엘리베이터
SMV Model Checking

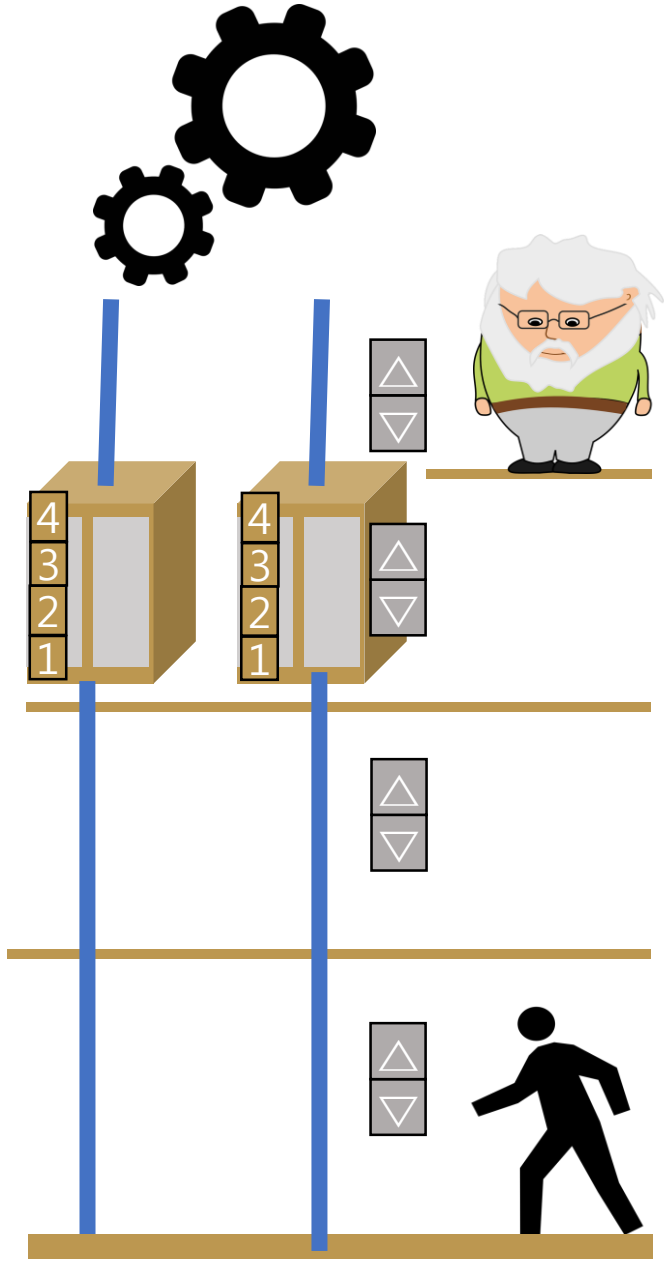
Konkuk Univ. IT융합정보보호학과
박선영, 오예원

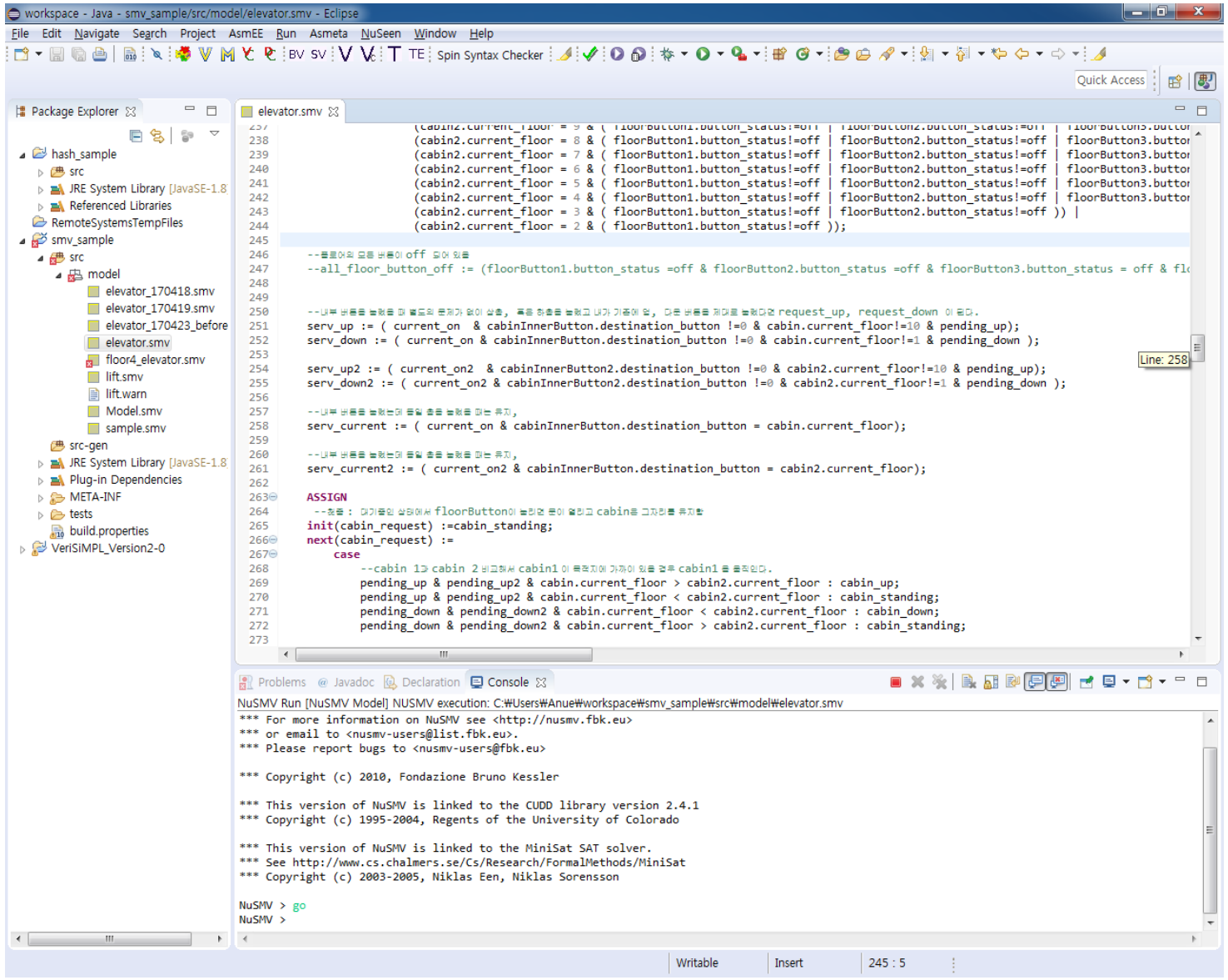
목차

- 엘리베이터 상태/변수 추출
- 요구사항(제약사항)
- 객체 간 관계
- State
- Variable
- Property
- 향후계획

상태/변수 추출

- Floor
  - Floor Button(x20) : request_up, request_down, false
- Cabin(x4) – 상층(1,11-20), 저층용(1-10)
  - Current_floor: 1..10 / 1..20
  - Direction : standing, moving_up, moving_down
  - Destination Button : 1..10 / 1,11..20
  - Door_request / Door
- Cabin Inner Button(x4) ㄱ
- Control(x2) – 상층, 저층용
  - Current_on / pending_up,down / serv_up,down
  - Cabin_request
- Door(Cabin 안에 포함)
  - Status : open, close



