Energy Management System in Intelligent Buildings (EMSIB)

IoT & Control (Device & Sensor Layer)

Aday García López
Cristian Costa

Software Engineering
27/11, 10:45h

2025/2026

Purpose and guidelines

- The IoT & Control component is responsible for collecting real-time data from sensors installed in the building and controlling connected devices such as lights, HVAC systems, and renewable energy sources.
- Its main goal is to improve energy efficiency, comfort, and automation within intelligent buildings.

- Guidelines:

    - **Reliable:** ensure stable and reliable data transfer using MQTT communication and standardized IoT communication protocols.

    - **Local Automation:** support automatic local control based on sensor readings.

    - **Security:** guarantee secure communication between devices and the EMSIB server.

    - **Scalability:** design the system to easily integrate new sensors and devices as the building infrastructure expands.

Requirements

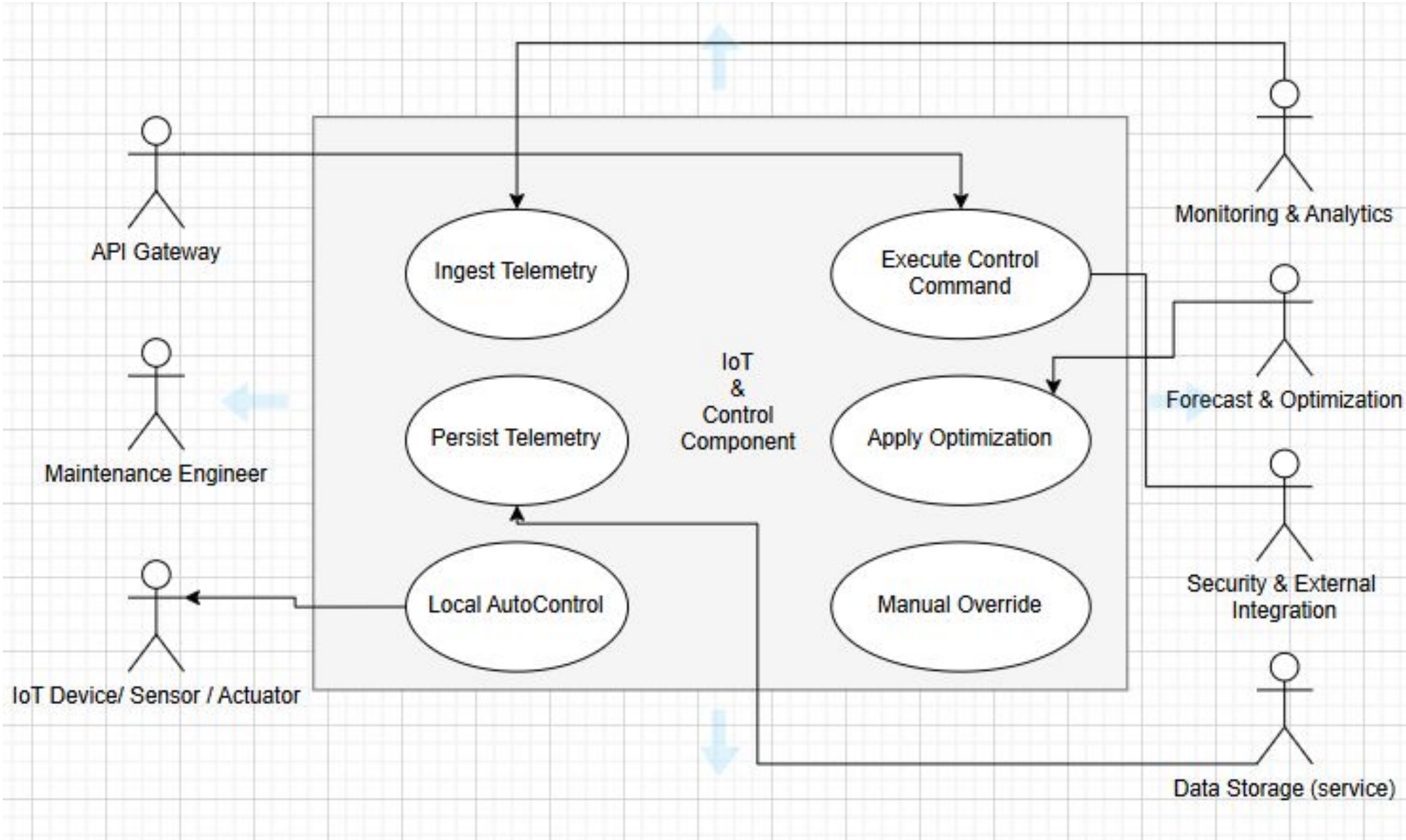
Functional Requirements

- Data acquisition: the component must collect data from sensors, meters, IoT devices in real time.
- Device control: it must control connected devices.
- Communication and integration: it must ensure secure and efficient communication with other EMSIB components.
- Data transmission: collected data must be transmitted to the Data Storage service for long-term persistence and made available to Monitoring & Analytics for visualization and analysis.
- Receiving optimization scenarios: it must receive predictive control parameters from the Forecast & Optimization Component and adjust device operation accordingly.
- Renewable integration: it must manage the connection and operation of renewable sources, prioritizing local energy usage before drawing from the grid.

Non-Functional Requirements

- Performance: sensor data must be processed and transmitted in real time with minimal latency.
- Scalability: the architecture must support horizontal scaling, allowing the addition of new buildings, sensors and devices without performance degradation.
