



TÀI LIỆU KỸ THUẬT
PHẦN MỀM NỀN TẢNG
AN NINH VẬT LÝ TÍCH HỢP
GSAFE-C3-PSIM

A. GIỚI THIỆU

I. THÔNG TIN CHUNG

Phần mềm Nền tảng An ninh vật lý tích hợp GSAFE-C3-PSIM là giải pháp phần mềm toàn diện “All-in-one” do CÔNG TY TNHH CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG GTEL (GTEL ICT) và CÔNG TY CỔ PHẦN GIẢI PHÁP CÔNG NGHỆ TRỰC TUYẾN GTEL (GTEL OTS) (*Tiền thân là CÔNG TY TNHH GIẢI PHÁP CÔNG NGHỆ TRỰC TUYẾN*) nghiên cứu, thiết kế, sản xuất và đồng sở hữu nhằm tối ưu hóa việc giám sát, điều hành và quản trị an ninh cho các cơ sở hạ tầng trọng yếu và tổ chức có yêu cầu bảo mật cao. Nền tảng tích hợp đồng bộ các hệ thống an ninh vật lý đa dạng như camera giám sát, kiểm soát truy cập, hệ thống báo cháy, phân tích video thông minh và cảm biến IoT, tạo thành một hệ sinh thái liên kết chặt chẽ, vận hành tập trung và hiệu quả.

Mục đích

Giải pháp được xây dựng nhằm cung cấp khả năng quản lý an ninh toàn diện, tăng cường phát hiện và cảnh báo sớm các nguy cơ, hỗ trợ điều phối và chỉ huy vận hành linh hoạt, đồng thời tối ưu hóa chi phí và nguồn lực cho doanh nghiệp và tổ chức. Mục tiêu chiến lược là hỗ trợ các đơn vị chuyển đổi số trong lĩnh vực an ninh vật lý, nâng cao năng lực quản lý, giảm thiểu rủi ro và đảm bảo vận hành liên tục trong môi trường phức tạp và đa chiều.

Phạm vi ứng dụng

- ♦ Giám sát và bảo vệ các địa điểm quan trọng.
- ♦ Điều hành, phối hợp và cảnh báo sớm các tình huống bất thường.
- ♦ Quản trị tài sản, nhân lực và năng lượng hiệu quả.
- ♦ Vận hành thông minh trong các mô hình đô thị thông minh, tòa nhà, khu công nghiệp...khác.

A. GIỚI THIỆU

II. ĐỐI TƯỢNG SỬ DỤNG

Giải pháp được thiết kế nhằm đáp ứng nhu cầu của các tổ chức và doanh nghiệp có yêu cầu cao về an ninh, quản lý tập trung và phản ứng nhanh trong môi trường phức tạp:

- ♦ **Cơ sở hạ tầng quan trọng quốc gia:** Trung tâm dữ liệu, hệ thống điện lực, viễn thông, cấp nước, giao thông vận tải.
- ♦ **Tổ hợp công nghiệp – sản xuất:** KCN quy mô lớn, nhà máy công nghệ cao, hệ thống logistics đa điểm.
- ♦ **Bất động sản thông minh – thương mại:** Tòa nhà văn phòng, khu dân cư cao cấp, trung tâm thương mại, khách sạn – resort.
- ♦ **Khối chính phủ – quốc phòng – doanh nghiệp lớn:** Trụ sở cơ quan, doanh nghiệp đa quốc gia, lực lượng tác chiến an ninh và PCCC.
- ♦ **Đơn vị quản lý đô thị và đơn vị vận hành hạ tầng kỹ thuật:** Ban quản lý đô thị thông minh, trung tâm điều hành giao thông.
- ♦ Dành cho mọi cấp độ ứng dụng – từ cá nhân, tổ chức, doanh nghiệp, chính quyền địa phương đến cấp quốc gia có nhu cầu cấp thiết trong việc tích hợp, vận hành và quản lý hiệu quả các hệ thống an ninh vật lý đa dạng trong một nền tảng thống nhất mang lại hiệu quả và linh hoạt.

A. GIỚI THIỆU

III. LỢI ÍCH CHUNG

- ♦ **Nâng tầm An ninh Toàn diện:** Giám sát tập trung 24/7, phát hiện sớm và cảnh báo tức thời mọi mối đe dọa.
- ♦ **Tối ưu hóa Vận hành & Chi phí:** Tự động hóa quy trình nghiệp vụ, giảm thiểu nhân lực vận hành trực tiếp, tiết kiệm chi phí quản lý và bảo trì.
- ♦ **Phản ứng Tức thời & Hiệu quả:** Cho phép chỉ huy, điều phối lực lượng an ninh và các hệ thống phản ứng một cách nhanh chóng, đồng bộ khi có sự cố.
- ♦ **Quyết định Chính xác dựa trên Dữ liệu:** Cung cấp thông tin, phân tích và báo cáo trực quan, hỗ trợ lãnh đạo ra quyết định kịp thời và chính xác.
- ♦ **Vận hành liên tục & Chỉ huy Điều hành:** Kết nối chặt chẽ các lực lượng và hệ thống, đảm bảo thông tin liên lạc và phối hợp tác chiến hiệu quả.
- ♦ **Mở rộng Linh hoạt:** Kiến trúc microservices cho phép dễ dàng mở rộng, nâng cấp và tích hợp thêm các hệ thống mới theo nhu cầu phát triển.

A. GIỚI THIỆU

IV. ĐẶC ĐIỂM NỔI BẬT

- ♦ **Kiến trúc Zero Trust & bảo mật đa lớp:** Tuân thủ chuẩn an ninh quốc tế (TLS 1.3, OAuth2, JWT), phân tầng dữ liệu theo vai trò và vùng rủi ro, kết hợp kiểm soát truy cập theo bối cảnh.
- ♦ **Nền tảng hợp nhất – All-in-One:** Một hệ thống duy nhất tích hợp điều hành an ninh, vận hành và phân tích dữ liệu, hỗ trợ triển khai nhanh, vận hành ổn định và dễ mở rộng.
- ♦ **Tích hợp công nghệ tiên tiến:** Hỗ trợ đa chuẩn công nghiệp (ONVIF, OPC UA, BACnet, REST API...), kết nối liền mạch với các hệ thống hiện có. Tích hợp các năng lực AI, ML, Video Analytics, Edge Computing và nền tảng đám mây (Hybrid Cloud).
- ♦ **Khả năng tùy biến chuyên sâu:** Cho phép xây dựng các “adapter” tương thích với hạ tầng và quy trình hiện hữu của từng tổ chức, đảm bảo tính tương thích – mở rộng mà không phá vỡ cấu trúc lõi.
- ♦ **Chiến lược dữ liệu trung tâm:** Thiết kế xoay quanh dữ liệu, hướng tới xây dựng năng lực phân tích chuyên sâu, khai thác dữ liệu làm nguồn lực chiến lược cho vận hành và ra quyết định.

B. CÁC PHÂN HỆ VÀ TÍNH NĂNG CHÍNH

Nền tảng Tích hợp hệ thống An ninh vật lý bao gồm các phân hệ và khối tính năng lõi như sau

I. NỀN TẢNG LIÊN THÔNG TÍCH HỢP THÔNG MINH

- ◆ Nền tảng liên thông tích hợp là sự kết hợp của nhiều công nghệ và công cụ tiên tiến, tạo ra một nền tảng kết nối duy nhất giúp các hệ thống an ninh khác nhau có thể liên kết, phối hợp hoạt động hiệu quả và bảo mật. Nền tảng này đóng vai trò là trung tâm tích hợp toàn diện cho tất cả các hệ thống an ninh vật lý, đảm bảo tính đồng bộ, tuân thủ quy chuẩn và tập trung mọi cảnh báo an ninh về Trung tâm An ninh vật lý tích hợp để quản lý và xử lý. Đáp ứng các yêu cầu tính năng, công nghệ.

a. Công nghệ nền tảng

STT	Chuẩn tích hợp	Mô tả
1	Microservices Architecture	Kiến trúc dịch vụ nhỏ, độc lập giúp mở rộng dễ dàng và linh hoạt trong tích hợp
2	Middleware & Message Broker	Các hệ thống trung gian như MQTT, Kafka, RabbitMQ để đảm bảo truyền dữ liệu theo thời gian thực giữa các hệ thống
3	API Gateway	Cung cấp một lớp giao tiếp tiêu chuẩn giữa hệ thống bên ngoài và các dịch vụ nội bộ
4	Database đa tầng	Kết hợp SQL (PostgreSQL, MySQL) và NoSQL (MongoDB, Elasticsearch) để lưu trữ dữ liệu có cấu trúc và phi cấu trúc

