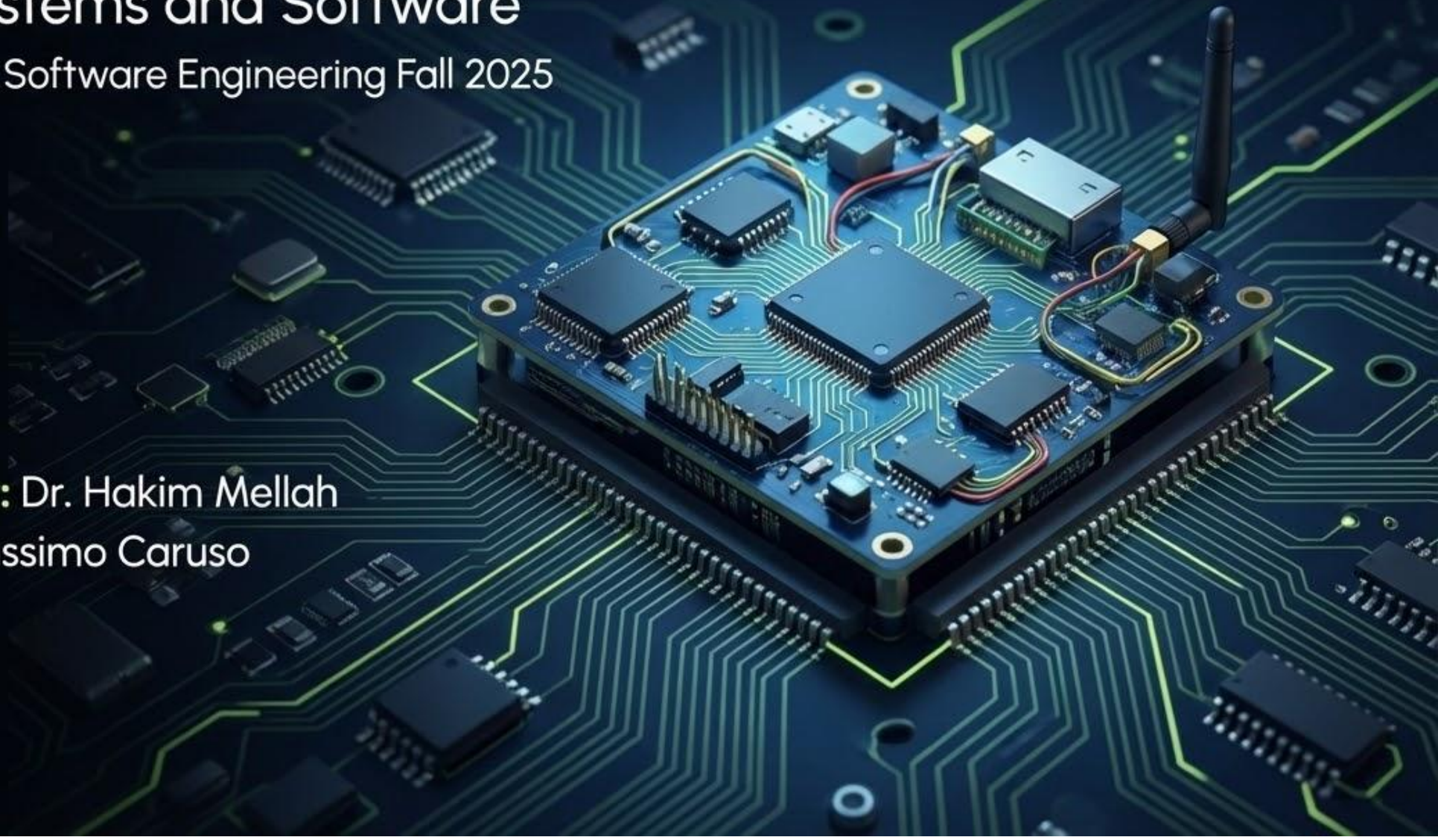
SOEN 422 Presentation

Embedded Systems and Software

Computer Science & Software Engineering Fall 2025



- **Course Instructor:** Dr. Hakim Mellah
- **Presented by:** Massimo Caruso (40263285)

