Codfinitt

Intelligent Operations Platform

Reference No.	PV-P9025201
Document Type	Project Overview
Version	0.3
Date	07-Sep-2025

1. Introduction

1.1. Purpose

This document provides a comprehensive overview of our evolving Intelligent Operations Platform (IOP). It outlines the current system (AISSS), our strategic roadmap, system goals, data architecture, key UI modules, and proposed enhancements to transition into a full-scale industrial intelligence infrastructure.

Modern industrial environments generate vast volumes of data every second – ranging from telemetry and video to sensor and machine logs. While much of this data is currently used for specific, siloed purposes, it holds a potential to deliver cross-functional intelligence. To make this data actionable in real time, IOP brings advanced AI-powered analytics directly to the edge, processing data where it is created, minimising latency, and enabling autonomous decisions in mission-critical environments.

By transforming raw operational signals into actionable insights, the platform drives measurable efficiency across industrial domains – whether fine-tuning manufacturing lines, streamlining quality control, optimising logistics, or enhancing site surveillance through drones and computer vision.

1.2. Scope

The Intelligent Operations Platform supports real-time monitoring, rule-based event detection, and incident management workflows across diverse sectors such as construction, manufacturing, transportation, logistics, and energy.

What began as a computer vision-based AI Site Safety System (AISSS) is evolving into a modular, multi-tenant platform capable of:

- Integrating multimodal sensors (video, telemetry, RFID, GPS, vibration, etc.)
- Performing AI-driven analysis at the edge with minimal infrastructure
- Scaling across geographically distributed or remote sites with limited connectivity
- Synchronising data to the cloud using resilient satellite uplinks or intermittent backhaul
- Offering predictive analytics, trend forecasting, and performance optimisation
- Providing unified control interfaces and dashboards for operational orchestration

2. Current System Overview – AISSS

2.1. Core Features

- Real-time AI inference on video streams (e.g., PPE, zone breaches)
- Redis Streams and RabbitMQ for messaging
- GStreamer for video processing
- .NET microservices deployed via Docker
- Edge-focused architecture with recording, rule engine, and notification modules

2.2. Deployment Status

- Modular microservices architecture
- Edge-capable but software-centric
- No hardware orchestration layer yet

3. Platform Goals

3.1. Intelligent Infrastructure Platform Vision

We aim to evolve the current system into a robust AI Infrastructure for Industrial Intelligence, capable of:

- Multimodal sensor ingestion (beyond video)
- Predictive and generative analytics
- Industry-agnostic safety, monitoring, and reporting
- Deployment on edge devices, centralised cloud, or hybrid setups

4. Proposed System Enhancements

4.1. Strengthen AI Capabilities

- Add predictive models (e.g., incident likelihood)
- Generate automated reports (e.g., daily safety summaries)
- Fuse sensor + video + logs for smarter evaluation

4.2. Support Cross-Industry Use Cases

- Extend to manufacturing, logistics, oil & gas, education, etc.
- Add modules for:
    - Fall detection, Intrusion detection etc.
    - Chemical hazard monitoring, Equipment behaviour analysis etc.

5. Architectural Upgrades

5.1. Device & Asset Management

Transition from camera-centric design to a Device and Asset Management layer to support:

- GPS, temperature, gas, sound, RFID, vibration sensors
- Device grouping by Units and Sites
- Rule configuration by asset type

This enables:

- Smooth upgrade path
- Breaking camera-only dependency
- Full IoT ecosystem integration

5.2. Multimodal AI & Ingestion

- Input Expansion
  - Add MQTT/REST for real-time ingestion
  - Timestamped, location-tagged data
  - Unified internal representation
- Model Expansion
  - Vision models (CV), anomaly detectors, time-series models
  - Composite rule evaluation using multiple sensor types

6. Data Model Redesign

6.1. Sites

- Represents a geographical or logical location (e.g., plant, campus).
- A tenant/organisation can have multiple sites at different geographic locations.
- Reference:

Field	Type	Description
site_id	UUID	Unique identifier
name	String	Human-friendly site name (e.g., “Greenfield High Campus”, “Plant 3”)
description	String	e.g., “East coast site”
type	Enum	(Campus, Plant, Depot, Zone, Region, etc.)
address	String	
timezone	Enum	e.g., “Asia/Kolkata”
location	GeoPoint or JSON	Optional GPS location or bounding polygon
status	Enum	(Active, Inactive, Maintenance etc.)

metadata	JSON	Additional configuration, map overlays, owner info, etc.
created_at	Timestamp	

6.2. Units

- Equivalent of Zones in AISSS.
- One Site can have many Units.
- Represents a logical grouping of assets/devices within a site - can be a bus, machine, drone, packaging line, etc.
- Unit type drives routing, analytics logic
- Reference:

Field	Type	Description
unit_id	UUID	Unique identifier
site_id	UUID	Foreign key to Site
name	String	Human-friendly unit name (e.g., "Bus 3", "Line A", "Drone-Delta")
description	String	e.g., "Entry restricted to authorised personnel"
type	Enum	(Vehicle, Drone, Packaging Line, Warehouse, etc.)
location	JSON	Latitude, Longitude, Altitude etc.
status	Enum	(Active, Inactive, Maintenance etc.)
metadata	JSON	Specs, capacity, operator, image, routing info, etc.
parent_unit_id	UUID (nullable)	For hierarchical grouping, e.g., Arm A under Robot 1
created_at	Timestamp	

6.3. Assets

- Equivalent of Devices in AISSS.
- One Unit can have many Assets.
- Represents a control point or telemetry source (e.g., camera, thermal sensor, GPS, RFID reader etc.).
- Reference:

Field	Type	Description
asset_id	UUID	Unique identifier
unit_id	UUID	Foreign key to Unit
name	String	e.g., "GPS Tracker", "IR Camera", "Temp Sensor 3"
type	Enum	(GPS, RFID, PLC, Camera, UWB, TempSensor, etc.)
status	Enum	(Active, Inactive etc.)
manufacturer	String	Optional
model	String	Optional

tags	Array of String	e.g., ["temperature", "critical", "production"]
location_offset	JSON	e.g., position within unit or relative to mount
config	JSON	Sample rate, thresholds, stream topic names, etc.
created_at	Timestamp	

6.4. Telemetry

- Raw, continuous measurements flowing in from assets (camera frames, sensor readings, audio snippets, model inference outputs etc.)
- Reference:

Field	Type	Description
telemetry_id	UUID	Unique ID
asset_id	UUID	Source asset
modality	Enum	e.g., "Video"
timestamp	Timestamp	Data capture time
payload	JSON	Dynamic sensor values (temp, RPM, voltage, etc.)
ingested_at	Timestamp	When the system received it

6.5. Events

- A redesign of Incidents layer in AISSS.
- Distilled, atomic signals generated when a predefined rule or threshold is violated (e.g., "Speed limit exceeded", "RFID not detected", "High temperature detected").
- Acts as a triggering layer that captures the system's intelligence and provides visibility into what's happening in the field.
- Represent raw, real-time rule violations.
- Generated in high volume and at high frequency.
- Used primarily for monitoring and analytics.
- Every Event is a potential Incident, but not every Event becomes an Incident.

6.6. Incidents

- A new layer split from Incidents in AISSS.
- Workflow-managed representation of one or more related events that require attention, escalation, resolution, or documentation.
- May aggregate multiple related Events into a single trackable case (e.g., repeated temperature violations across a time window).
- Created manually or automatically based on the severity, frequency, or aggregation of Events.

- Integrated into audit, reporting, and alerting workflows.
- Reference:

Field	Type	Description
incident_id	UUID	Unique identifier
event_ids	Array of UUID	One or more events constituting an incident
name	String	Human-friendly incident name
description	String	Summary of the incident either entered by a user (during manual creation) or AI generated (in automatic creation)
evidence	JSON	Metadata containing violation values, snapshot_uri, filename, etc.
status	Enum	(Open, Acknowledged, Closed etc.)
created_at	Timestamp	

6.7. Incident Policies in Safety Rules

- Defines escalation logic.
- Example policy:

  If Noise > 95dB persists > 5 mins → Trigger 1 incident, not 20 alerts

6.8. Incident Status

- Tracks incident lifecycle.
- Status transitions (e.g., OPEN → ACKNOWLEDGED)
- Comments and timestamps
- Assigned users

7. Core UI Modules

7.1. Dashboard

Purpose: High-level snapshot of system health and key metrics, and operational alerts, with role-based customised widgets.