B. CÁC PHÂN HỆ VÀ TÍNH NĂNG CHÍNH

STT	Chuẩn tích hợp	Mô tả
5	AI & Machine Learning	Kiến trúc dịch vụ nhỏ, độc lập giúp mở rộng dễ dàng và linh hoạt trong tích hợp
6	Cloud & Edge Computing	Hỗ trợ triển khai On-premise, Hybrid Cloud và Edge Computing để xử lý dữ liệu nhanh chóng và giảm tải mạng.

b. Tiêu chuẩn tích hợp

STT	Chuẩn tích hợp	Mô tả
1	Giao tiếp IoT	Hỗ trợ các chuẩn như MQTT, CoAP, OPC-UA để kết nối với cảm biến, thiết bị IoT
2	Giao tiếp API	Sử dụng RESTful API, GraphQL, gRPC để kết nối với các ứng dụng phần mềm
3	Chuẩn Video & Giám sát	Hỗ trợ các giao thức như ONVIF, RTSP, WebRTC để tích hợp hệ thống camera giám sát
4	Chuẩn bảo mật & xác thực	+ OAuth2, OpenID Connect: Xác thực người dùng + TLS/SSL: Mã hóa dữ liệu + Zero Trust Architecture: Đảm bảo an toàn thông tin khi giao tiếp giữa các hệ thống

B. CÁC PHÂN HỆ VÀ TÍNH NĂNG CHÍNH

STT	Chuẩn tích hợp	Mô tả
5	Hỗ trợ đầy đủ các chuẩn tích hợp phổ biến, phục vụ kết nối với nhiều hệ thống khác nhau	+ ONVIF (Open Network Video Interface Forum) + OSDP (Open Supervised Device Protocol) + REST API (Representational State Transfer API) + SOAP (Simple Object Access Protocol) + OPC UA (Open Platform Communications Unified Architecture) + SDK (Software Development Kit) + Giao thức Access Control (Kiểm soát truy cập). + Tích hợp ALPR (Automatic License Plate Recognition). + Tích hợp BMS (Building Management System). + MQTT (Message Queuing Telemetry Transport) + BACnet (Building Automation and Control Networks) + Modbus + SNMP (Simple Network Management Protocol) + LDAP (Lightweight Directory Access Protocol) + SAML (Security Assertion Markup Language) + OAuth 2.0 / OpenID Connect + TLS/SSL (Transport Layer Security / Secure Sockets Layer) + Zigbee/Z-Wave + LoRaWAN (Long Range Wide Area Network) + WebSocket + IPv6 / IPv4

B. CÁC PHẦN HỆ VÀ TÍNH NĂNG CHÍNH

STT	Chuẩn tích hợp	Mô tả
		+ Tích hợp PCCC (Fire Alarm Integration) + Tích hợp SCADA (Supervisory Control and Data Acquisition) + Tích hợp AI Video Analytics + Blockchain trong An Ninh

II. HỆ THỐNG PHẦN MỀM TRUNG TÂM AN NINH TẬP TRUNG

a. Trung tâm An ninh Vật lý

- ♦ Giám sát An ninh Tập trung 24/7: Quản lý và giám sát đa mục tiêu từ xa, liên tục và hiệu quả.
- ♦ Điều hành Xử lý Sự vụ Nhanh chóng: Tiếp nhận, phân tích và điều phối xử lý mọi sự cố an ninh một cách tập trung, tối ưu hóa thời gian phản ứng và nguồn lực.
- ♦ Tích hợp Toàn diện Hệ thống An ninh: Kết nối và tổng hợp cảnh báo từ tất cả các hệ thống công nghệ (CCTV, Kiểm soát ra vào, PCCC, Báo trộm, SOS, GPS, Mobile, Loa IP, Thiết bị ngoại vi).
- ♦ Chỉ huy & Điều phối Lực lượng Hiệu quả: Tiếp nhận cảnh báo từ mọi lớp an ninh, PSOC xử lý thông tin, chỉ huy và điều phối lực lượng phản ứng kịp thời để bảo vệ mục tiêu và ngăn chặn mối đe dọa (tội phạm, khủng bố, hỏa hoạn, an ninh phi truyền thống, thiên tai).
- ♦ Phân tích Dữ liệu & Hỗ trợ Ra Quyết định:
 - Tổng hợp, phân tích dữ liệu an ninh đa nguồn.
 - Cung cấp thông tin nhanh chóng, chính xác cho cấp chỉ huy, đặc biệt trong các tình huống khẩn cấp.
 - Chủ động nhận diện và cảnh báo sớm các nguy cơ tiềm ẩn, tăng cường khả năng phòng ngừa.

B. CÁC PHÂN HỆ VÀ TÍNH NĂNG CHÍNH

▮ b. Hệ thống trung tâm An ninh

Hệ thống phần mềm Trung tâm An ninh Tập trung

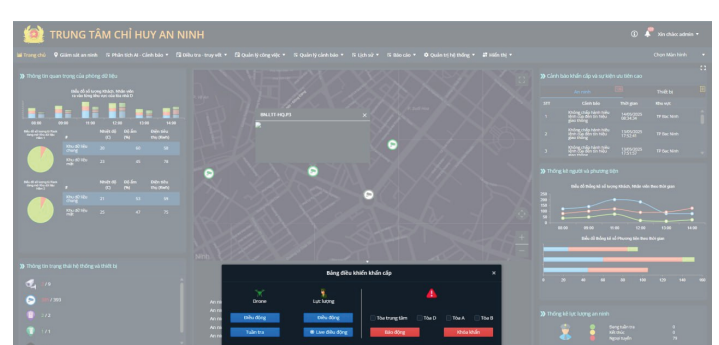
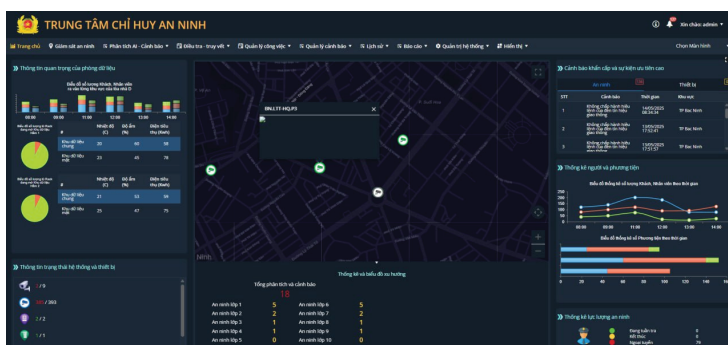
Dashboard GIS Thông minh	Quản lý & Điều khiển Từ xa	Quản lý Sự kiện & Cảnh báo	Quản lý Lực lượng & Tuần tra	Xử lý Tình huống Khẩn cấp	Báo cáo & Thống kê	Quản trị Hệ thống
--------------------------	----------------------------	----------------------------	------------------------------	---------------------------	--------------------	-------------------

Mô tả Các tính năng lõi Hệ thống phần mềm Trung tâm An ninh

- ◆ Dashboard GIS Thông minh: Hiển thị trực quan toàn bộ tình hình an ninh trên bản đồ số (GIS), tích hợp cảnh báo từ tất cả các lớp an ninh.
- ◆ Quản lý & Điều khiển Từ xa: Điều khiển camera PTZ, kích hoạt hệ thống đèn/còi báo động, đóng/mở cửa khẩn cấp, quản lý hệ thống VMS và AI Analytics.
- ◆ Quản lý Sự kiện & Cảnh báo: Tiếp nhận, phân loại, xử lý và lưu trữ mọi sự kiện, cảnh báo an ninh.
- ◆ Quản lý Lực lượng & Tuần tra: Lập kế hoạch, theo dõi (GPS), báo cáo tuần tra, điểm danh lực lượng an ninh.
- ◆ Xử lý Tình huống Khẩn cấp: Xây dựng và kích hoạt các kịch bản an ninh tự động hoặc bán tự động để ứng phó với các tình huống khẩn cấp.