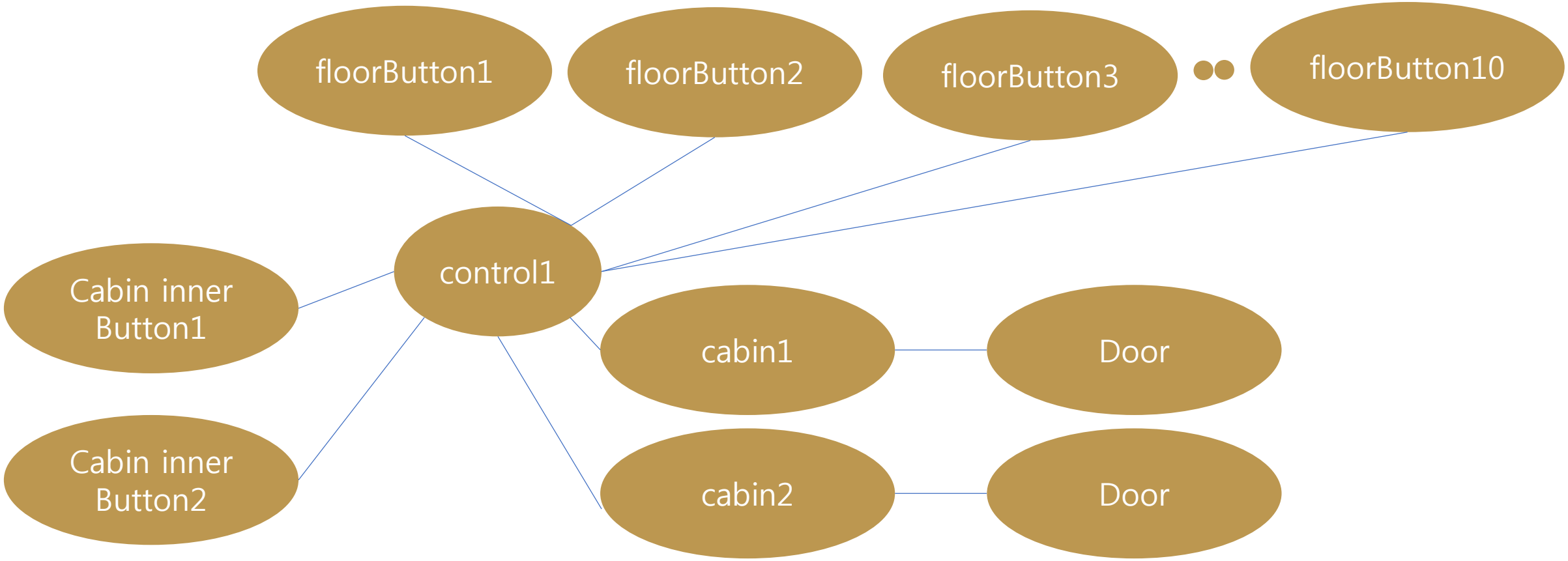

workspace - Java - smv_sample/src/model/elevator.smv - Eclipse
File Edit Navigate Search Project AsmEE Run Asmeta NuSeen Window Help
Spin Syntax Checker
Quick Access
Package Explorer
hash_sample
src
JRE System Library [JavaSE-1.8]
Referenced Libraries
RemoteSystemsTempFiles
smv_sample
src
model
elevator_170418.smv
elevator_170419.smv
elevator_170423_before
elevator.smv
floor4_elevator.smv
lift.smv
lift.warn
Model.smv
sample.smv
src-gen
JRE System Library [JavaSE-1.8]
Plug-in Dependencies
META-INF
tests
build.properties
VeriSiMPL_Version2-0
elevator.smv
(cabin2.current_floor = 8 & (floorButton1.button_status!=off | floorButton2.button_status!=off | floorButton3.buttor
(cabin2.current_floor = 7 & (floorButton1.button_status!=off | floorButton2.button_status!=off | floorButton3.buttor
(cabin2.current_floor = 6 & (floorButton1.button_status!=off | floorButton2.button_status!=off | floorButton3.buttor
(cabin2.current_floor = 5 & (floorButton1.button_status!=off | floorButton2.button_status!=off | floorButton3.buttor
(cabin2.current_floor = 4 & (floorButton1.button_status!=off | floorButton2.button_status!=off | floorButton3.buttor
(cabin2.current_floor = 3 & (floorButton1.button_status!=off | floorButton2.button_status!=off)) |
(cabin2.current_floor = 2 & (floorButton1.button_status!=off));
--플로어의 모든 버튼이 off 되어 있을
--all_floor_button_off := (floorButton1.button_status =off & floorButton2.button_status =off & floorButton3.button_status = off & flo
--내부 버튼을 눌렀을 때 별도의 문제가 없이 상승, 혹은 하강을 눌렀고 내가 기준에 왼, 다른 버튼을 제어로 눌렀다면 request_up, request_down 이 된다.
serv_up := (current_on & cabinInnerButton.destination_button !=0 & cabin.current_floor!=10 & pending_up);
serv_down := (current_on & cabinInnerButton.destination_button !=0 & cabin.current_floor!=1 & pending_down);
Line: 258
serv_up2 := (current_on2 & cabinInnerButton2.destination_button !=0 & cabin2.current_floor!=10 & pending_up);
serv_down2 := (current_on2 & cabinInnerButton2.destination_button !=0 & cabin2.current_floor!=1 & pending_down);