Features:

a. Global health map
   - Visualize Sites on a map with real-time status indicators.
   - Unit clusters with asset markers.

b. System overview
   - Uptime summaries, last check-in timestamps across all sites and units.

- Achieved operational efficiency
- Connected assets summary – Cards showing total assets, categorized by type and operational status.
- Active alerts / failures – Cards showing active alerts, categorized by severity.

7.2. Monitoring

Purpose: Real-time monitoring and historical event tracking.

Features:

a. Insights
   - System-generated suggestions based on analytics (e.g., "Redundant unit detected").
   - List view with filters by date, asset type, severity.
   - Modal for detailed view and historical context.

b. Event Feed
   - Real-time stream of Events (e.g., "Temperature Threshold Exceeded").
   - Click-to-expand modal for root cause and associated rules.

c. Incidents
   - List of all Incidents triggered by rules or escalated by users.
   - Modal with extended details like full timeline, status, related asset info.
   - Actions: Acknowledge, Comment, Reassign, Escalate.

d. Notification Logs
   - Log of all system-dispatched alerts (SMS, Email, In-App).
   - Filter by channel, user group, and status.

e. Playback
   - Timeline-based video retrieval (for camera assets).
   - Playback controls, annotations, tagging incidents.

7.3. Asset Registry

Purpose: Manage all IoT assets like cameras, sensors, audio devices, Starlink, drones etc.

Features:

a. Assets
   - List View: Table with asset metadata (type, status, serial ID), with filtering/sorting.
   - Details View: Modal with extended information of the Asset.
   - Create / Modify: Modal form with validations and field-specific help.

b. Units
    - List View: Grouping of assets, with filtering/sorting.
    - Details View: Modal with extended information of the Unit.
    - Create / Modify: Modal form with validations and field-specific help.

c. Health Monitoring
    - Show last heartbeat, signal strength, disconnection logs.

d. Maintenance
    - Display scheduled maintenance, service history, and upcoming updates.

7.4. Sites

Purpose: Manage tenant sites and associated units.

Features:

a. Sites
    - List View: All registered sites, with filtering/sorting.
    - Details View: Modal with extended information of the Site.
    - Create / Modify: Modal form with validations and field-specific help.

7.5. Operations

Purpose: Define and manage analytics for insight, and safety rules that trigger events and alerts.

Features:

a. Analytics
    - List View: All defined analytics rules with filtering.
    - Details View: Modal with metric types, logic description, and execution plan.
    - Create New: Multi-step wizard to configure data source and logic.
    - Modify / Clone: Allow editing and re-use of templates.

b. Rules
    - List View: All active rules triggering events/incidents.
    - Details View: Modal with violation conditions, incident policy.
    - Create New: Multi-step wizard to configure data source, violation criteria, and action.
    - Modify / Clone: Editing and/or converting to Analytics workflows if needed.

7.6. Users & Access Control

Purpose: Role-based access control and user management and grouping.

Features:

a. Users
   - List all users with site access info and last login.
   - View and edit roles, contact info, group membership.

b. Roles
   - Manage role definitions for menu access, site-level visibility, and app-specific controls.

c. Groups
   - Group users for collective actions like broadcast notifications.

d. Accessibility
   - List of app functionalities or privileges

7.7. Network & Connectivity

Purpose: Manage network connectivity.

