Problem Statement: Secure Vault Access System using FSM

Scenario:

A high-security research facility needs a digital access control system for its vault. The system should allow access only if a 4-bit security code is entered correctly twice in a row. Additionally, to enhance security, a biometric sensor provides an 8-bit authentication code that must also match a stored value before access is granted.

System Requirements:

Inputs:

1. Security Code (A3 A2 A1 A0) – A 4-bit user input entered sequentially.

2. Clock (CLK) – Controls the system operation and transitions.

3. Reset (RST) – Resets the entire system to the initial state.

4. Biometric Authentication (B7 B6 B5 B4 B3 B2 B1 B0) – An 8-bit authentication value that must match a predefined stored value (BIO_REF).

5. Enter Key (ENTER) – Confirms each security code entry.

Outputs:

1. Access Granted (ACCESS) – Goes HIGH (1) when both the correct security code is entered twice in a row and biometric authentication is successful.

2. Access Denied (FAIL) – Goes HIGH (1) if a wrong security code is entered, resetting the system.

3. State Indicator (STATE[2:0]) – Represents the current state for debugging purposes.

Additional Constraints:

1. Optimization Focus:

- Minimize the number of states for efficiency.
- Implement using JK or D Flip-Flops instead of latches.

2. Security Features:

- After 3 consecutive failures, the system locks for 30 seconds (use a counter-based delay).

- The biometric sensor must be sampled only after correct code verification to reduce power consumption.