16 The lift controller case study

Note that this case study is entirely fictional and doubtless over-simplifies real lift systems.

16.1 Elicitation notes

Notes for just one of a series of (imaginary) interviews are given here. A move to simulate the poorly ordered and presented nature of such notes has been made, but there is some compromise towards comprehensibility!

Client - skyhi elevator co. Contact (technical) Jason Hukins 01202 489345, X 4783. I/v 15/6.

Previous s/w contractor unsatisfactory. (Late and buggy!) Full h/w details available. Looking for full spec by 1/10. Will pay instalment for spec and negotiate for the rest (Andy can cover this - needs to contact Geoff Shepperd (finance director).) H/w all to hand - full specs available (got copies). Interface blocks all operate at 0-5 V (20 mA) - direct port connection no prob.

Max 4 lifts per controller, max 20 floors. One lift per shaft (next generation won't be !). All lifts, same # of floors.

Requirements:-
All lifts (if >1) to be used approximately equally.

Lift only reverses direction if no outstanding lift calls in current direction (lift send-button inside lift, lift call-button outside lift !)

Must not change motor polarity whilst moving ! (It'll blow.)
In emergency, stop all motors (if poss.).

Lift calls should be serviced by the lift that will get there soonest (approx.). Tricksy to predict - could pick up more calls on the way.

Services calls in the order it gets there - not the order they are made.

Indicators:-
Light for each floor - one set in each lift + one set on each floor (all switch together - can treat as one set).
Switch on basis of nearest floor so one off, one on when about half way between.

Sensors:-
3 sets for each floor - warning either side + at. Go hi (5 V) when lift present (i.e. 20 cm either side). If stopping, send slow signal to motor within 0.3 secs of warning and stop 0.2 +/- 0.1 secs after at signal. (Stop delay has to be configurable.) Top and bottom floors only have one set of warning sensors. (Obviously?)

Lift must always stop when arriving at top or bottom!
Lift normally moves at 1.2 m/sec. In slow mode, 0.3 m/sec. Takes approx. 1 sec to slow (i.e. about 0.75 m) and moves about 0.15 m between stop signal and actually stopping.

Lift will stop at a floor if there is a lift-send or a lift call and moving right way or if top/bottom. -R

Doors:-
Doors cycle every time it stops. (Note - cannot cancel a request.)

Controller only needs to send open/close signal - doors handle the rest. Door sensors (just the one pair per lift) go hi when shut/open. Never move lift with doors open! -R

Also one block sensor per door but connects direct to door controller - we don't need to worry.

If lift call or send request while doors open or closing, open again and restart wait. (Wait is 4 secs +/- 0.5.) -R

Note max pins - each lift fast, slow, direction (3 out) + sensors, (#floors x 3) -2 (all in) + indicators (#floors, out) + doors, close/open + closed/opened (2 out, 2 in).

To start lift go straight to fast, to stop must go to slow first (except in emergency? - he'll check). -R

Next wed - 10:00 - ring on Tue to confirm.

16.2 Requirements document

16.2.1 Problem domain

16.2.1.1 Overview

A software-based system is required to control lifts (elevators) manufactured by Skyhi Lifts. Lifts are constrained to shafts (one lift per shaft) and are moved up and down by winding motors (one winding motor per lift).

Users can call a lift to a floor by pressing buttons outside the lift (call-buttons) and can send lifts to a floor by pressing buttons inside the lift (send-buttons). There are indicators to show the users the current floor of each lift.

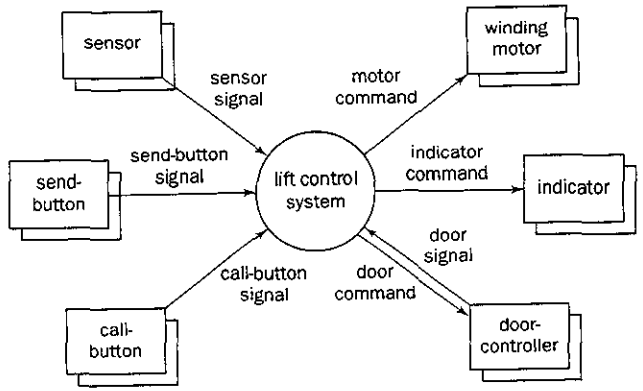


Figure 16.1

Context diagram (Figure 16.1)

All signals to and from the lift system components are via electric cables. All signals operate upon a hi/lo basis where hi is within the range 3–5 V and lo is < 1 V. Maximum draw-down current is 20 mA. All input signals (i.e. from the terminators to the control system) may take up to 10 milliseconds to stabilise within the specified ranges.