B. CÁC PHÂN HỆ VÀ TÍNH NĂNG CHÍNH

- ◆ Báo cáo & Thống kê: Trực quan hóa dữ liệu, tạo báo cáo tùy chỉnh, phân tích rủi ro và hiệu suất hệ thống.
- ◆ Quản trị Hệ thống: Quản lý người dùng, phân quyền, cấu hình, giám sát trạng thái hoạt động, sao lưu/phục hồi dữ liệu.
- ◆ Quản lý hồ sơ an ninh người và phương tiện ra vào



B. CÁC PHÂN HỆ VÀ TÍNH NĂNG CHÍNH

III. ỨNG DỤNG DI ĐỘNG

Tính năng nổi bật

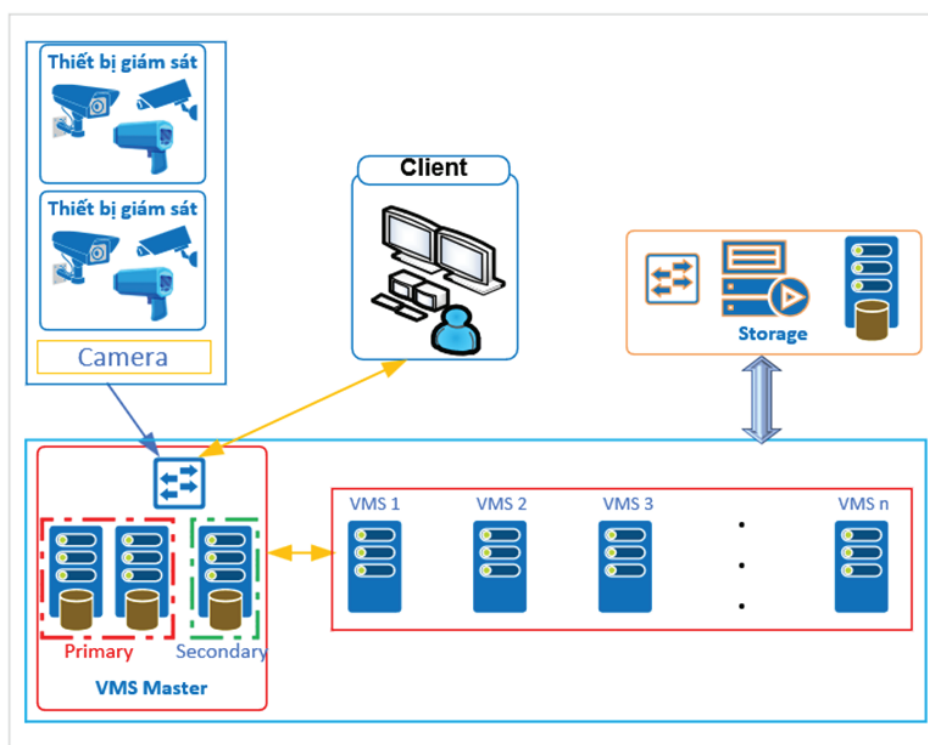
- ◆ Chỉ huy & Điều phối Linh hoạt:
 - Quản lý nghiệp vụ, giám sát an ninh trực tuyến.
 - Điều phối sự kiện, cảnh báo thông minh đến từng cá nhân/đơn vị.
 - Theo dõi, đánh giá tiến độ và phê duyệt kết quả công việc.
- ◆ Quản lý Lực lượng & Nhiệm vụ Hiệu quả:
 - Phân cấp, phân quyền nhân sự theo cơ cấu tổ chức.
 - Phân công công việc, nhiệm vụ theo kế hoạch.
- ◆ Kết nối Tác chiến Thông suốt:
 - Liên lạc đa kênh (radio, vệ tinh, di động, internet) ổn định.
 - Nhận lệnh điều động, lịch tuần tra, cảnh báo tức thời từ Trung tâm.
 - Định vị GPS, phân tuyến, chốt trực trên bản đồ số.
 - Báo cáo hiện trường, nhật ký tuần tra, SOS khẩn cấp.
- ◆ Hỗ trợ Nghiệp vụ & Ra Quyết định:
 - Tiếp nhận và xử lý "nóng" các sự kiện, cảnh báo, vi phạm.
 - Tra cứu nhanh dữ liệu, bằng chứng liên quan.
 - Báo cáo, thống kê tổng hợp theo yêu cầu.



B. CÁC PHẦN HỆ VÀ TÍNH NĂNG CHÍNH

IV. HỆ THỐNG PHẦN MỀM QUẢN LÝ CAMERA TẬP TRUNG

Phần mềm Quản lý camera tập trung



Mô hình kết nối Server VMS

- ◆ Phần mềm hỗ trợ mô hình tập trung lẫn phân tán, trong đó kiến trúc dạng lưu trữ phân tán, quản trị tập trung là tối ưu cho các hệ thống quản lý nhiều cấp.
- ◆ VMS tại các Trung tâm cấp trên hoàn toàn có thể kết nối trực tiếp đến hệ thống VMS của Trung tâm cấp dưới mình để có thể quản lý, vận hành hệ thống hòa cùng những camera đã có ở cấp trên mà không cần phát sinh luồng kết nối camera trực tiếp từ cấp dưới lên cấp trên, đồng thời có các ưu điểm:
 - Khả năng mở rộng
 - Tính sẵn sàng cao
 - Xử lý song song
 - Tính linh hoạt

B. CÁC PHẦN HỆ VÀ TÍNH NĂNG CHÍNH

Các tính năng chính của Phần mềm

- ◆ Có khả năng kết nối, quản lý tập trung không giới hạn số lượng camera (* tùy thuộc năng lực thiết bị phần cứng và license quản lý camera được trang bị)
- ◆ Kết nối, quản lý toàn bộ các camera/đầu ghi theo chuẩn IP/OnVif
- ◆ Hỗ trợ kết nối bàn điều khiển joystick điều khiển chung cho tất cả camera PTZ, cho phép điều khiển quay quét camera trực tiếp trên VMS bằng chuột điều khiển
- ◆ Hỗ trợ sẵn nhiều khung hình hiển thị, cho phép tùy chỉnh khung hình hiển thị, cho phép tùy chỉnh layout hiển thị
- ◆ Cho phép người dùng xem với các độ phân giải thấp/ cao để tối ưu đường truyền
- ◆ Không giới hạn khả năng lưu trữ (* tùy thuộc vào cấu hình phần cứng)
- ◆ Ghi hình và Playback:
 - Ghi hình theo kiểu Motion & Continuous & Event
 - Hỗ trợ Lịch ghi hình theo các ngày trong tuần
 - Ghi hình theo cơ chế cân bằng tải HDD thông minh.
 - Xuất dữ liệu hình ảnh ra file.
 - Hỗ trợ kỹ thuật: theo chu kỳ dự án hoặc yêu cầu khách hàng

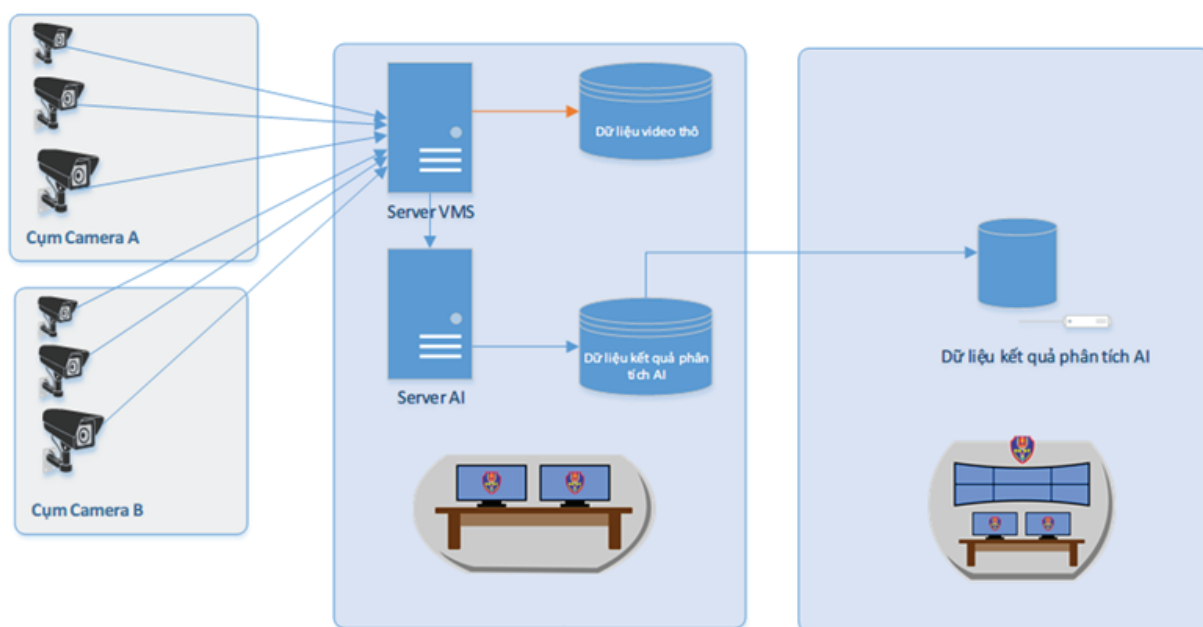
Cấu hình máy chủ (khuyến nghị)