Problem & The Sentinel Solution

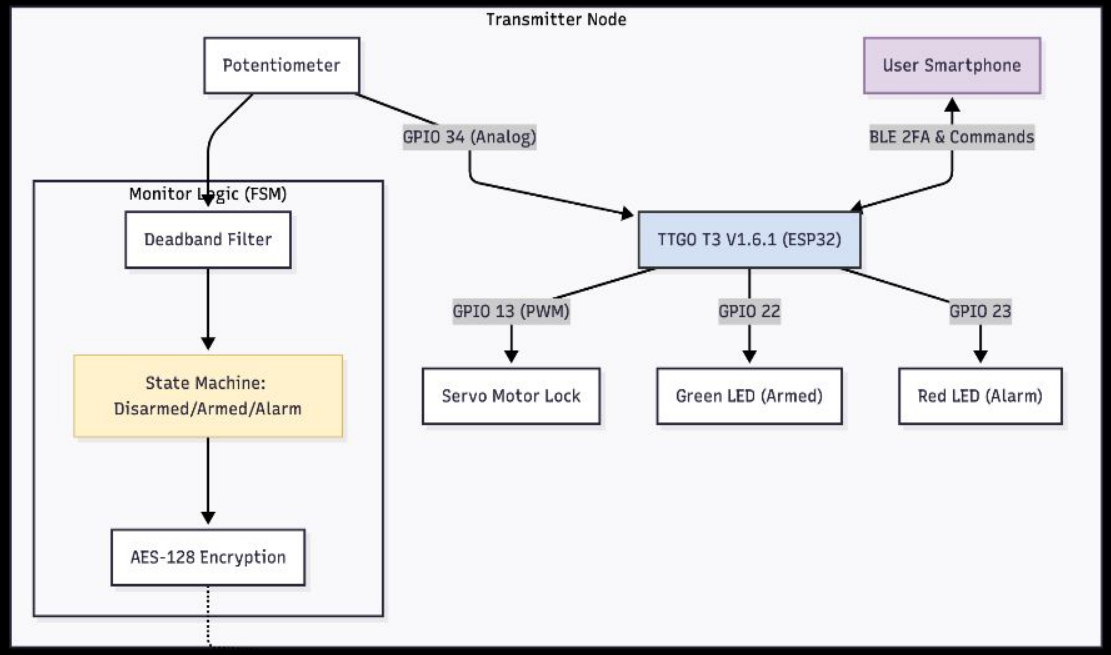
The Challenge

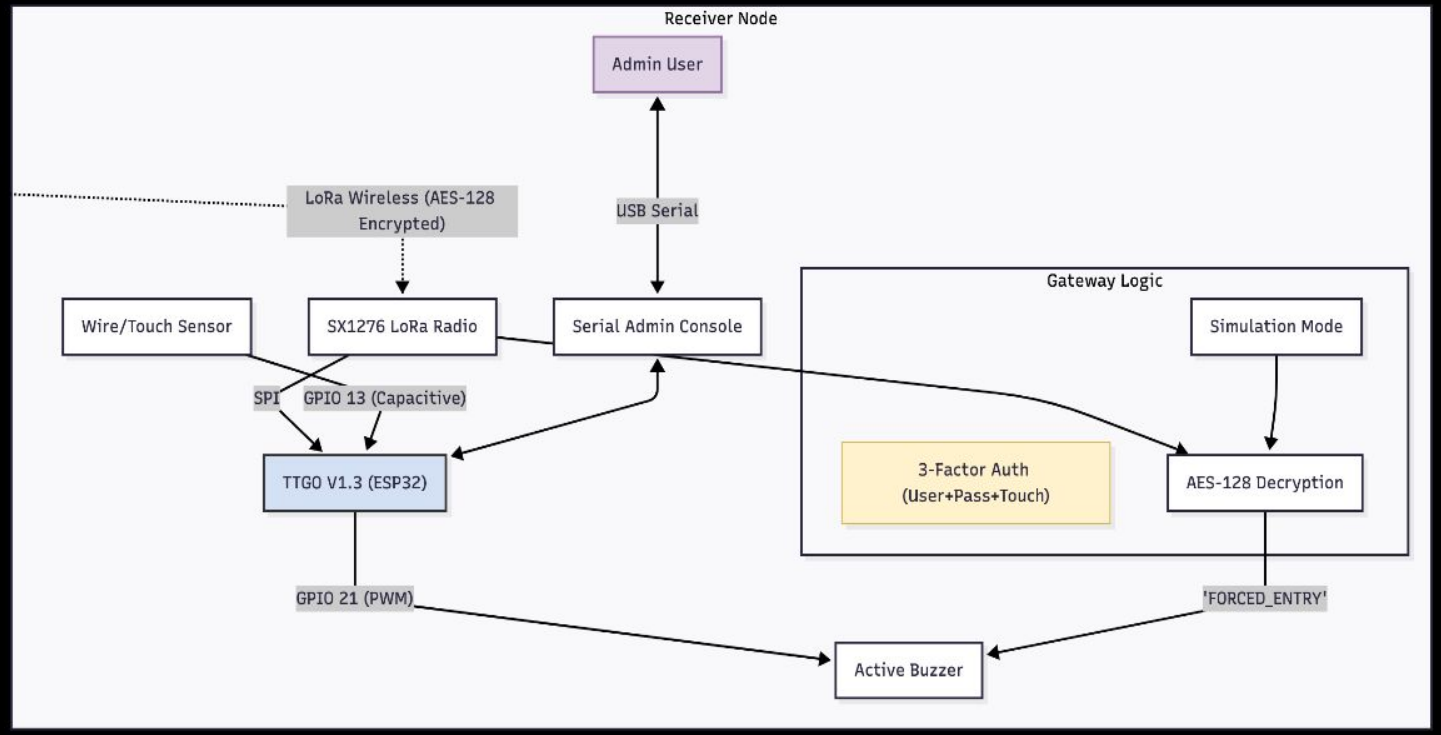
University labs house sensitive assets where standard keys lack audit trails, and Wi-Fi security is vulnerable to power/network outages.

The "Air-Gapped" Solution

- **Independent Network:** Uses a private LoRa (Long Range) link, ensuring security even when campus Wi-Fi is down.
- **Smart Actuation:** A Servo-based lock that allows manual control via potentiometer when disarmed, but rigidly locks when armed.
- **Robust Access Control:**
  - **Mobile:** BLE Challenge-Response (2FA).
  - **Admin:** Serial Console with Physical Biometric Touch.