Features:

a. Network Statistics
   - Latency Trends: Min/Avg/Max over time.
   - Packet Loss Heatmap: Highlight problem (high-loss) zones.
   - Bandwidth Graphs: Per site/unit/app.
   - Jitter Monitoring: Important for real-time video streams.

b. Data Usage
   - Breakdown by Fixed vs Mobile: Monthly / Real-time Data Usage.
   - Burst Plan Utilization: Visuals and thresholds (e.g., mobile data caps).
   - Quota Alerts: e.g., Notify at 80% quota.
   - Forecasts: Predict future consumption using trends.

c. Diagnostics
   - On-demand Ping / Traceroute.
   - DNS checks, endpoint reachability.
   - Optional: Edge mesh connectivity map.

d. Offline Mode
   - Queue Monitor: Track un-synced data.
   - Offline Duration Tracker: Show impact window.

7.8. Reports & Analytics

Purpose: Generate business insights, and KPIs.

Report types:

a. Safety Trends: Violation types, frequency by site/asset.
b. Operational KPIs: Downtime, utilization, response times.
c. Scheduled Reports: Email reports with templated filters.
d. Export Options: PDF, CSV
e. Filters: Site, asset, time range, unit type.

7.9. Apps

Purpose: Interface to access add-on applications.

Features:

a. Grid/List view of all installed or subscribed apps.
b. Launch apps inside iframe sandbox.
c. View app version, last updated date.

7.10. Marketplace

Purpose: To let tenants subscribe to AI models, analytics packs, or advanced rule sets.

Features:

a. Browse AI Models (e.g., Fire Detection, PPE Detection, Anomaly Detection) and Business Apps by domain (e.g., Safety, Energy, Logistics).
b. Pricing models, feature sets, and usage limits.
c. Subscription & Billing status.

7.11. System Configuration

Purpose: Manage platform-level settings.

Features:

a. Global Policies: Timezone, units, naming rules.
b. Notification Settings: Default channels, retry policies.
c. Usage Quota Alerts
d. Update Intervals: Data sync, firmware checks.
e. Firmware & Software: Upload packages, view update logs.
f. Offline Sync Settings: Admin config only (for network fallback behaviour).

8. Technology Stack Overview

Frontend	Angular (Web), Flutter (Mobile)
Backend	.NET (C#), Python, C++, gRPC, REST

Data Store	Postgres, Redis
Message Queue	RabbitMQ, Redis Streams
Real-time Engine	SignalR/WebSockets
AI Models	PyTorch / ONNX (deployed via Triton etc.)
Deployment	Docker, Kubernetes, Edge-ready
Sensor Ingestion	MQTT, REST, WebSockets
IoT Integration	GPS, RFID, MQTT
Notification System	Firebase, Azure Hub
Cloud Sync	AWS S3, Azure Blob, Starlink fallback

9. Security & Data Integrity

To ensure secure and trustworthy operations across critical environments, the platform implements the following practices.

- TLS encryption for all data in transit between services and clients.
- Role-Based Access Control (RBAC) to enforce granular permission boundaries.
- Secure token-based authentication (JWT) for all API access.
- Signed system logs for non-repudiable auditing of critical actions.
- Insert-only audit tables to ensure immutable and traceable changes across key entities.
- Encrypted credentials and secrets, managed via a secure vault service.

10. Scalability & Performance

The platform is engineered for high-throughput, low-latency processing at scale.

- Modular microservice architecture allows for independent scaling and fault isolation.
- Redis-based real-time buffering and stream processing enables sub-second telemetry handling.
- Support for multi-tenancy across institutions (e.g., schools, municipalities, manufacturing sites) with isolation and logical partitioning.
- Horizontal scalability for cloud and edge deployments, including containerised workloads and Kubernetes orchestration.
- Robust data sync layer with auto-retry, backpressure handling, and fallback queuing for intermittent connectivity at the edge.

11. Appendix

11.1. Sample: Industry-Wise Data Mapping

Industry	Site	Unit	Assets
School Transportation	Springfield School	Bus 3	GPS, RFID, Camera
Logistics	Depot B	Vehicle 12	GPS, Load Sensor, Camera
Manufacturing	Plant A	Packaging Line A	PLC, Camera, Sensor, Reject Counter
Oil & Gas	Refinery Site X	Pump Cluster 4	Valve sensor, UWB tag, PLC
Surveillance	Mining Zone Delta	Drone Alpha	RGB Camera, Thermal Imager, IR Sensor, GPS