- ◆ CPU: 2x Intel 32 Core
- ◆ RAM: 256 GB
- ◆ Ổ cứng: 2x 500 GB
- ◆ Hệ điều hành hỗ trợ: Linux/ Windows

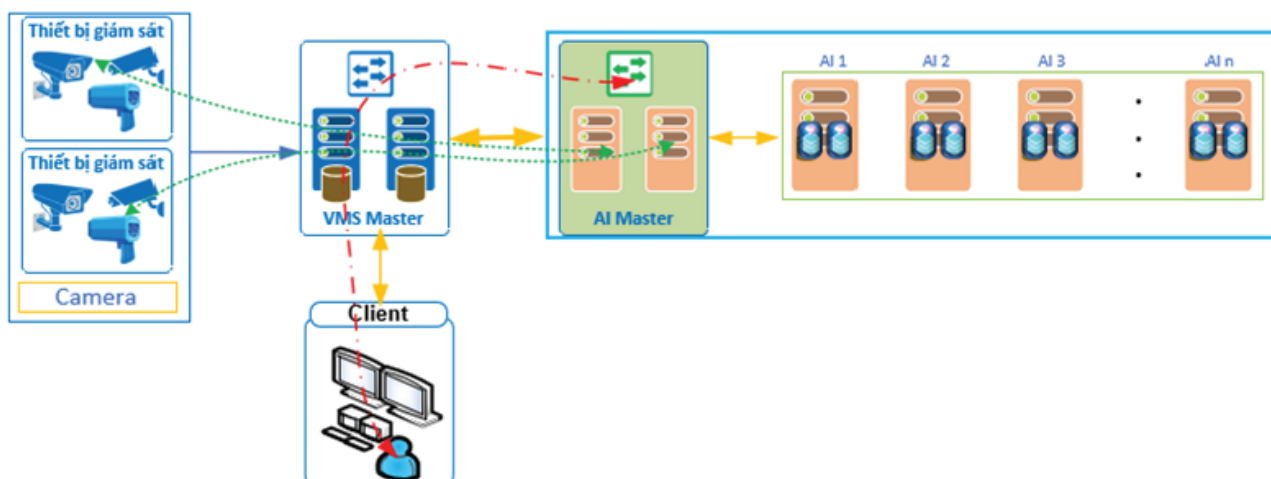
B. CÁC PHẦN HỆ VÀ TÍNH NĂNG CHÍNH

Phần mềm Quản lý camera tập trung tích hợp Trí tuệ nhân tạo

- Phần mềm sử dụng mô hình phân tích và xử lý AI tập trung tại server trung tâm, phù hợp các hệ thống lớn, phân tích, xử lý AI tổng hợp và sự phát triển không ngừng của công nghệ hiện nay. Các hệ thống server phân tích cần có cấu hình đủ mạnh để đáp ứng bài toán phân tích tổng hợp, phức tạp.



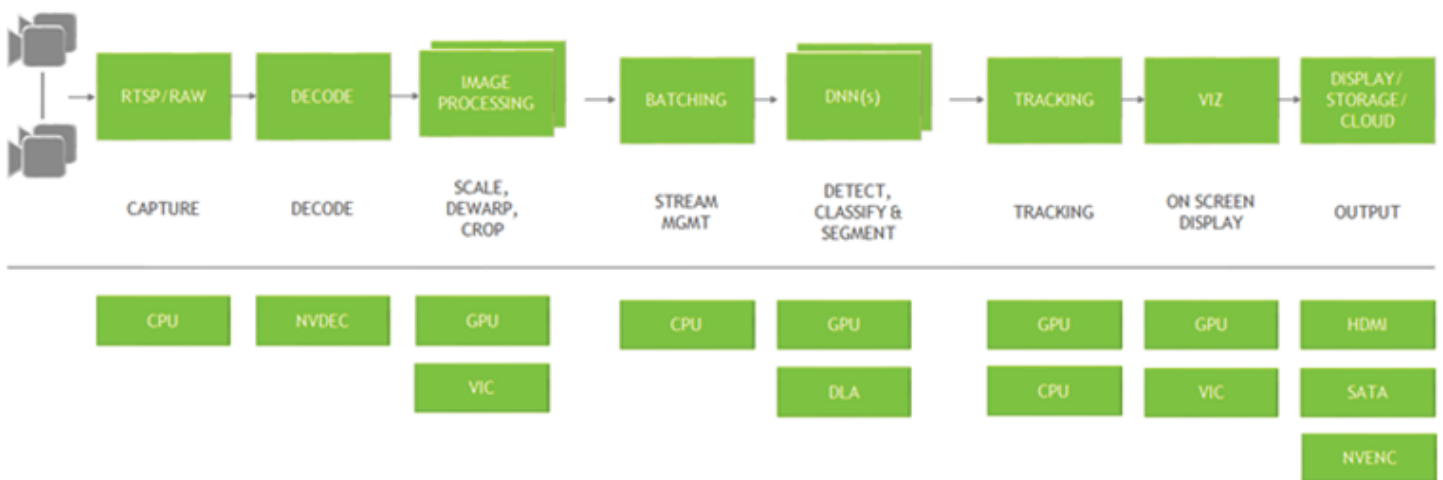
Mô hình phân tích và xử lý AI tập trung



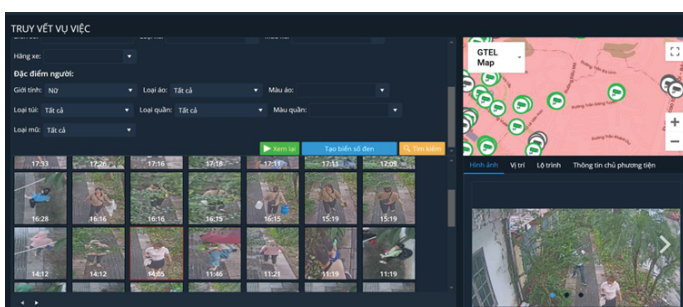
Mô hình kết nối Server VMS

B. CÁC PHẦN HỆ VÀ TÍNH NĂNG CHÍNH

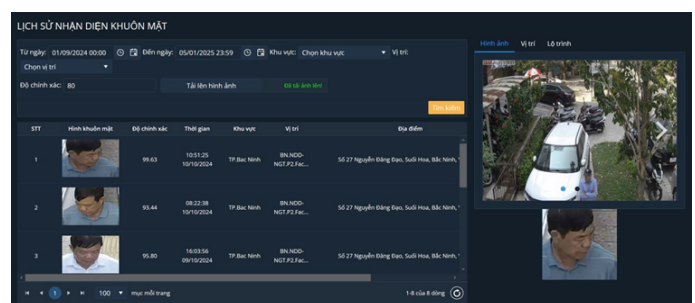
- Phần mềm ứng dụng Deepstream SDK của Nvidia vào các bài toán phân tích, xử lý AI. DeepStream của NVIDIA cung cấp một kiến trúc linh hoạt, hỗ trợ xử lý video thời gian thực và tích hợp sâu với GPU NVIDIA, hỗ trợ tích hợp dễ dàng với các công nghệ AI phổ biến, tạo ra một pipeline mạnh mẽ và linh hoạt để xây dựng và triển khai ứng dụng AI trong lĩnh vực xử lý video và hình ảnh.



