
    - Time display using local time zone.
  - Integration with live views:
    - Ability to auto-focus site live view on a camera matching the alert’s device.

- **Incident Reporting**
  - Manual incident report records with:
    - Site association.
    - Title.
    - Description.
    - Severity (low, medium, high, critical).
    - Reported-by identifier.
    - Reported-at timestamp.
    - Resolved-at timestamp.
    - Metadata payload.
    - Organization association.
  - Incidents page for:
    - Listing incidents.
    - Viewing details.
    - Marking incidents resolved.

- **Video Clip Management**
  - Video clip metadata with:
    - Detection event association.
    - Device association.
    - Site association.
    - File path or storage path.
    - Thumbnail path.
    - Duration.
    - Start time.
    - End time.
    - File size.
    - MIME type.
    - Organization association.
  - Playback page for:
    - Browsing available clips.
    - Requesting playback for selected intervals and incidents.

- **Analytics and Heatmaps**
  - Aggregated heatmap records with:
    - Site association.
    - Start date.
    - End date.
    - Heatmap data with spatial and temporal information.
    - Resolution.
    - Organization association.
  - Analytics pages for:
    - Time-range based analysis of detections and alerts.
    - Heatmap visualizations of activity concentration.
    - Behavioral pattern analysis using AI services.

- **System Health and Telemetry**
  - System health records per device with:
    - Device association.
    - Organization association.
    - CPU usage.
    - Memory usage.
    - Disk usage.
    - Temperature.
    - Uptime.
    - Network latency.
    - Metadata payload.
    - Timestamp.
  - Device detail views include a summary of recent health telemetry.

- **Notification Routing Rules**
  - Notification preferences per organization or per user with:
    - Channel (SMS, email, push, webhook).
    - Severity filter (advisory, warning, critical, all).
    - Site filters (subset of sites, or all sites).
    - Active flag.
    - Channel-specific configuration payload.
    - Organization association.

```
    - Optional user association.
  - tRPC procedures for:
    - Listing notification preferences.
    - Creating notification rules.
    - Updating notification rules.
    - Deleting notification rules.

- **Settings and Preferences**
  - Settings hub page linking to:
    - Notifications settings.
    - System configuration settings.
    - User preferences.
    - API keys and integrations information.
    - Data retention preferences.
    - Export and backup settings.
  - System configuration page with:
    - Default live view layout control (auto, single, multi).
    - Auto-focus-on-alerts toggle.
    - Play-sound-on-critical toggle for future audible alerts.
    - WebSocket auto-connect toggle.
    - Local persistence in the browser using `localStorage`.
  - User preferences page with:
    - Default landing page selection (dashboard, sites, alerts, incidents, analytics).
    - Compact mode toggle for denser layouts.
    - Reduce-motion toggle for reduced animations.
    - Local persistence in the browser using `localStorage`.
  - Data retention settings page with:
    - Detection and analytics data retention days.
    - Video clip retention days.
    - Keep-critical-incidents-forever toggle.
    - Local persistence using `localStorage` as policy values for the demo.
  - Export and backup page with:
    - Simulated CSV export triggers for incidents, alerts, and detections.
    - Operational guidance for backup and restore in production.
  - API keys and integrations page with:
    - Explanation that secrets are managed in environment variables and secret managers.
    - High-level categories of keys (authentication, database, AI, maps, external integrations).

- **Audit and Compliance**
  - Audit log records with:
    - Organization association.
    - User identifier.
    - Action (create, update, delete, view).
    - Resource type (site, device, zone, detection, alert, incident, and additional resources).
    - Resource identifier.
    - Changes payload.
    - IP address.
    - User agent.
    - Created-at timestamp.
  - Intended downstream use for compliance and traceability.

- **Connectivity and Networking**
  - Ngrok tunnel configuration for:
    - Exposing web UI.
    - Proxying API requests through the web host.
  - CORS and security headers configured to:
    - Permit development use over localhost.
    - Permit requests from configured ngrok domains.
    - Support demo headers for development authentication.
  - WebSocket configuration with:
    - CORS origin checks matching HTTP rules.
    - Safe behavior when WebSocket is not reachable over ngrok.

### 3. Camera Compatibility

- **Supported Camera Types by Integration Method**
  - IP cameras that can publish streams in an HLS format with an `.m3u8` URL.
  - Cameras connected to an edge device that repackages RTSP or ONVIF streams into HLS or WebRTC
streams.
```

  - WebRTC-capable cameras that expose a browser-compatible media endpoint through a signaling and gateway layer.
  - Locally attached cameras connected to the edge agent that can be encoded into a network stream for the web app.

- **Supported Protocols and Encapsulation**
  - HTTP(S) served HLS streams identified by `.m3u8` URLs.
  - HTTP(S) served video files or segments suitable for `<video>` playback.
  - WebRTC media streams accessible through the browser when a signaling server and gateway are available.