--내부 버튼을 눌렀는데 동일 층을 눌렀을 때는 유지,
serv_current := (current_on & cabinInnerButton.destination_button = cabin.current_floor);
--내부 버튼을 눌렀는데 동일 층을 눌렀을 때는 유지,
serv_current2 := (current_on2 & cabinInnerButton.destination_button = cabin2.current_floor);
ASSIGN
--현황 : 대기중인 상태에서 floorButton이 눌리면 문이 열리고 cabin은 그자리를 유지함
init(cabin_request) :=cabin_standing;
next(cabin_request) :=
case
--cabin 1과 cabin 2 비교해서 cabin1 이 목적지에 가까이 있을 경우 cabin1 을 움직인다.
pending_up & pending_up2 & cabin.current_floor > cabin2.current_floor : cabin_up;
pending_up & pending_up2 & cabin.current_floor < cabin2.current_floor : cabin_standing;
pending_down & pending_down2 & cabin.current_floor < cabin2.current_floor : cabin_down;
pending_down & pending_down2 & cabin.current_floor > cabin2.current_floor : cabin_standing;
Problems Javadoc Declaration Console
NuSMV Run [NuSMV Model] NUSMV execution: C:₩Users₩Anue₩workspace₩smv_sample₩src₩model₩elevator.smv
*** For more information on NuSMV see <http://nusmv.fbk.eu>
*** or email to <nusmv-users@list.fbk.eu>.
*** Please report bugs to <nusmv-users@fbk.eu>
*** Copyright (c) 2010, Fondazione Bruno Kessler
*** This version of NuSMV is linked to the CUDD library version 2.4.1
*** Copyright (c) 1995-2004, Regents of the University of Colorado
*** This version of NuSMV is linked to the MiniSat SAT solver.
*** See http://www.cs.chalmers.se/Cs/Research/FormalMethods/MiniSat
*** Copyright (c) 2003-2005, Niklas Een, Niklas Sorensson
NuSMV > go
NuSMV >
Writable
Insert
245 : 5

요구사항(제약사항)

- FloorButton(x20) :
  - 10층과 20층 에서는▲ 버튼을 누를 수 없다.
  - 1층에서는 ▼ 버튼을 누를 수 없다.
  - 무한히 ▲ 를 요청하거나, ▼ 상태만 요청 할 수 없음(언젠가는 대기 상태로 전환)
- Door :
  - 문은 운행 중간에 문이 열리면 안되며 오로지 대기 중에만 문이 열림.
  - 고층 엘리베이터의 경우 저층에 머물러 있을 때도 문이 열리면 안됨.
- Cabin
  - (저층)10층이면 더 올라갈 수 없음 / 1층이면 더 내려갈 수 없음
  - (고층) 11층이면 1층으로만 내려갈 수 있음 / 20층이면 더 올라갈 수 없음
  - (고층) 고층은 저층에서 머무를 수 없으며 별도의 요청이 없을 때는 1층으로 이동
- CabinInnerButton
  - 저층의 경우 1-10만 누를 수 있으며 고층의 경우 1,11-20만 누를 수 있음
- Control
  - (공통) 무한히 올라가는 cabin을 올려 보내는 상태이거나 내려 보내는 상태일 수 없음
  - (공통) FloorButton에서 요청 발생 시 저층 용 2개 중 가까운 위치인 것에 동작 하도록 처리(요구사항)