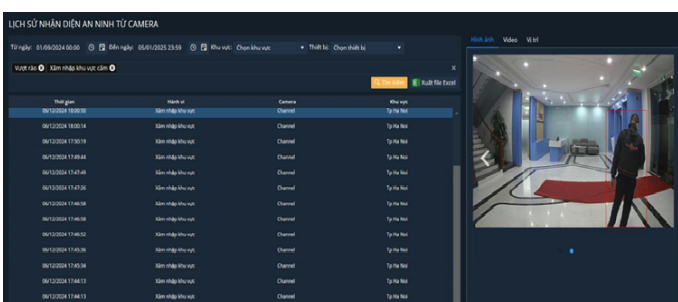
Mô hình kết nối Server VMS



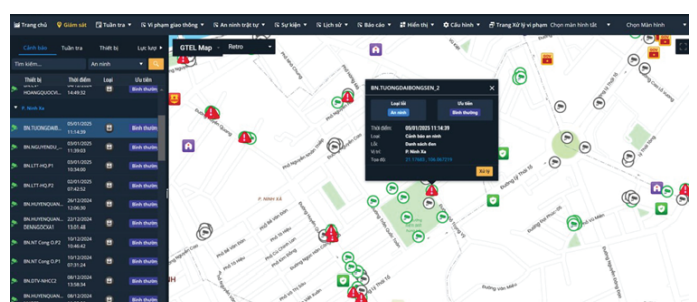
Truy vết



Nhận diện khuôn mặt



Nhận diện Xâm nhập vào vùng/Di chuyển/Ra khỏi vùng khu vực cần bảo vệ



Bản đồ vị trí cảnh báo và vị trí camera

B. CÁC PHÂN HỆ VÀ TÍNH NĂNG CHÍNH

Các tính năng chính của Phần mềm

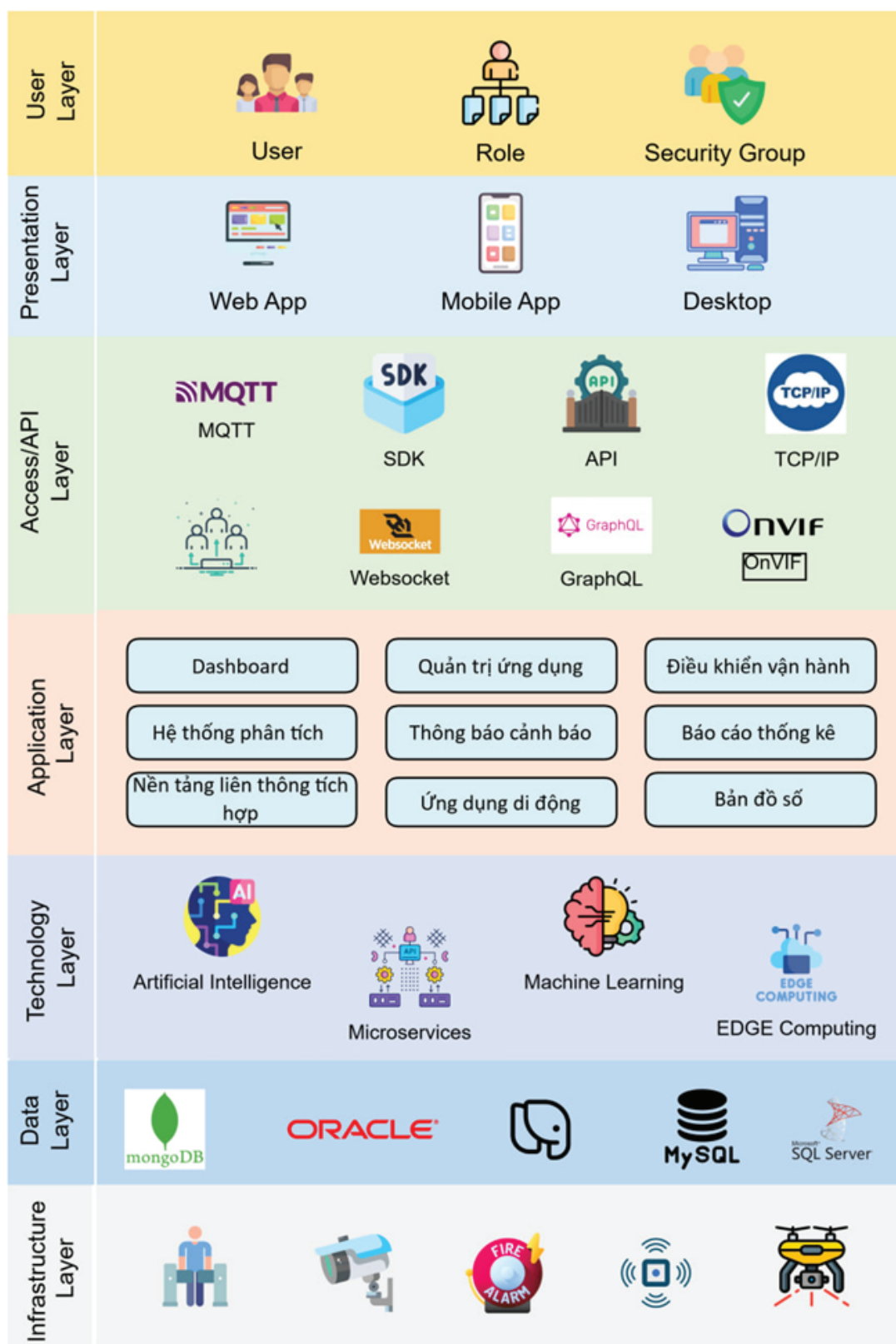
- ◆ Phát hiện các hành vi vi phạm an ninh trật tự như: tụ tập đám đông, đối tượng lảng vảng, xâm nhập vùng trái phép, đi vào vùng cấm, chui barrier, vượt rào, leo tường.
- ◆ Phát hiện gây rối trật tự công cộng, nhận diện hành vi đánh nhau, nhận diện hung khí.
- ◆ Phát hiện hành vi vi phạm giao thông, nhận diện biển số xe vi phạm, phát hiện phương tiện đi vào đường cấm.
- ◆ Phát hiện vật cản trên đường, cảnh báo tai nạn tự động.
- ◆ Phát hiện phương tiện trong danh sách đen, căn cứ trên danh sách biển số, tìm kiếm thiết bị (phương tiện) theo chủng loại, màu sơn..
- ◆ Phát hiện vi phạm đi lùi, đi ngược chiều trên đường cao tốc, phương tiện dừng đỗ không đúng nơi quy định, trên làn dừng khẩn cấp.
- ◆ Cảnh báo các vi phạm về an ninh trật tự như: tụ tập đám đông, gây rối trật tự công cộng, hành vi chui barrier, đối tượng lảng vảng, xâm nhập vùng trái phép, đi vào vùng cấm, vượt rào, leo tường.
- ◆ Cảnh báo nguy cơ ùn tắc giao thông dựa trên thu thập và phân tích thông tin lưu lượng.
- ◆ Hỗ trợ kỹ thuật: theo chu kỳ dự án hoặc yêu cầu khách hàng

Cấu hình máy chủ (khuyến nghị)

- ◆ CPU: 2x Intel 32 Core
- ◆ RAM: 256 GB
- ◆ Ổ cứng: 2x 500 GB
- ◆ Hệ điều hành hỗ trợ: Linux/ Windows

C. KIẾN TRÚC HỆ THỐNG

I. SƠ ĐỒ KIẾN THỨC HỆ THỐNG



Sơ đồ kiến trúc tổng thể

C. KIẾN TRÚC HỆ THỐNG

Mô tả chi tiết

(1) User Layer – Lớp người dùng (Truy cập & vận hành)

- ◆ Đây là lớp đại diện cho các vai trò và đối tượng sử dụng hệ thống gồm:
 - User: người dùng cuối thực hiện giám sát, phản hồi
 - Role: nhóm quyền chức năng theo vị trí (bảo vệ, kỹ thuật, điều hành...)
 - Security Group: nhóm bảo mật – kiểm soát truy cập theo chính sách phân tầng (RBAC, ABAC).
 - Giúp hệ thống an toàn, dễ kiểm soát, tránh lạm quyền và mất thông tin, đảm bảo người dùng chỉ truy cập đúng chức năng cho phép.