Architecture: Functional Block Diagram of the System



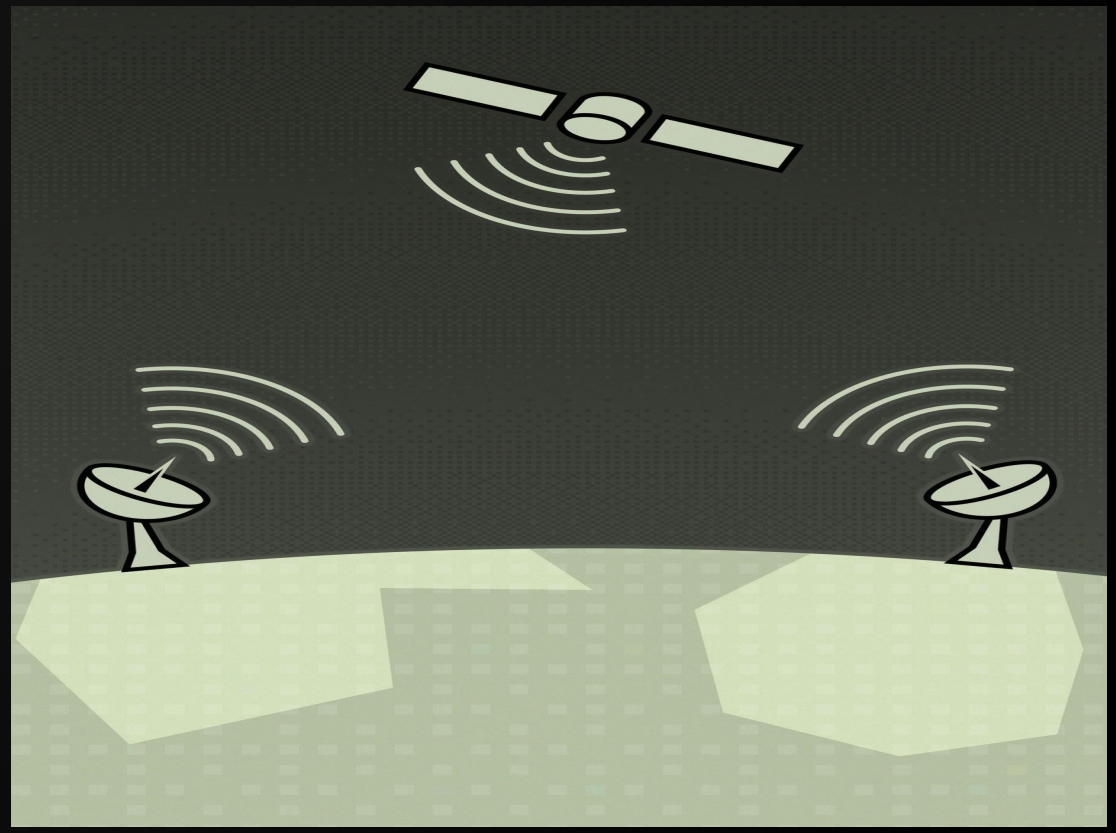


Architecture: Monitor Node (Transmitter)

Core Logic: Non-Blocking FSM

The system runs on a Finite State Machine (FSM) to manage concurrency without hanging.

- **States:** Locking → Armed → Alarm → Waiting_2FA → Disarmed.
- **Precise Sensing:** Potentiometer input uses *Deadband Filtering* (30 units) and Averaging (10 samples) to eliminate jitter and false positives.
- **Servo Control:**
  - *Disarmed:* Follows user's manual dial rotation.
  - *Armed:* Locks to 0°. Detection of any movement triggers "Forced Entry".



Architecture: Gateway Node (Receiver)

Secure Admin Interface

Designed for resilience, the Gateway abandons fragile web servers for a robust Serial Admin Console.

- **Authentication:** Requires *Admin Credentials + Physical Biometric Touch* (Capacitive Sensor on Pin 13) simultaneously.
- **3-Strike Lockout:** Failing to authenticate 3 times locks the system for 60 seconds to prevent brute-forcing.
- **Alerts:** Decrypts AES-128 LoRa packets and triggers an Active Buzzer (Pin 21) upon "Forced Entry".

Design Assessment & Reflections

Dimension	Critical Reflections & Implementation
Reliability	**Decision:** Switched from Web Server to Serial Console to prevent ESP32 heap fragmentation and WiFi timeouts. Implemented **Non-Blocking logic** to allow simultaneous Servo/LoRa/BLE operations.
Security	**Defense in Depth:** Uses AES-128 for data secrecy. Implemented a **3-Strike Lockout** on both BLE and Admin Console to stop brute-force attacks. Removed "Tamper Check" during 2FA entry to prevent infinite lockout loops.
Safety	**Fail-Safe:** System defaults to "Disarmed" (Potentiometer Control Enabled) on power-up to ensure manual access is possible if logic fails.
Ethical	**Privacy:** Biometrics are simulated via local capacitive touch thresholds, ensuring no actual personal data (fingerprints) is stored or transmitted.