- Security: all communications must be encrypted (TLS/HTTPS). Authentication and authorization must rely on OAuth2 and JWT tokens provided by the Security & External Integration Component.
- Reliability: the component must guarantee 99.5% uptime, implementing local buffering or fallback mechanism to prevent data loss during connectivity issues.
- Maintainability: the system should follow a microservice design with CI/CD support for easy deployment, updates, and debugging.
- Interoperability: the component must communicate using standard industrial IoT protocols to integrate easily with heterogeneous devices and external energy systems.

Use case diagram



The Use Case Diagram represents the interactions between the IoT & Control component and external actors such as:

- **Maintenance Engineer:** manages device maintenance and receives alerts.
- **API Gateway:** provides secure communication between the component and other system modules.
- **Monitoring & Analytics:** receives telemetry and sends feedback.
- **Forecast & Optimization:** sends predictive control commands to adjust building devices.

The main use cases include:

- Ingest Telemetry
- Persist Telemetry
- Local AutoControl
- Execute Control Command
- Apply Optimization
- Manual Override

Relations with other components

- **API Gateway:** it acts as the secure communication channel between IoT devices and the EMSIB platform. It authenticates incoming telemetry or control requests, routes them to IoT & Control, and ensures that only authorized data flows through.

- **Monitoring & Analytics:** the IoT & Control Component continuously sends real-time data to the Monitoring & Analytics Component. This data will be analyzed, processed, and visualized by the Monitoring & Analytics Component. Feedback can then be sent back to the IoT & Control Component to adjust device operation parameters.

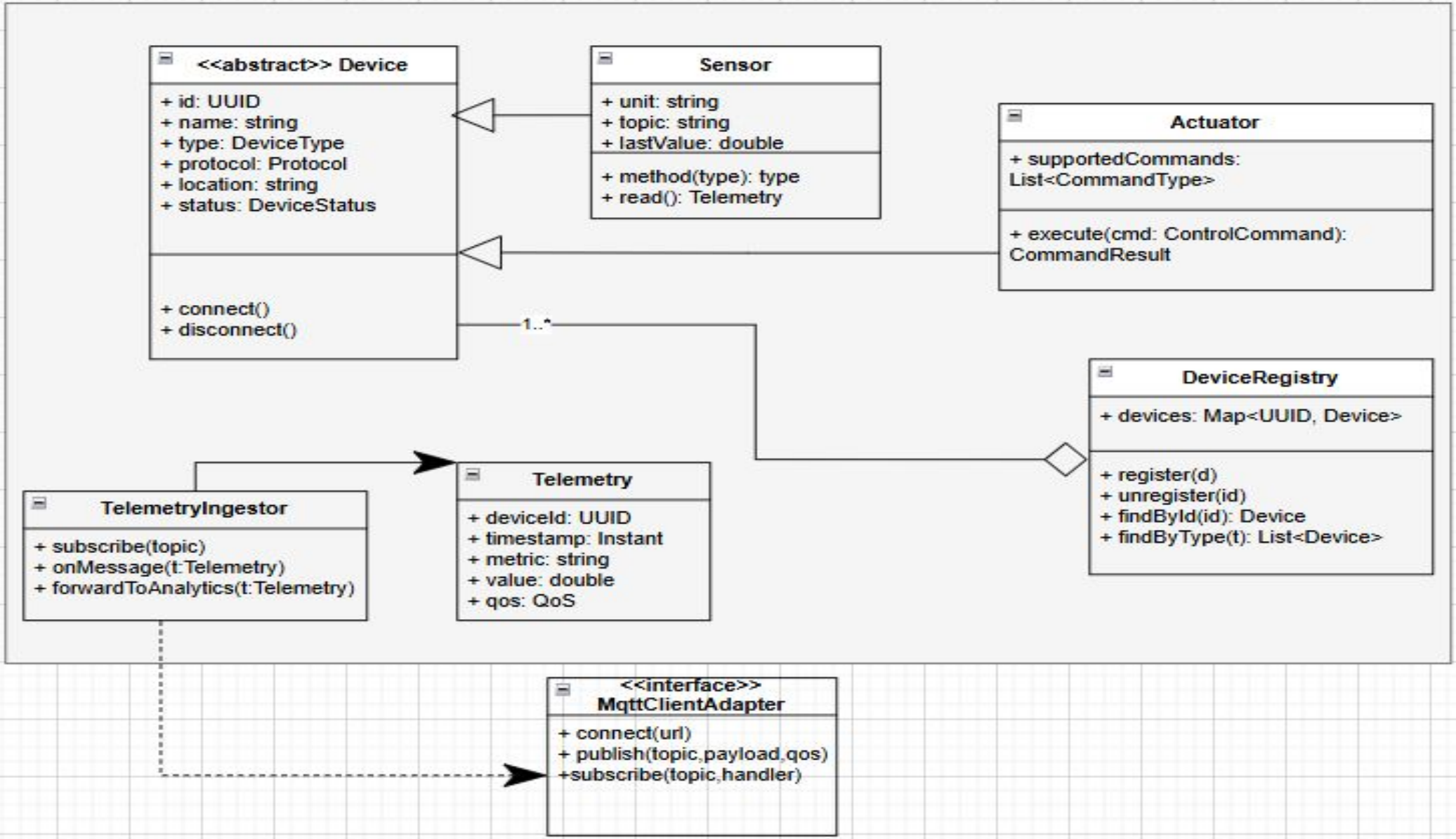
- **Forecast & Optimization:** the IoT & Control Component receives predictive control parameters and optimization scenarios from the Forecast & Optimization Component. These recommendations are used to automatically adjust lighting, HVAC, or renewable energy systems.