(2) Presentation Layer – Lớp trình bày giao diện

- ◆ Cung cấp giao diện hiển thị thông tin, cho phép tương tác người dùng:
 - Web App: vận hành qua trình duyệt (Chrome, Edge, Firefox...)
 - Mobile App: điều hành và giám sát cơ động trên iOS, Android
 - Desktop App: dành cho các trung tâm điều hành cố định, phòng SOC
 - Giao diện thân thiện, dễ tùy biến theo vai trò người dùng và thiết bị đầu cuối.

C. KIẾN TRÚC HỆ THỐNG

(3) Access/API Layer – Lớp tích hợp và giao tiếp

- ♦ Là cầu nối giữa các hệ thống, đảm bảo khả năng mở rộng và liên kết linh hoạt:
 - RESTful API: giao tiếp ứng dụng web
 - SDK: hỗ trợ lập trình viên tích hợp nhanh vào ứng dụng ngoài
 - Websocket: giao tiếp thời gian thực (event push, cảnh báo nhanh)
 - GraphQL: tối ưu hóa truy vấn dữ liệu, giảm tải mạng
 - Giao thức IoT: MQTT, TCP/IP, ONVIF – kết nối thiết bị vật lý
- ♦ Lớp này giúp nền tảng hoạt động như một “trung tâm tích hợp”, sẵn sàng mở rộng vào hệ sinh thái số.

(4) Application Layer – Lớp ứng dụng (Nghiệp vụ và điều hành)

- ♦ Tầng này tổng hợp các chức năng nghiệp vụ chính của nền tảng:
 - Dashboard: hiển thị toàn bộ trạng thái hệ thống theo thời gian thực
 - Quản trị ứng dụng: phân quyền người dùng, cấu hình hệ thống
 - Hệ thống phân tích: khai phá dữ liệu, đánh giá rủi ro, phân loại sự kiện
 - Cảnh báo thông minh: phát hiện sớm, gửi thông báo đến người xử lý
 - Báo cáo thống kê: tự động tổng hợp sự kiện, vận hành theo thời gian
 - Điều khiển vận hành: kịch bản tác chiến, điều phối nguồn lực (báo động, khóa cửa, phát loa...)
 - Ứng dụng di động: cho nhân viên tuần tra, trực trạm, tác nghiệp từ xa
 - Bản đồ số (GIS): hiển thị thiết bị, khu vực cảnh báo trên bản đồ động
- ♦ Đây là nơi điều phối và trực tiếp hỗ trợ hoạt động vận hành, giám sát và chỉ huy.

C. KIẾN TRÚC HỆ THỐNG

(5) Technology Layer – Lớp công nghệ xử lý (Nền tảng lõi)

- ♦ Là “bộ não” xử lý dữ liệu chuyên sâu, giúp hệ thống trở nên thông minh và có khả năng học hỏi:
 - Artificial Intelligence (AI): Nhận diện hình ảnh, hành vi bất thường, đột nhập, tập trung đông người...
 - Machine Learning (ML): Phân tích dữ liệu lịch sử, đưa ra dự báo (predictive analytics)
 - Microservices: Cấu trúc phần mềm dạng dịch vụ – mỗi module độc lập, dễ mở rộng và triển khai
 - Edge Computing: Xử lý dữ liệu ngay tại thiết bị biên – giảm độ trễ, tối ưu băng thông
- ♦ Lớp này quyết định hiệu quả xử lý thông tin và năng lực phản ứng thời gian thực của toàn hệ thống.

(6) Data Layer – Lớp dữ liệu (Lưu trữ và truy xuất dữ liệu)

- ♦ Đảm nhiệm việc lưu trữ, phân loại, xử lý truy vấn và trích xuất dữ liệu từ hệ thống. Các thành phần chính:
 - Hệ quản trị cơ sở dữ liệu quan hệ: PostgreSQL, MySQL, SQL Server, Oracle
 - Cơ sở dữ liệu NoSQL: MongoDB – lưu dữ liệu log, metadata, trạng thái thiết bị
 - Lưu trữ không cấu trúc: hình ảnh, video, bản đồ, báo cáo (có thể tích hợp object storage hoặc cloud S3)
- ♦ Dữ liệu từ tầng thiết bị sẽ được xử lý, phân tích và lưu tại tầng này phục vụ vận hành, phân tích và truy xuất.

C. KIẾN TRÚC HỆ THỐNG

(7) Infrastructure Layer – Lớp hạ tầng thiết bị (Thiết bị vật lý)

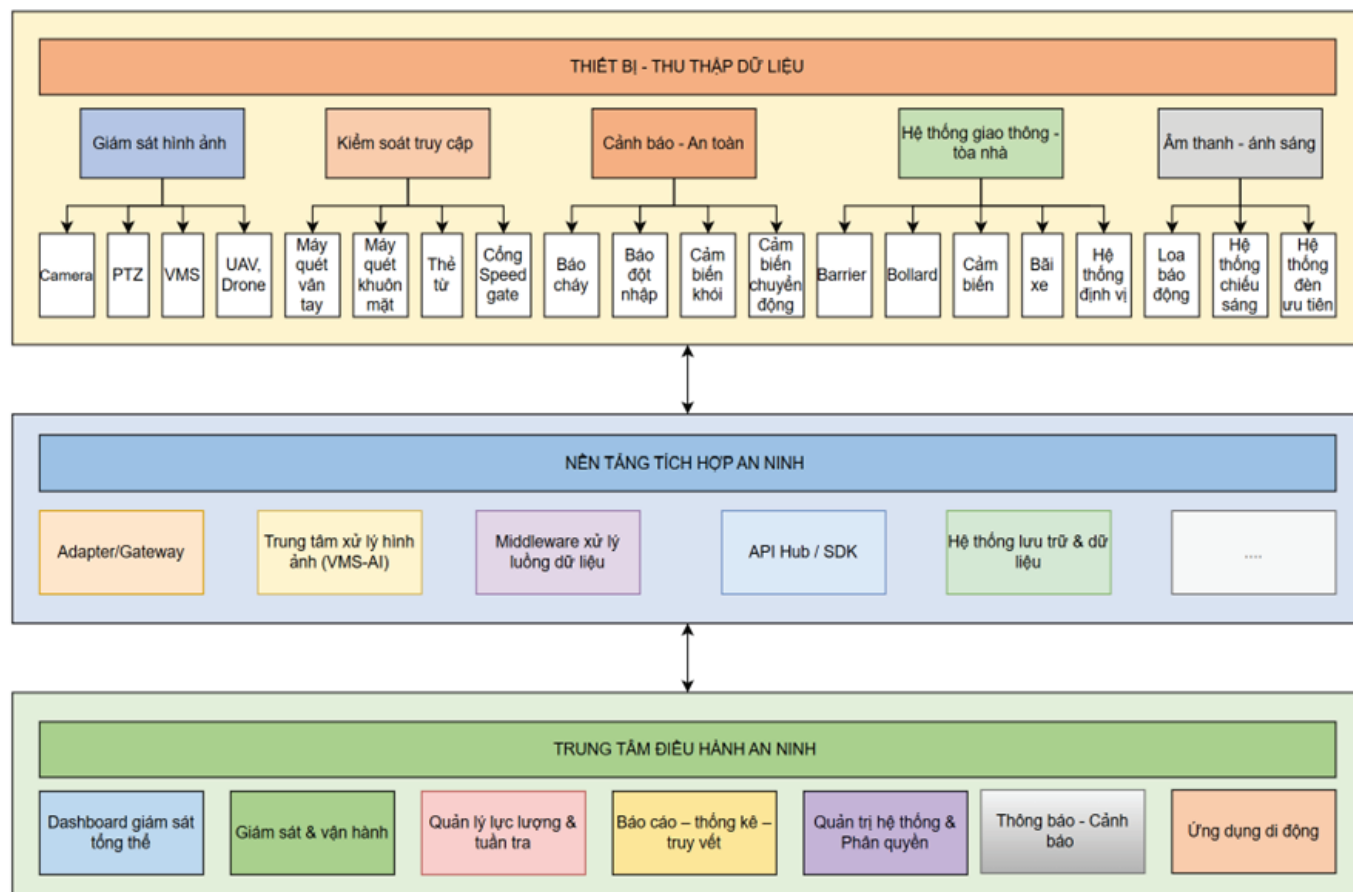
- ◆ Là tầng phụ trách thu thập tín hiệu, hình ảnh, trạng thái từ các thiết bị vật lý trong hệ thống. Bao gồm:
 - Thiết bị kiểm soát ra vào (cổng từ, máy quét thẻ, sinh trắc học)
 - Camera giám sát (CCTV) chuẩn ONVIF, có thể hỗ trợ phân tích AI tại biên
 - Hệ thống báo cháy, cảm biến môi trường, cảnh báo gas, độ ẩm, chuyển động
 - Thiết bị truyền dẫn tín hiệu không dây (RFID, Zigbee, LoRa, BLE...)
 - Drone giám sát – thiết bị bay không người lái hỗ trợ tuần tra tự động
- ◆ Tầng này đóng vai trò là “nguồn dữ liệu đầu vào” cho toàn bộ hệ thống.