16.2.1.2 Problem frame

The problem frame is shown in Figure 16.2. (It may be supposed that there is also a relationship between users and the door mechanism, since the doors can

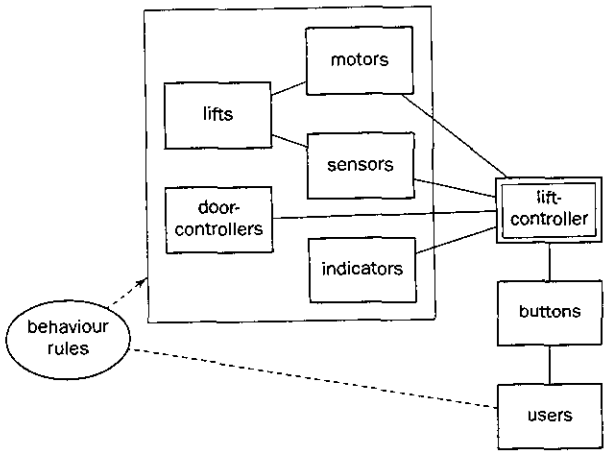


Figure 16.2

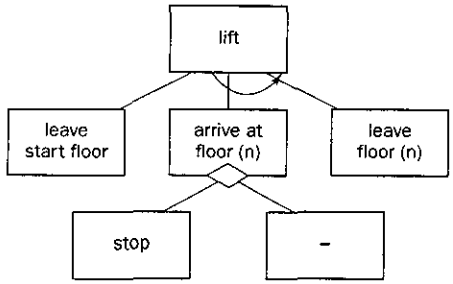


Figure 16.3

sense if a user is obstructing closure and will re-open. However, this is handled entirely by the door-controller and so is beyond the scope of the lift-controller.)

16.2.1.3 Lifts

A lift is constrained to move vertically up and down in its lift shaft. It follows that when a lift leaves a floor, the next floor it arrives at will be an adjacent floor or, possibly (if it reverses direction between floors), the same floor. This is illustrated in Figure 16.3.

16.2.1.4 Winding motors

Winding motors each have three control lines; slow, fast and polarity – which operate as per the decision table below (Table 16.1).

In fast mode, the motor moves the lift at 1.2 m/sec (+/– 10%). In slow mode, at 0.3 m/sec (+/– 10%). The motor mechanism itself ensures a gradual acceleration and deceleration as per Table 16.2.

16.2.1.5 Buttons

Whilst pressed, buttons produce a hi signal (when released, a lo signal). Within each lift there is a set of send-buttons, one for each floor. On each floor, outside

Table 16.1

slow	hi				lo			
fast	hi		lo		hi		lo	
polarity	hi	lo	hi	lo	hi	lo	hi	lo
wind up fast	✓				✓			
wind down fast		✓				✓		
wind up slow			✓					
wind down slow				✓				
stop							✓	✓

Table 6.2

	time	distance
rest to fast	2 sec	1.2 m
fast to slow	1 sec	0.75 m
slow to rest	1 sec	0.15 m

(All figures are subject to a tolerance of +/– 20%.)

the lifts, there is a set of call-buttons. This set consists of two buttons for each floor (one up call-button and one down call-button), except for the bottom floor, which has an up call-button only, and the top floor, which has a down call-button only. (There may actually be more than one set of call-buttons on each floor but, if so, they are linked and will appear to the controller as one set.)

16.2.1.6 Indicators

Indicator sets consist of one indicator light for each floor that the lift system services. For each lift there is a set of indicators inside it and a set on each floor outside it. For each lift, the two are linked and will appear to the controller as one set.

16.2.1.7 Sensors

Sensors detect the presence of a lift. When a lift is within 20 cm vertically (either side) of the sensor's nominal position it sends a hi signal; otherwise a lo signal. Each lift shaft has a set of sensors for each floor. For each floor (except top and bottom), there is a proximity-sensor (aka the 'at-sensor') at the nominal floor position, an above-sensor 1.5 m above (the nominal floor position) and a below-sensor 1.5 m below. The top floor has proximity- and below-sensors only and the bottom floor proximity- and above-sensors only.