- **Data Storage:** All collected telemetry data is transmitted to the Data Storage service for long-term persistence. The stored data is later accessed by the Monitoring & Analytics and Forecast & Optimization components for visualization, model training, and forecasting.

- **Security & External Integration Component:** IoT & Control relies on this component for authentication, authorization, and encryption key management. All communications use credentials and tokens issued by the Security layer, guaranteeing data integrity and privacy.

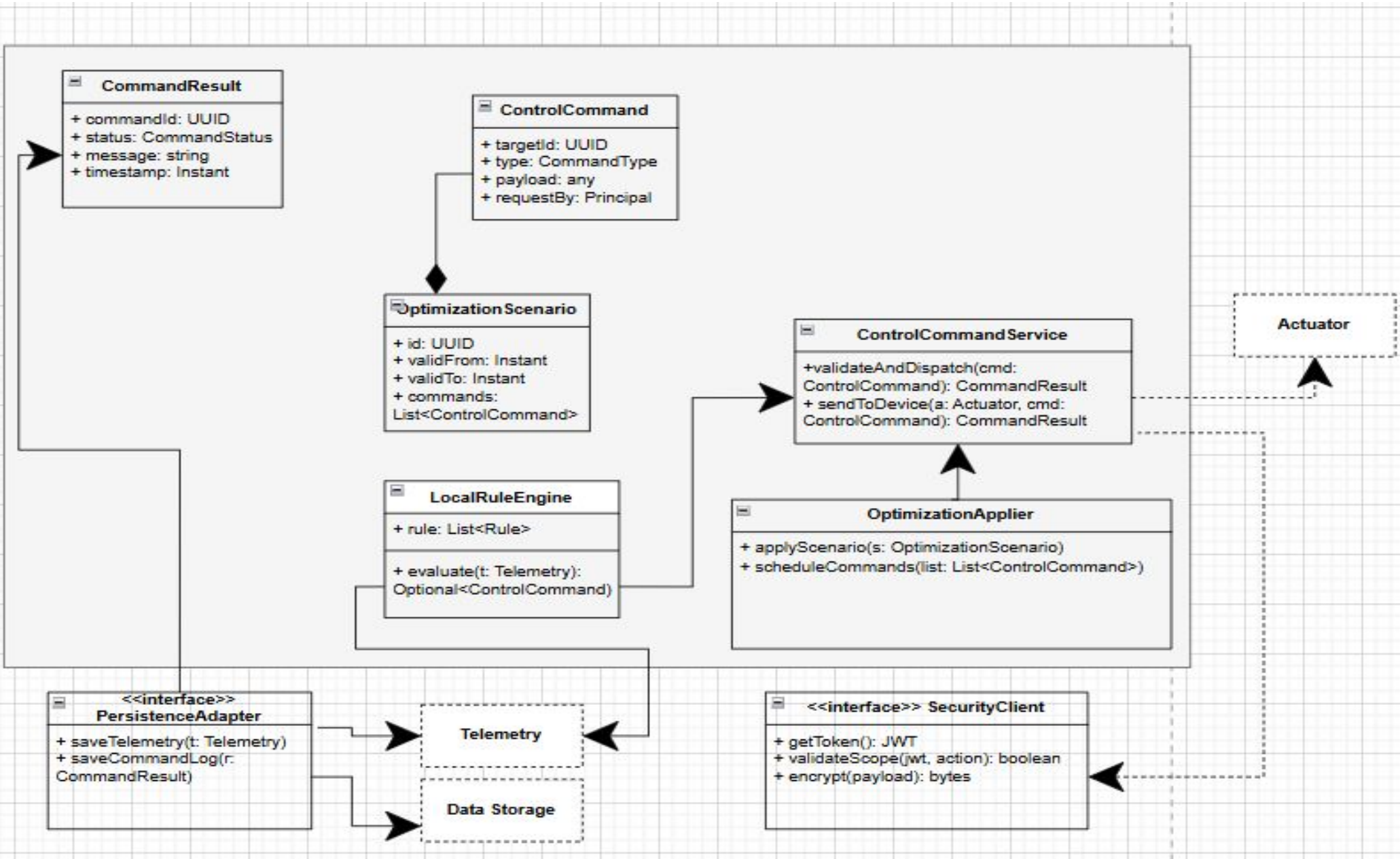
Class diagram - Domain & Ingestion

The Domain & Ingestion classes define the core data model for sensor readings, device types, and data acquisition methods within the IoT & Control system.



Class diagram - Control, Security & Persistence

These classes describe the logic used for device control, security validation, and persistence of data within the EMSIB architecture.



Scenario 1: Ingest Telemetry

Actors: Sensor, IoTService, Data Storage, Monitoring & Analytics.

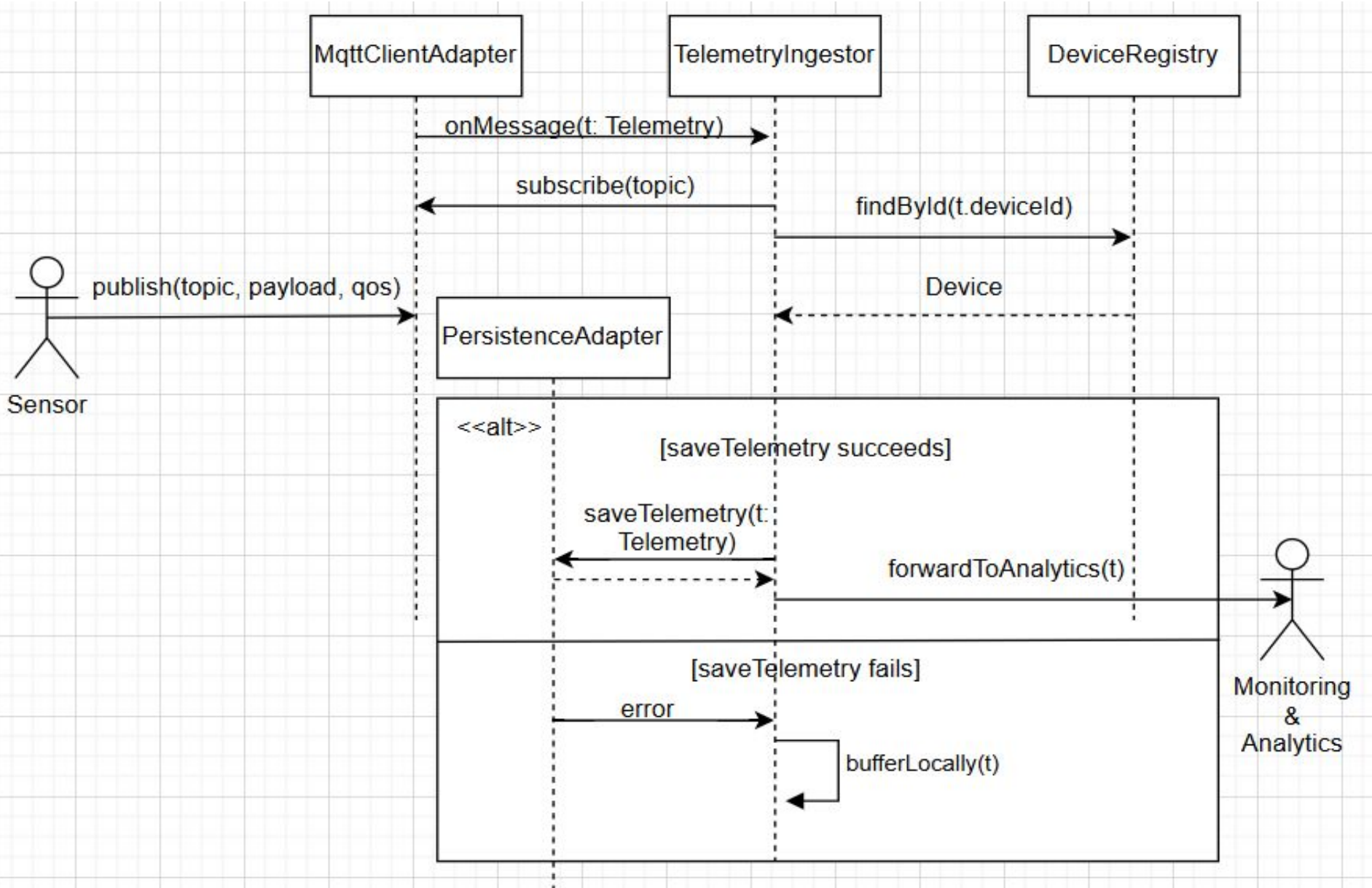
Main flow:

1. A Sensor collects environmental data (temperature, humidity, power usage).
2. The IoTService receives and validates the incoming data packet.
3. Valid data is stored in the Data Storage module.
4. IoTService forwards processed data to the Monitoring & Analytics module for visualization.

Alternative flow:
If communication with Data Storage fails, IoTService buffers the telemetry locally and retries transmission.

Result:
Sensor data is successfully stored and visualized in real time for analysis.

Sequence diagram - Ingest Telemetry



Scenario 2: Apply Optimization

Actors: Forecast & Optimization, API Gateway, IoTService, Controller, Device.

Main flow:

1. Forecast & Optimization generates a new command (e.g. lower HVAC temperature)
2. The command is sent through the API Gateway to the IoTService
3. IoTService validates the command and sends it to the Controller.
4. The Controller applies the command to the target Device.
5. The Device updates its state and reports back.
6. IoTService forwards the update to Monitoring & Analytics.

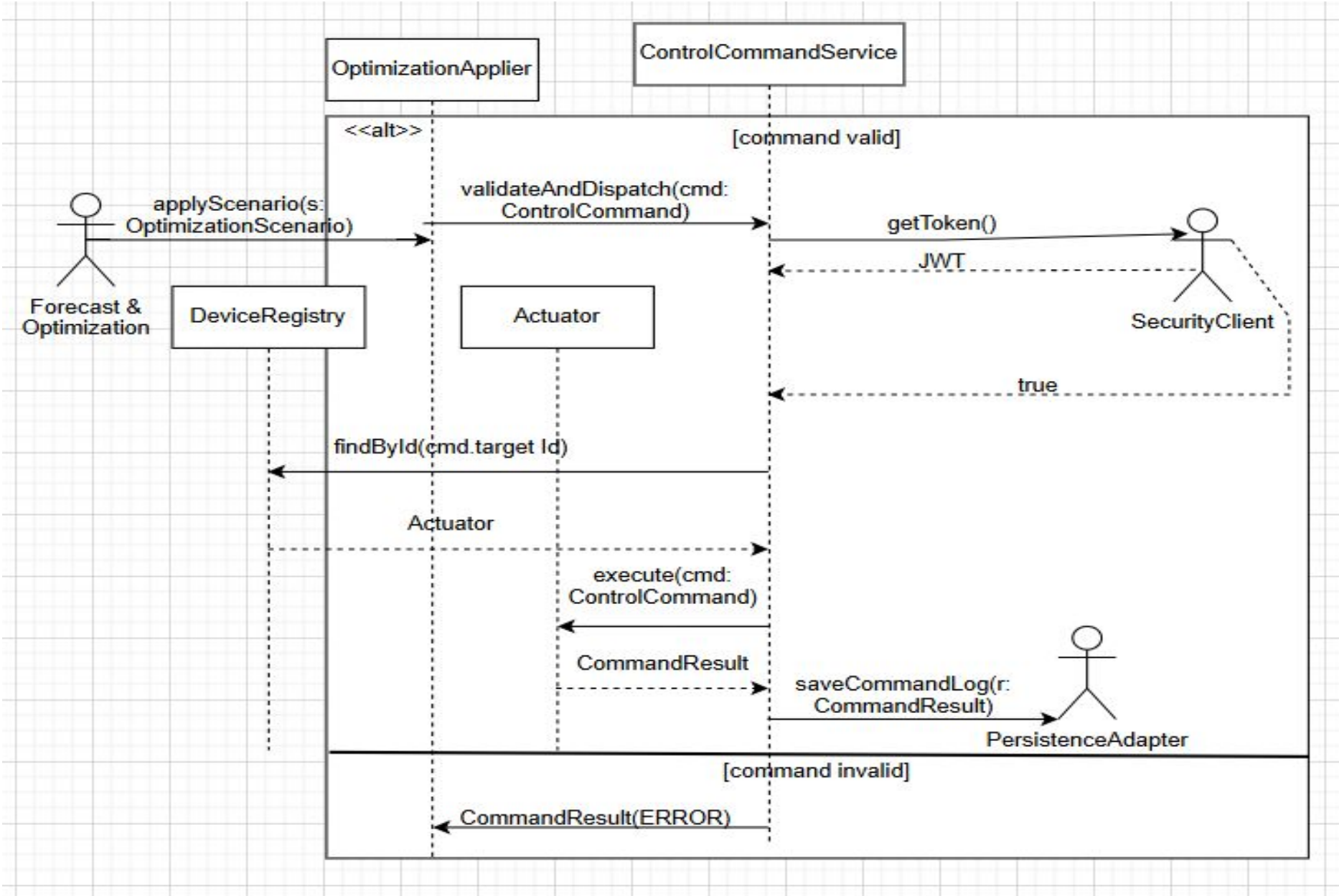
Alternative flow:

If validation fails, IoTService rejects the command and sends an error to the API Gateway.

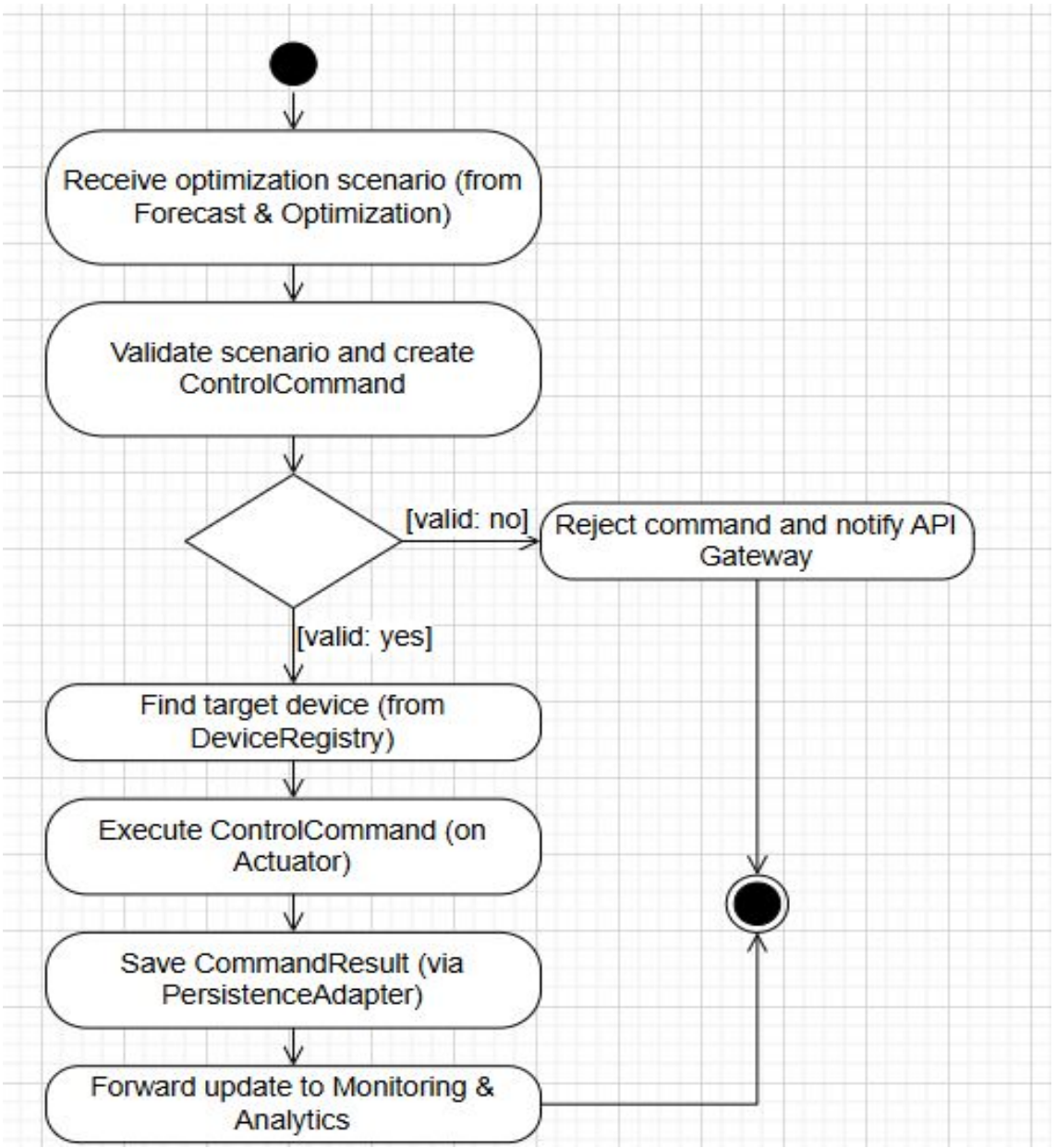
Result:

The device applies the optimized parameters, improving energy efficiency.

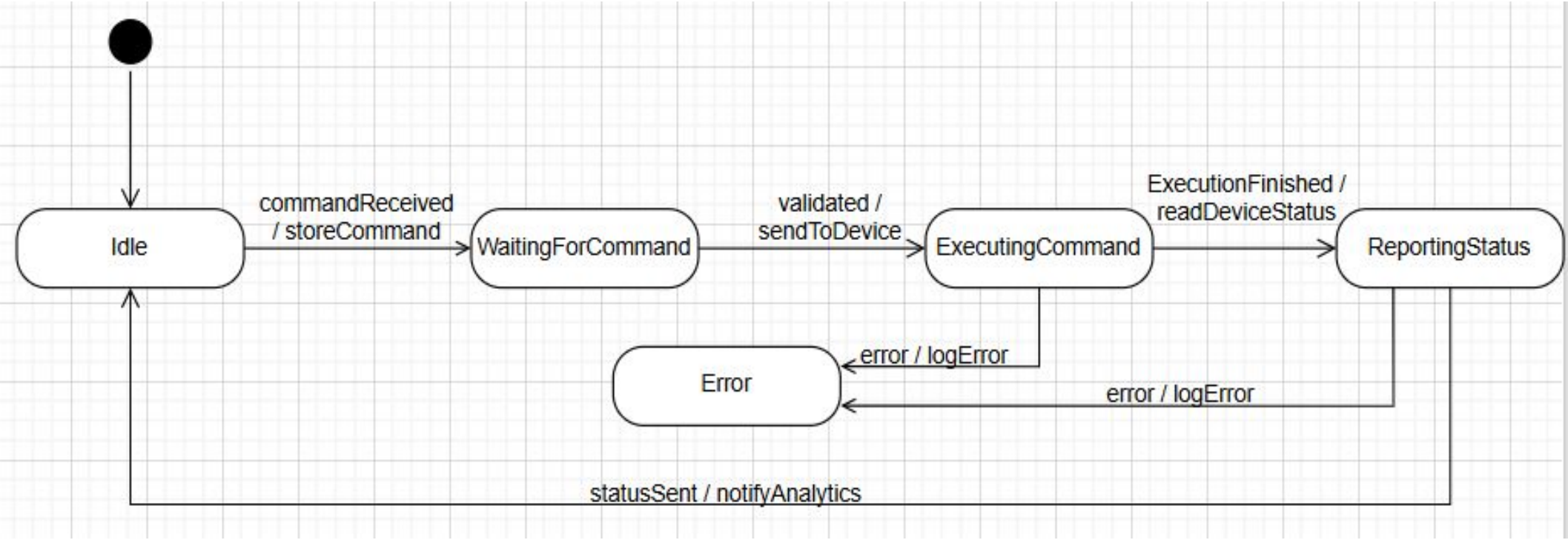
Sequence diagram - Apply Optimization



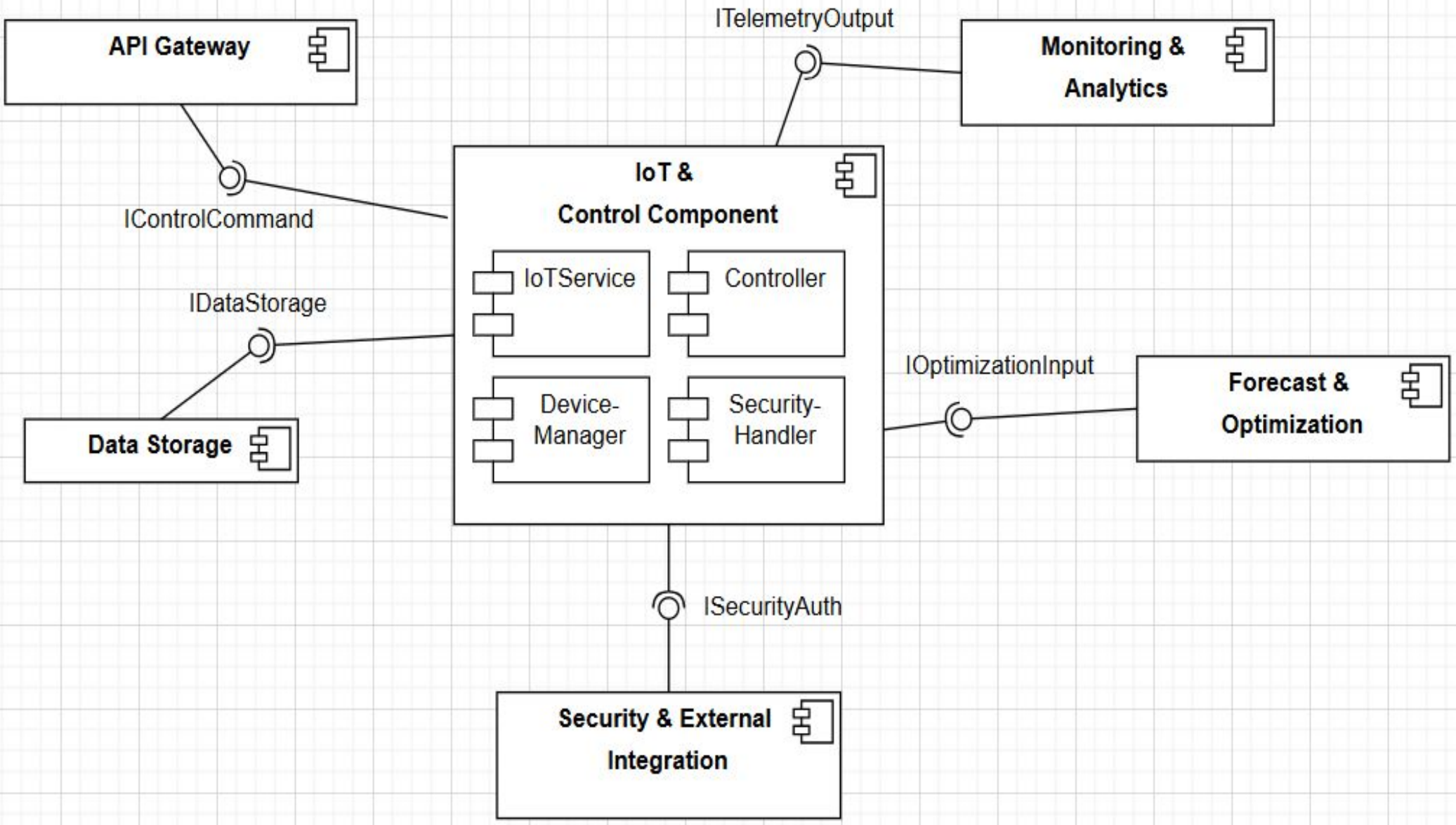
Activity diagram - Apply Optimization



State machine diagram - Device



Component diagram



Realization of guidelines and requirements

The IoT & Control component fulfills all defined guidelines and requirements:

- **Secure communication:** all telemetry and control traffic is encrypted using MQTT over TLS and HTTPS.
- **Real-time operation:** supports continuous monitoring, low-latency data acquisition, and automatic device-control.
- **Fault tolerance:** includes buffering, retry logic, and local fallback mechanism to prevent data loss during outages.
- **Scalability & maintainability:** designed as a modular microservice with clear interfaces, enabling independent scaling and easy updates.

Realization of relations with other components

The IoT & Control component demonstrates proper integration with all EMSIB modules:

- **API Gateway:** manages authentication and data routing.
- **Monitoring & Analytics:** receives sensor telemetry for visualization.
- **Forecast & Optimization:** provides predictive control parameters.
- **Data Storage:** ensures consistent and secure data storage.

Each interaction is compliant with EMSIB communication protocols and system security policies.

THANK YOU