Tính chất đặc trưng của kiến trúc tổng quát

- ◆ Toàn trình, khép kín: từ thu thập, xử lý, phân tích, cảnh báo đến điều hành và phản ứng.
- ◆ Bảo mật phân lớp: chuẩn hóa theo ISO/IEC 27001, hỗ trợ Zero Trust.
- ◆ Khả năng mở rộng cao: nhờ kiến trúc microservices và API mở.
- ◆ Tích hợp thông minh: hỗ trợ liên thông với hệ thống PCCC, giao thông, đô thị thông minh...

C. KIẾN TRÚC HỆ THỐNG

II. MÔ HÌNH KIẾN TRÚC HỆ THỐNG TÍCH HỢP AN NINH VẬT LÝ



Mô hình tổng thể Nền tảng tích hợp ANVL

C. KIẾN TRÚC HỆ THỐNG

Mô tả chi tiết của mô hình

(1) Thiết bị - Thu thập dữ liệu

- ♦ Thu thập dữ liệu từ các cảm biến, camera và thiết bị tại hiện trường. Đây là lớp kết nối giữa thế giới vật lý và hệ thống số hóa.
 - Giám sát hình ảnh: camera, PTZ, VMS, UAV/Drone -> phục vụ theo dõi diện rộng và thời gian thực.
 - Kiểm soát truy cập: máy quét khuôn mặt, vân tay, thẻ từ, cổng speedgate -> kiểm soát vào/ra tự động.
 - Cảnh báo - An toàn: báo cháy, đột nhập, cảm biến khói/ chuyển động -> xử lý tình huống khẩn cấp.
 - Hệ thống giao thông - tòa nhà: barrier, bollard, cảm biến, bãi xe, định vị -> hỗ trợ kiểm soát phương tiện.
 - Âm thanh - ánh sáng: loa, đèn chiếu sáng, đèn ưu tiên -> hỗ trợ truyền thông báo, chỉ dẫn.

(2) Nền tảng tích hợp an ninh

- ♦ Xử lý, tích hợp, đồng bộ hóa dữ liệu đa nguồn; kết nối dữ liệu thô thành luồng dữ liệu giá trị để phân tích và vận hành.
 - Adapter/Gateway: kết nối các thiết bị đa chuẩn.
 - Trung tâm xử lý hình ảnh (VMS-AI): phân tích video AI (nhận diện khuôn mặt, hành vi bất thường...).
 - Middleware: xử lý luồng dữ liệu, kết nối đến hệ thống điều hành.
 - API Hub/SDK: mở rộng tích hợp bên ngoài.
 - Lưu trữ dữ liệu: lưu trữ video, nhật ký, báo cáo...

C. KIẾN TRÚC HỆ THỐNG

(3) Trung tâm điều hành an ninh

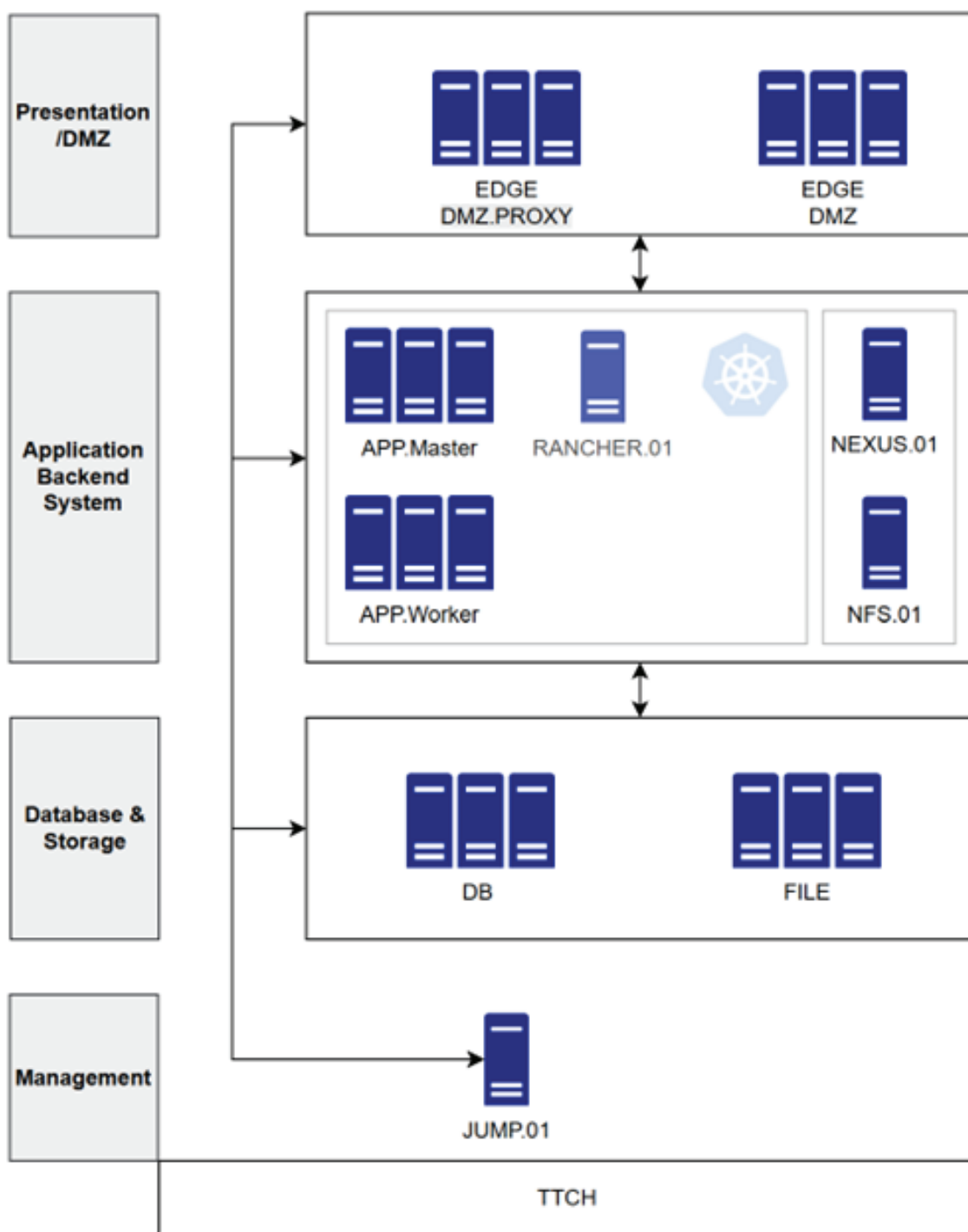
- ◆ Cung cấp giao diện trực quan để điều hành, phân tích, xử lý cảnh báo, điều phối lực lượng bảo vệ và truy vết sự kiện.
 - Dashboard giám sát tổng thể
 - Giám sát & vận hành
 - Quản lý lực lượng & tuần tra
 - Báo cáo - thống kê - truy vết
 - Phân quyền - quản trị hệ thống
 - Cảnh báo & thông báo
 - Ứng dụng di động

Mối liên kết giữa các lớp

- ◆ Dữ liệu từ các thiết bị hiện trường sẽ được đẩy về nền tảng xử lý, phân tích và chuyển thành các sự kiện (events).
- ◆ Các sự kiện này được hiển thị theo thời gian thực trên hệ thống dashboard và điều phối xử lý từ trung tâm điều hành.
- ◆ Thông tin cảnh báo, hình ảnh, video... được đồng bộ hai chiều giữa trung tâm và hiện trường qua nền tảng tích hợp.