16.2.1.8 Door-controllers

The doors on each lift have their own, in-built controller which handles door cycling (i.e. opening, waiting and closing), including re-opening when obstructed. (Through a mechanical linkage, the doors on the floor that the lift is on are automatically operated together with the doors of the lift itself.)

Doors will commence cycling upon receipt of a cycling signal (i.e. the door cycle line is sent hi for at least 0.1 seconds). A door controller sends a hi signal when the doors are closed; otherwise it is lo.

16.2.1.9 Users

Users are members of the general public. The majority of their characteristics (e.g. comfort under vertical acceleration, ability to reach and press buttons, time to enter/leave lifts, etc.) are already accommodated by the given hardware (including the door-controller).

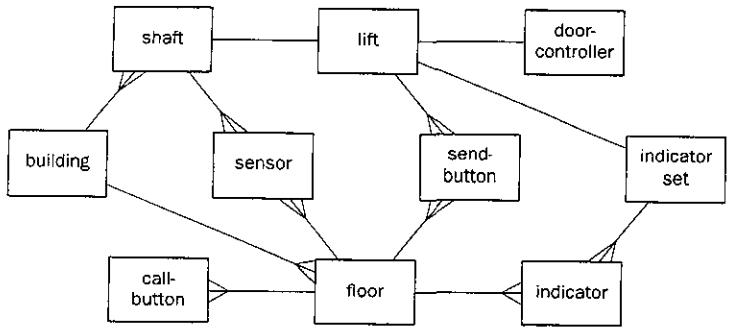


Figure 16.4

Additionally, it has been determined that, typically:

- Users report mild annoyance after a 20 second wait for a lift.
- If, from the indicators, it appears that, in response to a call-button request, no lift will arrive for at least 30 seconds, 50% of users will use the stairs for up to two floors.

16.2.1.10 Summary of sub-domain relationships

There are the following:

- many floors to each shaft;
- one lift to each shaft;
- one door controller to each lift;
- three sensors (above, at, below) per floor per shaft, except for top (at, below) and bottom (above, at) floors;
- one indicator set per lift;
- one indicator per floor per indicator set;
- one send-button per lift per floor;
- two call-buttons (one up, one down) per floor, except for top (down only) and bottom (up only) floors.

16.2.1.11 Entity relationship diagram

This is shown in Figure 16.4 above.

16.2.1.12 Data dictionary

```
building            ::= number-of-floors, number-of-lifts;
floor               ::= floor-id;
shaft               ::= lift-id;
hi-lo               ::= hi | lo;
hi                  ::= /* signal is "hi", i.e. 3 to 5 volts */;
lo                  ::= /* signal is "lo", i.e. < 1 volt */;
on-off              ::= on | off;
on                  ::= /* device is "on" (e.g. a button is pressed) */;
off                 ::= /* device is "off" */;

lift                ::= lift-id, direction, position;
direction           ::= "up" | "down";
position            ::= floor-id;

door-controller     ::= lift-id;
door-command        ::= hi-lo;
                    ::= /* "hi" starts lift door opening */
door-signal         ::= hi-lo;
                    ::= /* "hi" indicates that door is closed */

sensor              ::= lift-id, floor-id, sensor-type, on-off;
sensor-type         ::= "above" | "at" | "below";
sensor-signal       ::= hi-lo;
indicator-set       ::= {indicator};
indicator           ::= lift-id, floor-id, on-off;
indicator command   ::= hi-lo;

call-button         ::= floor-id, direction, on-off;
send-button         ::= lift-id, floor-id, on-off;
send-button-signal  ::= hi-lo;
call-button-signal  ::= hi-lo;

winding motor       ::= lift-id;
motor-command       ::= slow, fast, polarity;
slow                ::= hi-lo;
fast                ::= hi-lo;
polarity            ::= hi-lo;
```


16.2.2 Requirements

16.2.2.1 Safety

R1 The lift is never to be allowed to move above the top floor or below the bottom floor. (There is an emergency shut down system that will stop the motor if the lift goes above the top floor or below the bottom floor (by more than 10 cm), but this shut down system is beyond the scope of the control system.)

R2 The lift is not to be stopped from fast mode but should always be switched to slow mode for at least one second before stopping.

