Requirements Engineering

Access Control System with Face Biometrics and QR Code

Szymon Manijak, Szymon Leśniak, Maciej Rybak

January 27, 2026

1 System Goal

The goal of the system is to increase security and ensure reliable registration of employee entries into the factory premises by combining two authentication mechanisms:

- scanning an access pass in the form of a QR code,
- employee identification based on facial analysis.

The system aims to eliminate abuses involving sharing access passes, ensure reliable work time tracking, and provide reports on effectiveness and incidents.

2 Stakeholders

Stakeholder	Role Description
Factory Management	Expects a reduction in abuse and improved security
HR Department	Uses data for work time calculation
Security Department	Supervises entries and responds to incidents
System Administrator	Manages permissions and configuration
Employees	Use access passes and are subject to verification
IT Service / Provider	Carries out implementation and system maintenance

3 Glossary

Access Pass / QR Code – An individual code assigned to an employee.

Biometric Verification – Face identification based on an image from the camera.

Abuse – Entry inconsistent with permissions or falsification of identity.

Incident – A failed or suspicious entry attempt.

Employee Register – A database of persons authorized to enter.

Effectiveness Report – A summary of correct and incorrect entries and statistics.

4 Functional Requirements (FR)

4.1 Entry Mechanisms

FR1 – The system enables scanning of a QR pass.

FR2 – The system captures a facial photo during scanning.

FR3 – The system compares the face with the employee database.

FR4 – Access is granted only upon QR + biometric match.

FR5 – The system detects mismatches (e.g., face $\neq$ QR owner).

FR6 – The system records every entry attempt.

4.2 Employee and Permission Management

FR7 – Adding and removing employees.

FR8 – Managing entry permissions.

FR9 – Storing reference photos.

4.3 Reporting Module

FR10 – Entry report (by dates, employees).

FR11 – Incident and mismatch report.

4.4 Incident Management

FR12 – Automatic incident detection.

4.5 Logging and Audit

FR13 – Storing logs.

5 Non-functional Requirements (NR)

5.1 Performance

NR1 – Full verification $\leq$ 5 seconds.

NR2 – System availability minimum 90%.

NR3 – Handling a minimum of 10 consecutive entries in a short interval.

6 Constraints

C1 – Storage of the minimum required amount of biometric data.

7 Use Cases (UC)

7.1 UC1: Standard Employee Entry

Actor: Employee
Description:

1. Employee scans QR code.
2. System takes a facial photo.
3. System checks QR + face compatibility.
4. Access granted, event saved.

7.2 UC2: Entry Attempt with Mismatched Face

Actor: Unauthorized person / Employee
Description:

1. QR code correct.
2. Face mismatched.
3. Access denied.
4. Incident created and security notified.

7.3 UC3: Employee Management

Actor: Administrator
Description:

1. Add a new employee.
2. Grants access and sets a reference photo.
3. System saves the data.

7.4 UC4: Incident Review

Actor: Security Department
Description:

1. Display incident list.
2. Review photos and data.

8 Risks and Threats

Risk	Description	Mitigation
R1	Privacy concerns	Encryption, data retention policy
R2	Employee resistance	Communication and training
R3	Slow verification	Optimization + powerful hardware

9 Additional Agreements Questions Asked During The Meeting

The following list contains answers to questions asked to the client to clarify the system requirements.

Question: What essential data needs to be stored in the database? Answer: The database must store input data (facial images, employee data linked to QR codes) and report data (correct and incorrect entries with metadata).

Question: At what point should the scanning take place? Answer: QR code scanning happens before facial recognition occurs.

Question: How should the clocking-in system work (the rules)? Answer: The system registers every entry attempt. A correct verification (matching QR + matching face) is logged as a "correct entry". Any mismatch (e.g., incorrect face) is logged as an "incorrect entry" (incident).

Question: What will the hardware platform be? Answer: The target hardware platform is a laptop equipped with a CPU/GPU and an integrated camera.

Question: What data will be reported? Answer: Reports will include:

- **Correct Entries:** date, time, Employee ID.
- **Incorrect Entries (Incidents):** reason for denial (e.g., incorrect face), date, time, Employee ID associated with the used QR code.

Question: How many employees does the system need to support? Answer: The system must be prepared to support up to 20 employees.

Question: What is the maximum processing (verification) time? Answer: Full verification (QR + face) should not exceed 5 seconds. *(Note: This answer updates requirement NR1 from 2 seconds to 3 seconds).*

Question: What is the required identification accuracy? Answer: The system must achieve an accuracy rate of at least 90%.

Question: How long should the reports be stored? Answer: Reports (entry and incident logs) must be stored for 6 months.

Question: What is the deadline for delivering the documentation? Answer: Full system documentation must be delivered within 2 weeks.