C. KIẾN TRÚC HỆ THỐNG

III. MÔ HÌNH TRIỂN KHAI HỆ THỐNG



Mô hình triển khai Hệ thống

C. KIẾN TRÚC HỆ THỐNG

Mô hình được chia thành 4 lớp chính

- ◆ Presentation / DMZ: lớp trình bày, đảm bảo giao tiếp với bên ngoài.
- ◆ Application Backend System: lớp xử lý nghiệp vụ chính.
- ◆ Database & Storage: lưu trữ dữ liệu và cơ sở dữ liệu.
- ◆ Management: lớp quản lý truy cập hệ thống.

Chi tiết từng lớp

(1) Presentation / DMZ

- ◆ Lớp chịu trách nhiệm giao tiếp với người dùng bên ngoài hoặc các hệ thống khác.
 - EDGE.DMZ.PROXY: Các máy chủ proxy cân bằng tải, định tuyến và bảo vệ hệ thống khỏi truy cập trái phép.
 - EDGE.DMZ: Các máy chủ EDGE xử lý các yêu cầu từ bên ngoài vào hệ thống, có thể kết hợp với firewall và reverse proxy.

(2) Application Backend System

- ◆ Lớp xử lý nghiệp vụ chính, chạy các dịch vụ và ứng dụng chính.
 - APP.Master: Các node Master trong cụm Kubernetes – điều phối container, quản lý tài nguyên.
 - RANCHER.01: Máy chủ chạy Rancher – nền tảng điều khiển và quản lý các cụm Kubernetes.
 - APP.Worker: Các node Worker xử lý các tác vụ và triển khai container thực tế.
 - NEXUS.01: Máy chủ lưu trữ repository (kho lưu mã nguồn, build artifact).
 - NFS.01: Dịch vụ lưu trữ chia sẻ theo chuẩn NFS, dùng để mount vào các node.

C. KIẾN TRÚC HỆ THỐNG

(3) Database & Storage

- ◆ Lưu trữ dữ liệu và cơ sở dữ liệu.
 - DB: Các máy chủ cơ sở dữ liệu, phục vụ lưu trữ dữ liệu cho ứng dụng backend.
 - FILE: Các máy chủ lưu trữ dữ liệu file (log, media, backup...), tăng cường độ tin cậy và hiệu suất.

(4) Management

- ◆ Lớp quản lý truy cập hệ thống.
 - JUMP.01: Máy chủ Jumpbox, làm điểm truy cập trung gian để quản trị hệ thống. Người quản trị sẽ kết nối đến đây trước khi tiếp cận các máy chủ khác.

Kết nối mạng và luồng hoạt động

- ◆ Người dùng truy cập hệ thống thông qua các proxy trong lớp DMZ (EDGE.DMZ.PROXY).
- ◆ Các yêu cầu được chuyển tiếp đến hệ thống backend qua các EDGE servers.
- ◆ Kubernetes được triển khai với các node master và các node worker, quản lý và chạy các container ứng dụng.
- ◆ Rancher hỗ trợ quản trị cụm Kubernetes.
- ◆ Nexus phục vụ việc lưu trữ package, Docker image hoặc artifacts.
- ◆ Dữ liệu ứng dụng được ghi vào database hoặc lưu file vào các máy chủ lưu trữ file.

Quản trị viên kết nối hệ thống qua JUMP.01 để truy cập các máy chủ nội bộ an toàn .

C. KIẾN TRÚC HỆ THỐNG

Mục tiêu của hệ thống

- ◆ Kiểm thử khả năng triển khai hệ thống theo kiến trúc microservices sử dụng Kubernetes.
- ◆ Đánh giá hiệu năng, tính ổn định và khả năng mở rộng của hệ thống.
- ◆ Đảm bảo mô hình mạng, bảo mật và quản trị hoạt động hiệu quả trước khi triển khai chính thức.

D. YÊU CẦU HỆ THỐNG

I. YÊU CẦU MÔI TRƯỜNG PHẦN MỀM

- ◆ **Hệ điều hành:** Ubuntu Server, Windows Server 2019+
- ◆ **Hệ quản trị Cơ sở dữ liệu:** Hỗ trợ các hệ quản trị CSDL phổ biến như PostgreSQL, MySQL, MongoDB, Elasticsearch hoặc MS SQL.
- ◆ **Thư viện và Frameworks:** Sử dụng các thư viện và frameworks mã nguồn mở hiện đại, phổ biến đã được kiểm chứng và có cộng đồng hỗ trợ mạnh mẽ như OpenCV, TensorFlow (AI), Mapbox/Leaflet (GIS)
- ◆ **Trình duyệt Web:** Đảm bảo khả năng tương thích hoàn toàn với các phiên bản mới nhất của các trình duyệt web phổ biến: Google Chrome, Mozilla Firefox, Microsoft Edge, Safari.
- ◆ **Ứng dụng di động:** Hỗ trợ hệ điều hành Android và iOS

II. YÊU CẦU VỀ HẠ TẦNG PHẦN CỨNG

- ◆ Các thông số kỹ thuật chi tiết về cấu hình phần cứng máy chủ (CPU, RAM, dung lượng lưu trữ, IOPS) sẽ được đội ngũ chuyên gia của Gtel ICT tư vấn và thiết kế tối ưu dựa trên phân tích quy mô triển khai thực tế, số lượng thiết bị tích hợp, khối lượng dữ liệu dự kiến và các yêu cầu đặc thù về hiệu năng và độ sẵn sàng của từng khách hàng.
- ◆ Hệ thống được thiết kế để có thể triển khai linh hoạt trên các mô hình hạ tầng đa dạng, bao gồm On-premise, Private Cloud hoặc Hybrid Cloud.
- ◆ Yêu cầu về hạ tầng mạng: cần đảm bảo băng thông, độ trễ thấp và độ ổn định cao để truyền tải dữ liệu video hình ảnh và các luồng thông tin cảnh báo thời gian thực.

E. THÔNG TIN THƯƠNG MẠI

I. ĐĂNG KÝ BẢN QUYỀN

II. CÔNG BỐ SẢN PHẨM:

1. Tên thương mại: GSAFE-C3

2. Mã sản phẩm: GFASE-C3-PSIM

3. Nhà sản xuất: GTEL ICT - OTS

Đồng sở hữu: CÔNG TY TNHH CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG GTEL (GTEL ICT) và CÔNG TY CỔ PHẦN GIẢI PHÁP CÔNG NGHỆ TRỰC TUYẾN GTEL (GTEL OTS) (Tiền thân là CÔNG TY TNHH GIẢI PHÁP CÔNG NGHỆ TRỰC TUYẾN).

4. Xuất xứ: Việt Nam

5. Năm phát hành: 2022. Phiên bản v01.2025

6. Loại bản quyền: Vĩnh viễn.

7. Giới hạn người dung: Không giới hạn.

8. Chính sách thương mại:

- Cung cấp bản quyền theo phạm vi dự án hoặc server/cụm server.
- Cập nhật và hỗ trợ kỹ thuật: 01 - 03 năm hoặc theo yêu cầu của khách hàng.

9. Bảo hành hỗ trợ kỹ thuật:

TP. HCM: 385C Nguyễn Trãi, Phường Nguyễn Cư Trinh, Quận 1, TP. Hồ Chí Minh.

Tel: 028.7300.0148

Hà Nội: 103 -105 Nguyễn Tuân, Phường Thanh Xuân Trung, Quận Thanh Xuân,

Hà Nội. **Tel:** 069.234.8787





CÔNG TY TNHH CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG GTel

Trụ sở chính: 103, Nguyễn Tuân, P. Thanh Xuân Trung, Q. Thanh Xuân, TP. Hà Nội

Tel: 069.234.8787

Văn phòng HCM: 47 Phạm Viết Chánh, P. Nguyễn Cư Trinh, Q.1, TP.HCM

Tel: 028.7300.0148

Web: <https://gtelict.vn>



CÔNG TY CỔ PHẦN GIẢI PHÁP CÔNG NGHỆ TRỰC TUYẾN GTel

Trụ sở chính: 385C Nguyễn Trãi, P. Nguyễn Cư Trinh, Q. 1, TP. Hồ Chí Minh

VPHN: 103 - 105 Nguyễn Tuân, P. Thanh Xuân Trung, Q. Thanh Xuân, TP. Hà Nội

Tel: 028.2247.6869

Mail: info@ots.vn

Web: <http://ots.vn>