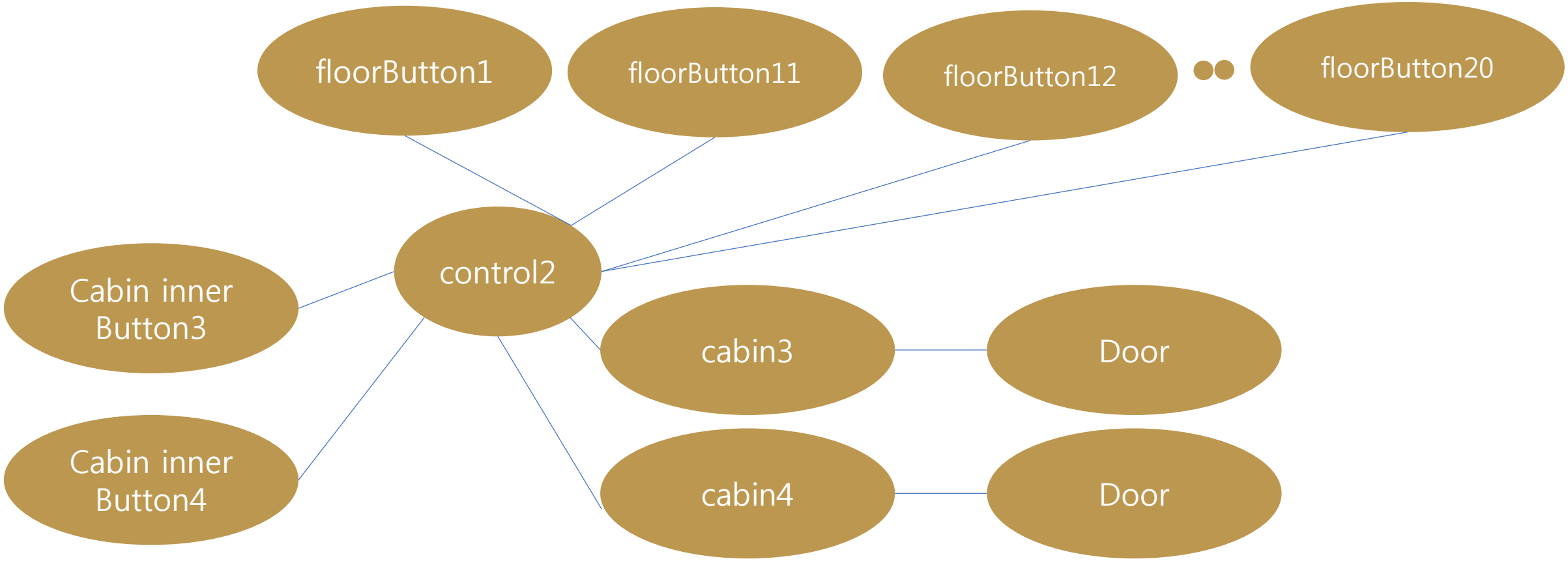
객체 간 관계

- 저층용

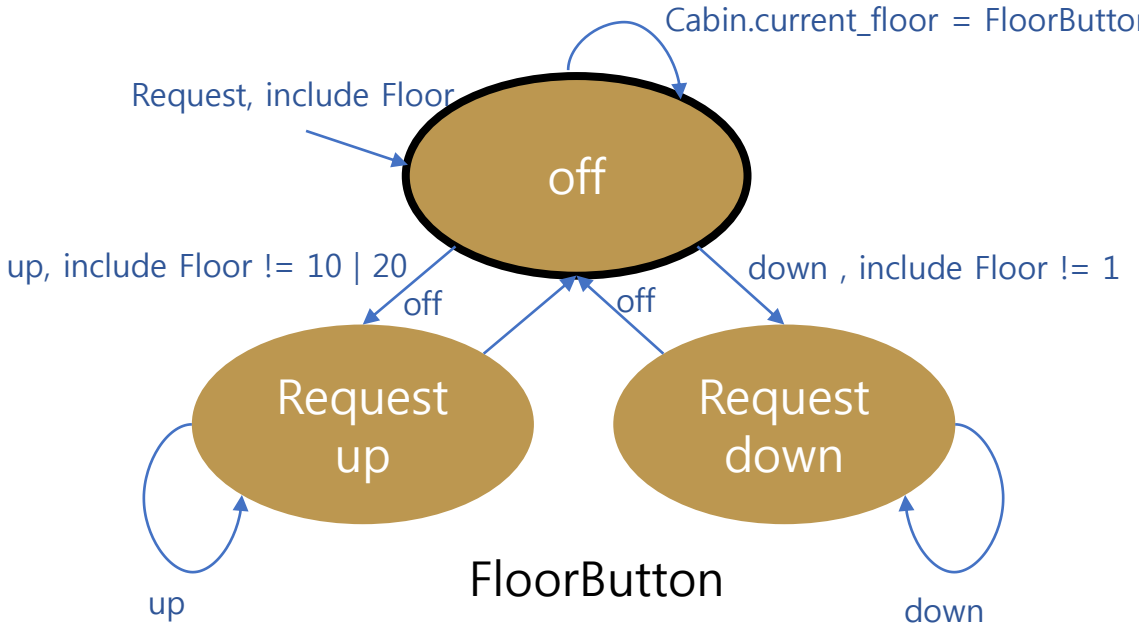

floorButton1
floorButton2
floorButton3
floorButton10
control1
Cabin inner Button1
Cabin inner Button2
cabin1
cabin2
Door
Door

