Elevator Control Logic - Formal Verification Test Cases

Test Case 1: Unreachable or Delayed Target Floor (L2)

Initial Conditions:

Elevator is currently at the top floor (d0 = 3).

Elevator is idle (DIR = #OFF).

No landing calls are active except for a down request at L1.

Car call for L2 is active.

Verification Goal:

Check whether the elevator can reach L2 within 15 steps.

LTL Specification:

VERIFY: [steps <= 15] (state == "L2 reached")

Purpose:

To detect flaws where internal requests like L2 are ignored or delayed due to incorrect logic.

Test Case 2: Priority Handling with Multiple Requests

Initial Conditions:

Elevator is at the second floor (d0 = 2).

Elevator is moving up (DIR = #UP).

Up landing call at L0 and down landing call at L3.

No car calls are active.

Verification Goal:

Ensure the elevator prioritizes requests in its current direction.

LTL Specification:

VERIFY: G(steps <= 15 => DIR == #UP -> PRIORITY(L3_request))

Purpose:

Ensure proper direction-based request handling to avoid servicing irrelevant calls like L0.

Test Case 3: Handling of Duplicate Requests on Same Floor

Initial Conditions:

Elevator is at the third floor (d0 = 3).

Elevator is idle (DIR = #OFF).

Car call for L2 is active.

Down landing call at L3 is active.

Verification Goal:

Ensure that redundant service calls on the same floor are avoided.

LTL Specification:

VERIFY: G(d0 == target_floor -> !REDUNDANT_CALLS)

Purpose:

Detect and prevent inefficient behavior due to repeated handling of already-serviced requests.

Test Case 4: Direction Switching Deadlock

Initial Conditions:

Elevator is at the first floor (d0 = 1).

Elevator is moving down (DIR = #DOWN).

Up landing calls are active at L2 and L3.

No car calls.

Verification Goal:

Ensure the elevator can eventually switch direction and reach L3 within 15 steps.

LTL Specification:

VERIFY: F(steps <= 15 -> reachable(L3))

Purpose:

Test direction-switching logic to avoid deadlocks or delays at bottom floor.

Test Case 5: Looping Movement Between Floors

Initial Conditions:

Elevator is at the second floor (d0 = 2).

Elevator is moving up (DIR = #UP).

Down landing call at L2.

Car calls at L0 and L3.

Verification Goal:

Ensure the elevator does not oscillate between L2 and L3.

LTL Specification:

VERIFY: G(steps <= 15 -> !LOOP(d0 = L2, d0 = L3))

Purpose:

Identify inefficiencies caused by poor priority or direction-switch logic.