- **Multi-Camera and Multi-View Support**
  - Multiple logical camera configurations per physical device.
  - Multiple devices and cameras per site.
  - Site-level multi-view grid layout with one tile per device or camera.
  - Focused camera view with manual selection and alert-driven selection.

- **Camera Metadata and Control Capabilities**
  - Per-camera metadata:
    - Resolution.
    - Frame rate.
    - Field-of-view mapping.
    - 360-degree camera support flag.
    - Active or inactive state.
  - Association of detection zones with camera views for:
    - Crossings.
    - Approaches.
    - Exclusion zones.
    - Custom safety regions.

### 4. Sensor and Signal Compatibility

- **Video-Based Sensors and Analytics**
  - Person detection.
  - Vehicle detection.
  - Animal detection.
  - Object type classification for additional categories configured in the AI pipeline.
  - Zone-based intrusion and approach detection.
  - Risk scoring signals including:
    - Speed factor.
    - Direction factor.
    - Dwell time factor.
    - Zone factor.
    - Time-of-day factor.

- **Non-Video Sensors (Normalized via Events and Alerts)**
  - Track occupancy sensors normalized into detection events and alerts.
  - Perimeter intrusion sensors normalized into detection events and alerts.
  - Vibration sensors normalized into detection events and alerts.
  - Environmental sensors normalized into detection events and alerts.
  - Radar units normalized into detection events and alerts.
  - LiDAR units normalized into detection events and alerts.
  - Any sensor or device capable of sending data through the edge agent or API that is mapped into:
    - Detection events.
    - Risk scores.
    - Alerts.
    - System health records.

- **MeshConnect Network Sensors**
  - Mesh node connection state (connected, disconnected, syncing, error).
  - Signal strength and link quality indicators.
  - Neighbor node relationships and topology graph.
  - Node throughput measurements.
  - Node latency measurements.
  - Wi-Fi and Ethernet bridge configuration values.

- **System Health and Device Telemetry Sensors**
  - CPU usage monitoring.

- Memory usage monitoring.
- Disk usage monitoring.
- Device temperature monitoring.
- Device uptime monitoring.
- Network latency monitoring.

### 5. Authentication, Authorization, and Demo Mode

- **Demo Authentication**
  - Demo login flow granting a demo admin role with full access.
  - Demo mode flags stored in browser storage and cookies.
  - tRPC context that:
    - Ensures a demo organization record.
    - Ensures a demo user record.
    - Ensures the demo user has an admin role.

- **Access Control Model**
  - Organization-scoped data segregation across:
    - Sites.
    - Devices.
    - Detection events.
    - Alerts.
    - Incidents.
    - Video clips.
    - Heatmaps.
    - Notification preferences.
    - System health.
    - Audit logs.
  - Role model with:
    - Admin role.
    - Supervisor role.
    - Viewer role.
  - Protected procedures using a shared context enforcing organization and role checks.

### 6. Export, Backup, and Retention

- **Data Export**
  - User-initiated export actions for:
    - Incident lists.
    - Alert lists.
    - Detection lists.
  - Export workflow in the demo environment:
    - Simulated CSV generation.
    - User feedback through toast notifications.

- **Data Retention**
  - Policy values for:
    - Detection and analytics data retention in days.
    - Video clip retention in days.
    - Critical incident permanent retention.
  - Intended enforcement using:
    - Database retention policies.
    - Object storage lifecycle rules.

- **Backup Strategy Guidance**
  - Full database backup recommendations.
  - Object storage versioning and retention configuration.
  - Regular restore testing recommendations.

### 7. Extensibility and Integration Points

- **Edge Agent Integration**
  - Designed to run on embedded or industrial computers.
  - Interfaces with:
    - Cameras.
    - Sensor buses.
    - Local storage.
    - Central API.
  - Capable of:

    - Running AI inference.
    - Streaming local video.
    - Pushing detections and telemetry upstream.

- **API and tRPC Layer**
  - Strongly typed endpoints for:
    - Sites.
    - Devices.
    - Zones.
    - Detection events.
    - Alerts.
    - Incidents.
    - Heatmaps.
    - Notification preferences.
    - System health.
  - Shared validator schemas for input validation and type safety.

- **AI and Analytics Services**
  - Integration hooks for:
    - Natural language incident analysis.
    - Advanced analytics and reporting.
    - Vector search over detection embeddings.
  - Support for:
    - External AI providers configured through environment variables.

### 8. Summary

- Canopy Sight provides a comprehensive foundation for:
  - Live monitoring of multiple cameras and sites.
  - AI-driven detection, alerting, and incident management.
  - Telemetry, analytics, and heatmap visualization.
  - Notification routing, policy configuration, and export workflows.
- The platform is **camera-agnostic and sensor-agnostic** at the protocol and data model level and is designed to ingest any video stream or sensor signal that can be:
  - Encapsulated into supported streaming formats for video.
  - Normalized into detection events, alerts, incidents, or telemetry records for sensors and devices.