객체 간 관계

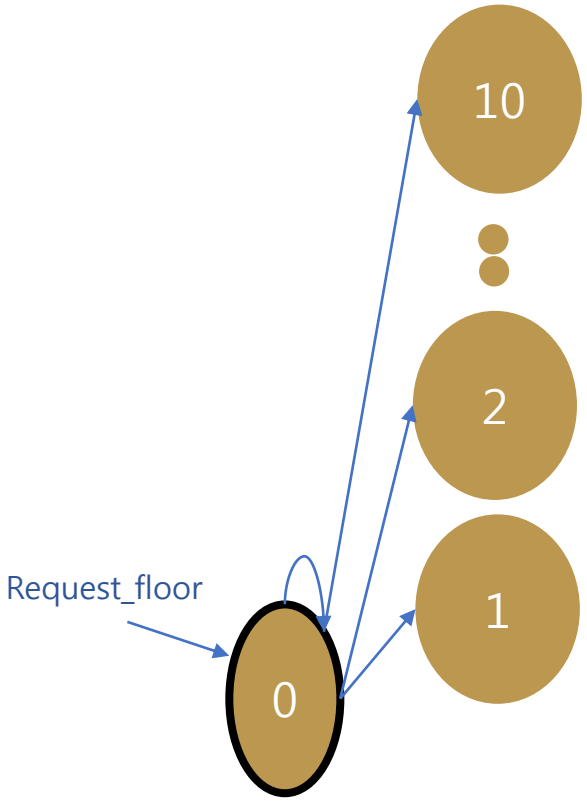
- 고층용


floorButton1
floorButton11
floorButton12
floorButton20
control2
Cabin inner Button3
Cabin inner Button4
cabin3
cabin4
Door
Door

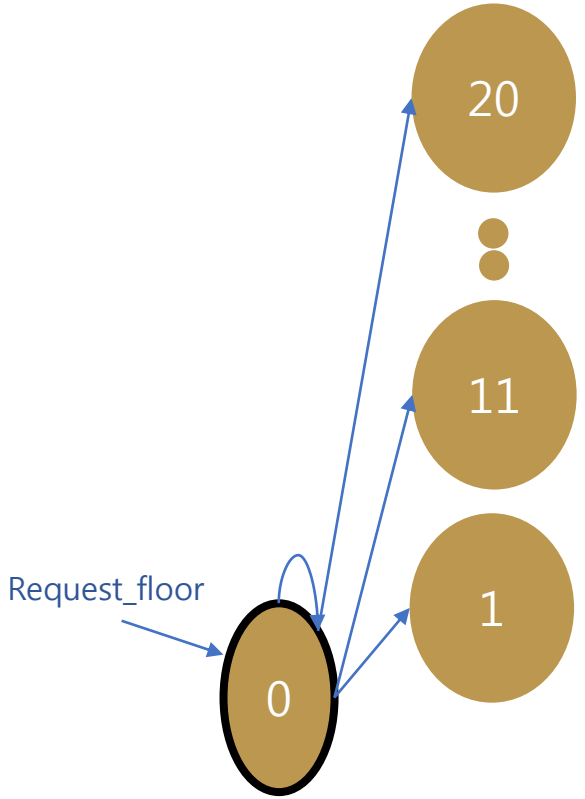
State : Floor Button / Cabin inner Button



FloorButton

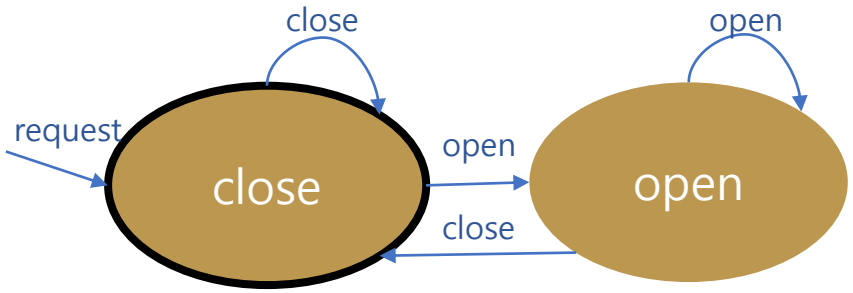


Cabin inner Button(저층)