R3 The motor polarity is not to be changed whilst the lift is moving. (This could wreck the winding gear.)

R4 The lift is never to be moved with the doors open.

R5 With the stop-delay correctly configured (as below) the lift will stop within +/– 1.5 cm of the floor being serviced.

16.2.2.2 Call servicing

R6 A call is established by pressing a send-button (inside the lift) or a call-button (outside the lift) for the relevant floor and, in the case of call-buttons, for the relevant direction. (Duplicate calls are ignored.)

R7 Calls are cancelled only when serviced by a lift.

R8 To service a send-button call, the relevant lift must stop at that floor. A call-button call may be serviced by any lift that is travelling in the correct direction stopping at that floor.

R9 A lift will stop at a floor if:

R9.1 there is a send-button call for that floor or

R9.2 there is call-button call and the lift is moving in the right direction or

R9.3 if it is the top or bottom floor

Where there is more than one lift:

R10 Send-button calls must be serviced by the relevant lift.

R11 Call-button calls should be serviced by the lift that is likely to arrive there soonest. (It is appreciated that this cannot be guaranteed because the selected lift might be requested to service a new call whilst en route.)

R12 Each lift should be used an approximately equal amount.

R13 A lift will reverse direction only when stopped at a floor.

R14 A lift will reverse direction only if it has no outstanding calls in its current direction of travel.

R15 For each lift, one indicator at a time should be illuminated, that being the one for the floor that the lift is (approximately) nearest to.

16.2.2.3 Configuration

R16 The service technician must be able to set:

R16.1 number of lifts

R16.2 number of floors

R16.3 stop signal delay, for each lift (in the range 0.10 to 0.40 seconds)

16.2.2.4 Performance

R17 The maximum number of lifts is four, the minimum one.

R18 The maximum number of floors is 20, the minimum two.

16.2.2.5 Reliability

R19 The control system should not violate any safety requirements. Non-safety critical control errors (e.g. lift sent to wrong floor) should not occur more than once per week of operation.

16.2.2.6 Physical environment

R20 The control system must fit within a volume of 1 × 0.5 × 0.5 m.

R21 The control system must operate over a temperature range of 0–40°C.

R22 RF emissions must comply with BS50081–2.

16.3 Specification

[Note, only the system behaviour section of the specification is given. To save space, the various standard, 'wrapper' parts (see Section 5.4.3) and replicated requirements are omitted.

Included (in call-outs) are indications of whereabouts the various requirements are addressed by the edesign. This is not usual (indeed, for some requirements it is virtually impossible since their realisation can be very 'diffuse') but may prove illuminating.]

16.3.1 Hardware interfaces

16.3.1.1 Ports and pins

The control system interfaces with the hardware via 32 pin ports.

- Port 1 is left spare.
- Ports 2 and 3 are allocated to call buttons.
- Starting with port 4, each lift is assigned 4 ports to be referenced as ports 4n, 4n+1, 4n+2, 4n+3, where n is the lift number (starting at 1).

Table 16.3 shows the pin allocations.

16.3.1.2 Event responses

Events occur when the following signals go hi:

- below-sensor-signal (l, f) – lift (l) is 150 cm (+/– 20 cm) below floor (f)
- at-sensor-signal (l,f) – lift (l) is at (+/– 20 cm) floor (f)
- above-sensor-signal (l) – lift (l) is 150 cm (+/– 20 cm) above floor (f)
- door-sensor-signal (l) – door is closed
- send-button-signal (l, f) – request to send lift (l) to floor (f)
- call-button-signal (f, d) – request for any lift to call at floor (f) and then proceed in direction (d)

and when the following signal goes low:

- door-sensor-signal (l) – door is opening/open/closing

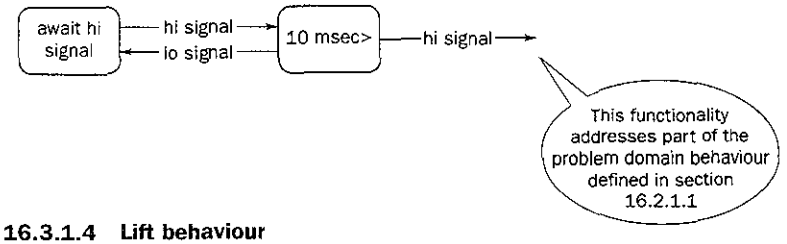
16.3.1.3 Signal de-bouncing

In order to allow for stabilisation, all input signals will be handled as below.