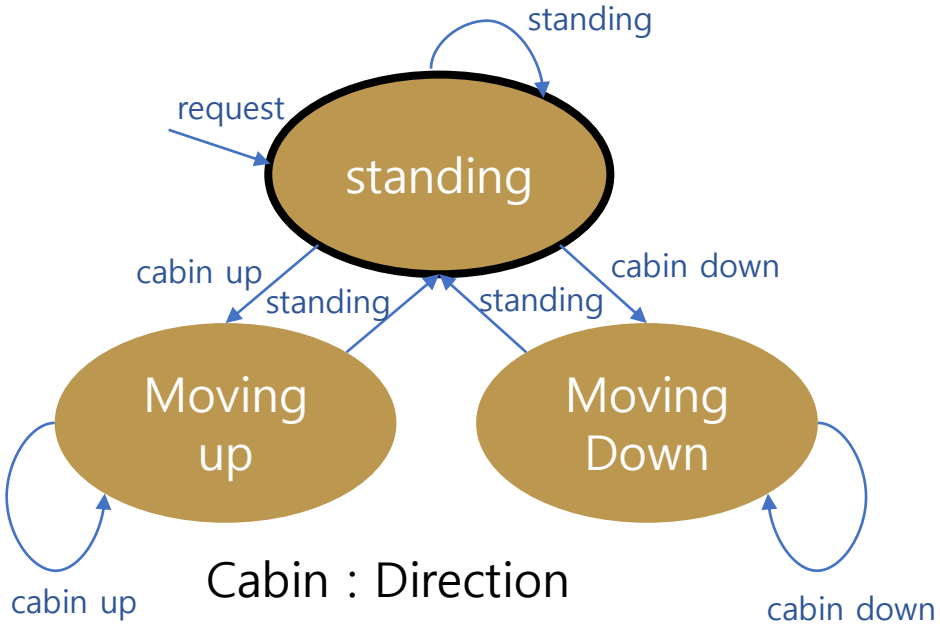


Cabin inner Button(고층)

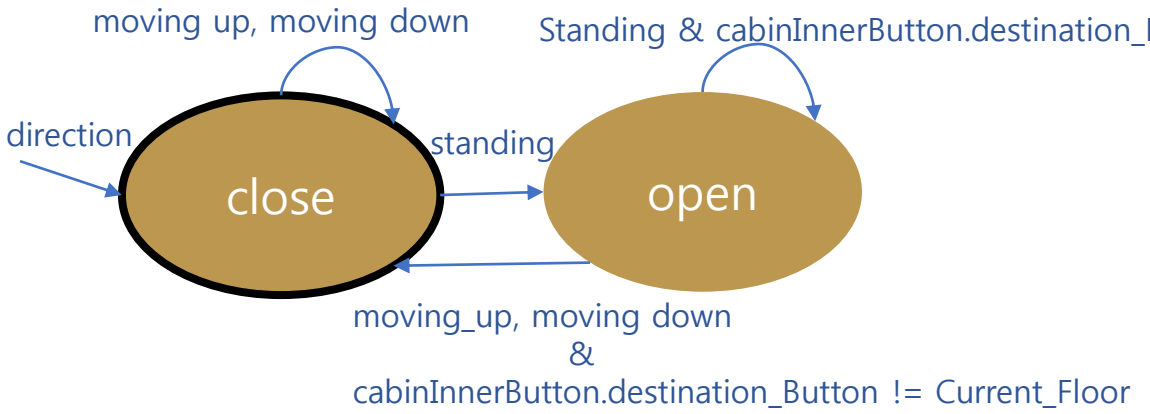
State : cabin(저층)



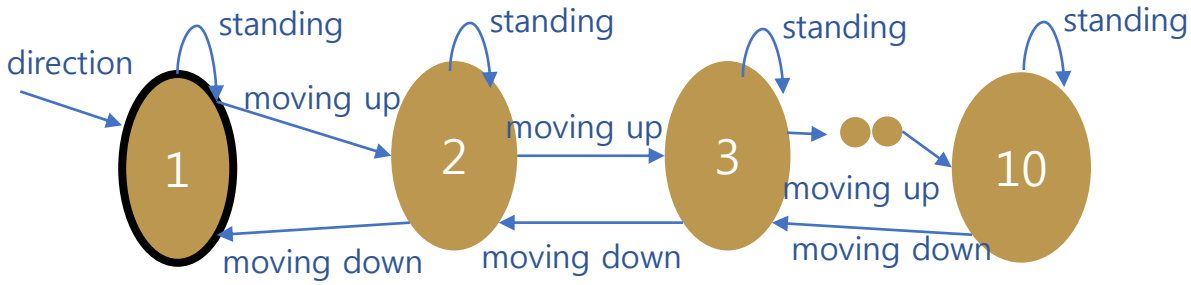
Door



Cabin : Direction

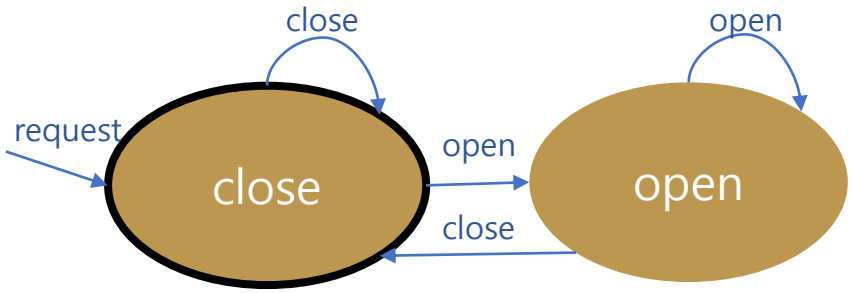


Cabin : Door_request

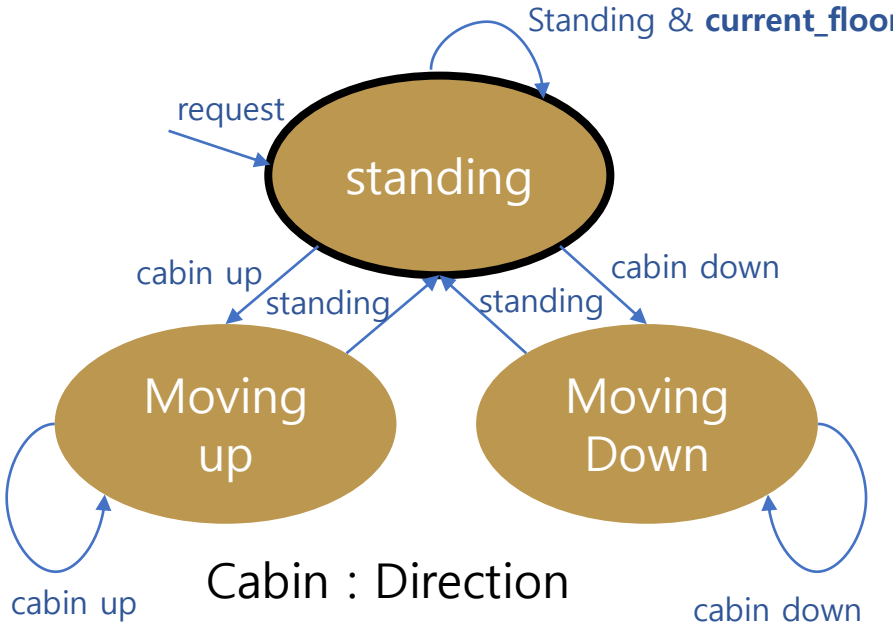


Cabin : current_floor

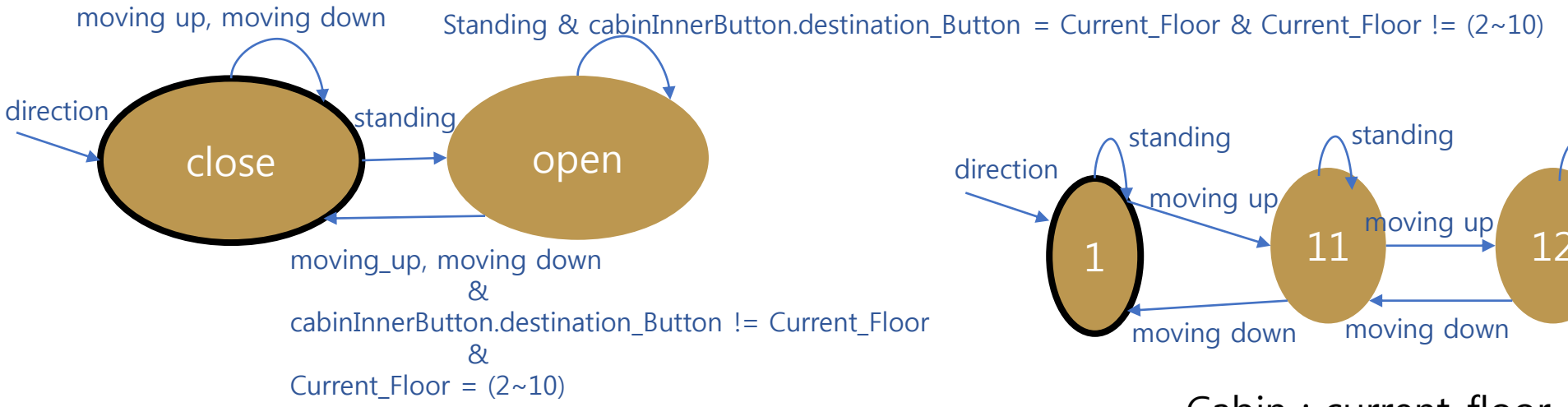
State : cabin(고층)