Table 16.3

Port	Purpose	Pin 0	Pin 1	Pin 2	Pin 3	...	Pin 29	Pin 30	Pin 31
1	spare								
2	up call buttons	floor 0	floor 1	floor 2	floor 3	etc. (to 20)	unused	unused	unused
3	down call buttons	unused	floor 1	floor 2	floor 3	etc. (to 20)	unused	unused	unused
4 (4n)	lift (1) sensors	unused	at 0	above 0	below 1	etc. (to 10)	above 10	unused	unused
5 (4n+1)	lift (1) sensors	below 11	at 11	above 11	below 12	etc. (to 20)	unused	unused	unused
6 (4n+2)	lift (1) indicators + motor	floor 0	floor 1	floor 2	floor 3	etc. (to 20)	motor slow	motor fast	motor polarity
7 (4n+3)	lift (1) send buttons + door	floor 0	floor 1	floor 2	floor 3	etc. (to 20)	unused	door sensor	door com'nd
8 (4n+1)	lift (2) sensors	unused	at 0	above 0	below 1	etc. (to 20)	above 10	unused	unused
etc.									

(Note, floor 0 is the bottom (ground) floor.)



16.3.1.4 Lift behaviour

Most of the responses to sensor signals and the door signal are captured in the following state chart (Figure 16.5) showing the emergent behaviour of a *single* lift[114].

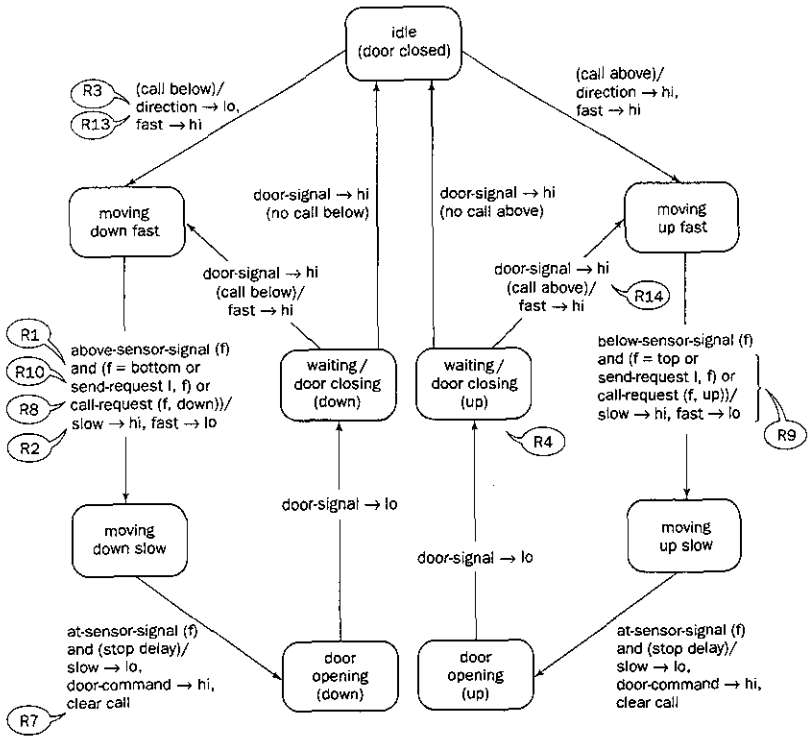
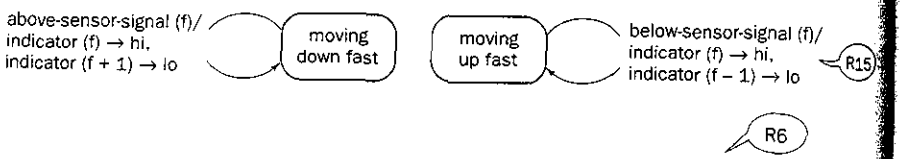


Figure 16.5

[114] [It may be observed that the given edesign is fairly simplistic. It would be possible, indeed, desirable, for the controller to check upon the progress of lifts by taking account of sensor signals going from hi to lo as well. For example, when a lift leaves floor(f) and goes upwards, the at-floor(f) sensor should go lo, followed by the above-floor(n) going lo before the below-floor(f+1) sensor goes hi. Any departure from this sequence would indicate a fault which could be reported. Further, from the known speeds of the lifts, it would also be possible to check that signals occur within expected time windows. Such sophisticated behaviour can be incorporated into finite state machine models but this is left to the reader as an exercise.]

In addition, the indicators are operated as per the following state charts:



Send-button-signals cause calls (above or below) to be allocated to the appropriate lift.

Where there is more than one lift, call-button-signals are handled in the following way:

R10

- Allocate the call to the lift with the shortest response time.
- If lifts have equal response times, then select one of those lifts randomly.

R8+R11

Response time for each lift is calculated as:

R12

(1.2 * floor-height (metres) * number-of-floors-to-travel) +
(number-of-stops-en-route * (waiting-time (seconds) + 8))

16.3.2 User interface

The user interface hardware (button panels and indicator panels) are pre-existing and so are not defined here. From the user perspective, the emergent behaviour of the system is reflected in the following use-case:

LIFT JOURNEY
User calls lift and travels to required destination floor.
Actors
User
Pre-conditions:
None
Post-condition:
The user will be at their required destination floor
Interaction

1. The user arrives outside a lift door and presses the relevant call-button
2. A lift arrives and the door opens
3. The user enters the lift
4. The user presses the send-button for the required destination floor
5. The door closes, the lift travels to the destination floor (possibly stopping at other floors en route) and the door opens
6. The user exits the lift

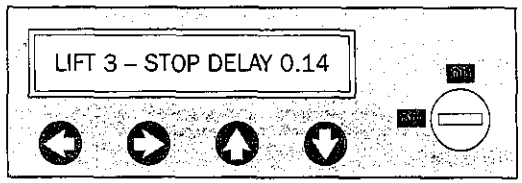


Figure 16.6

16.3.3 Technician interface

R16

The service technician can configure:

- number of lifts;
- number of floors;
- stop signal delay, for each lift (in the range 0.10 to 0.40 seconds).

Figure 16.6 illustrates (approximately to scale) the configuration panel which consists of a 30 character display and four buttons (left, right, up, down). There is also a key operated switch which must be switched to on in order to be able to change configuration.

The sequence of operation is depicted in the state chart (Figure 16.7).

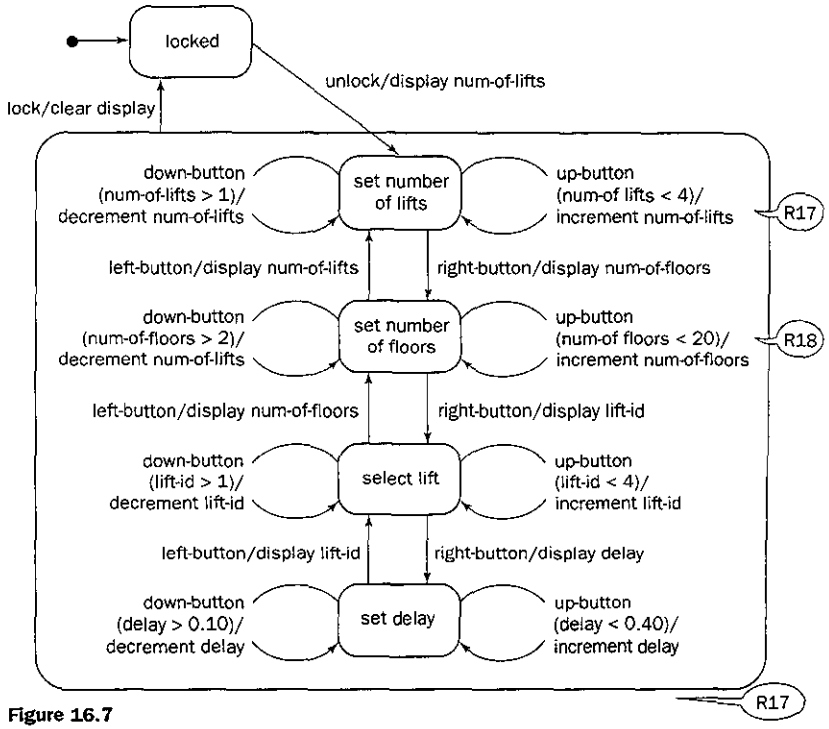


Figure 16.7