Door



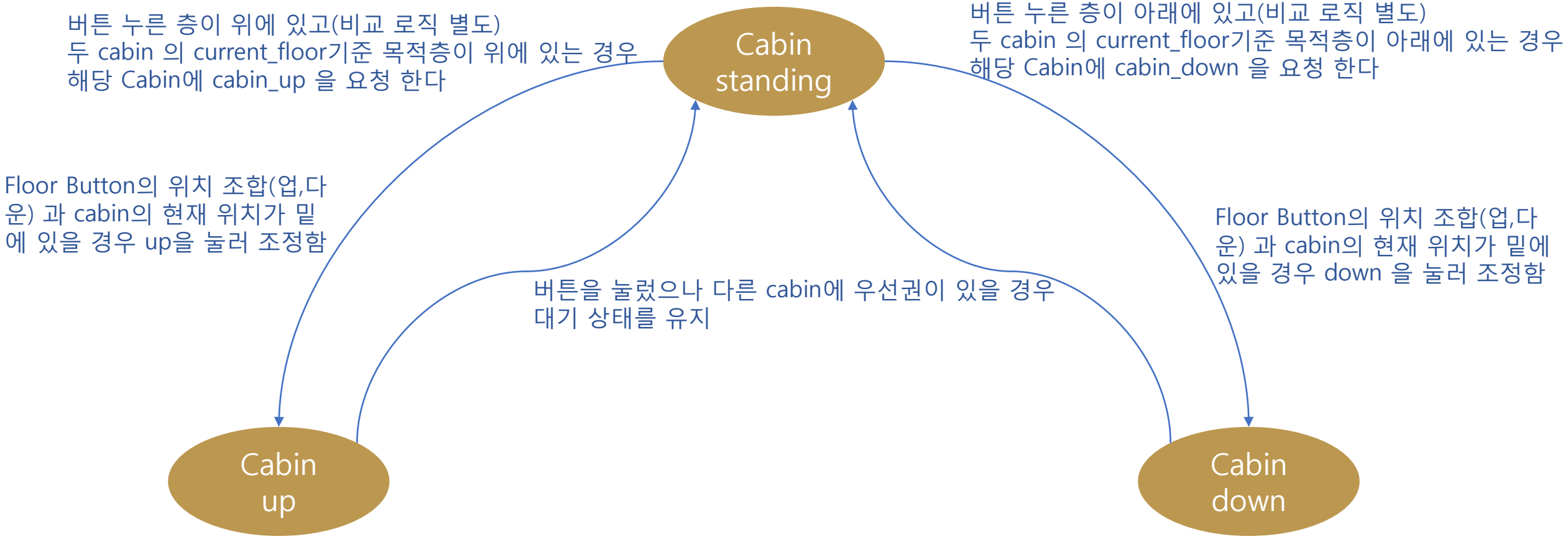
Cabin : Direction



Cabin : Door_request

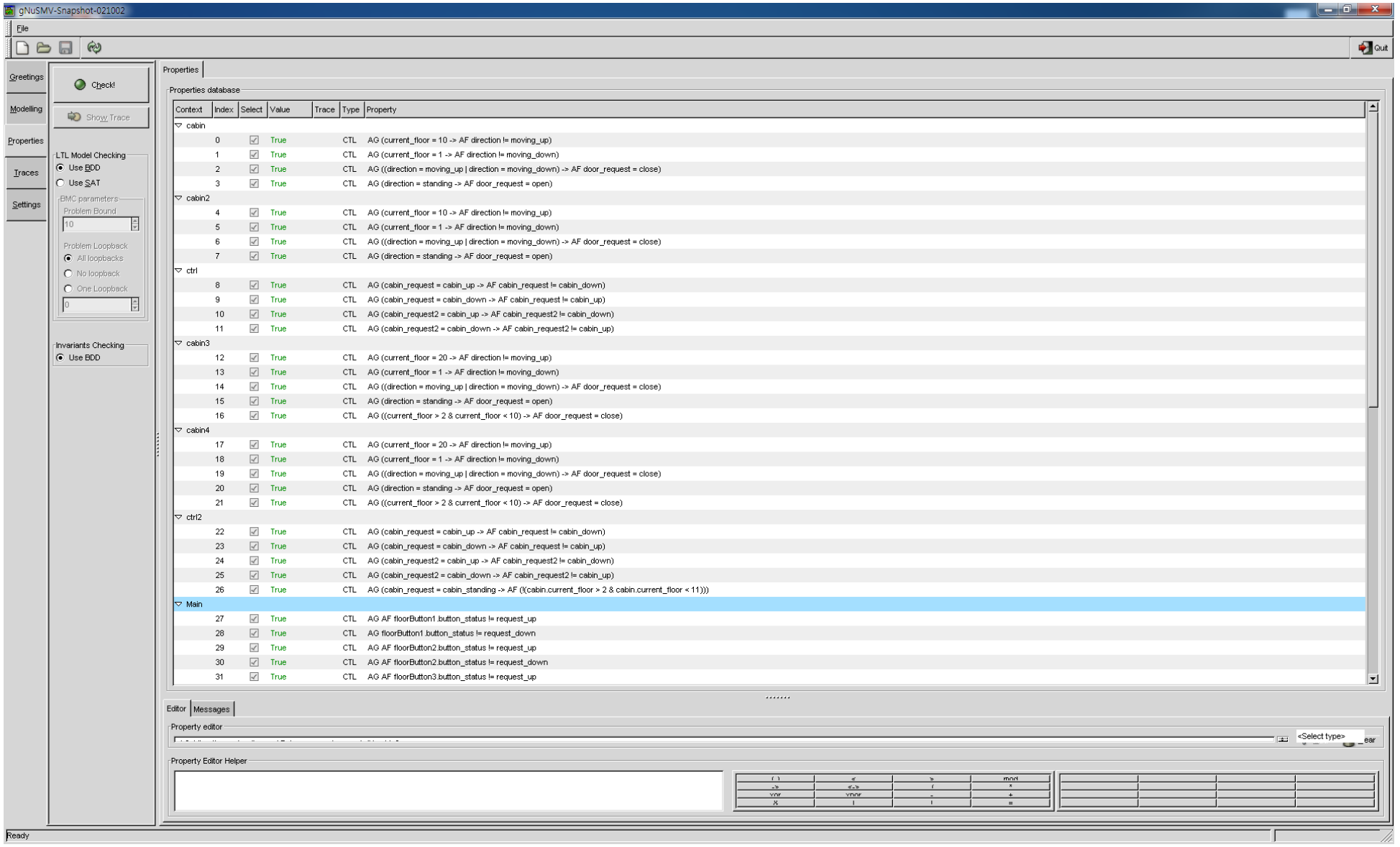
Cabin : current_floor

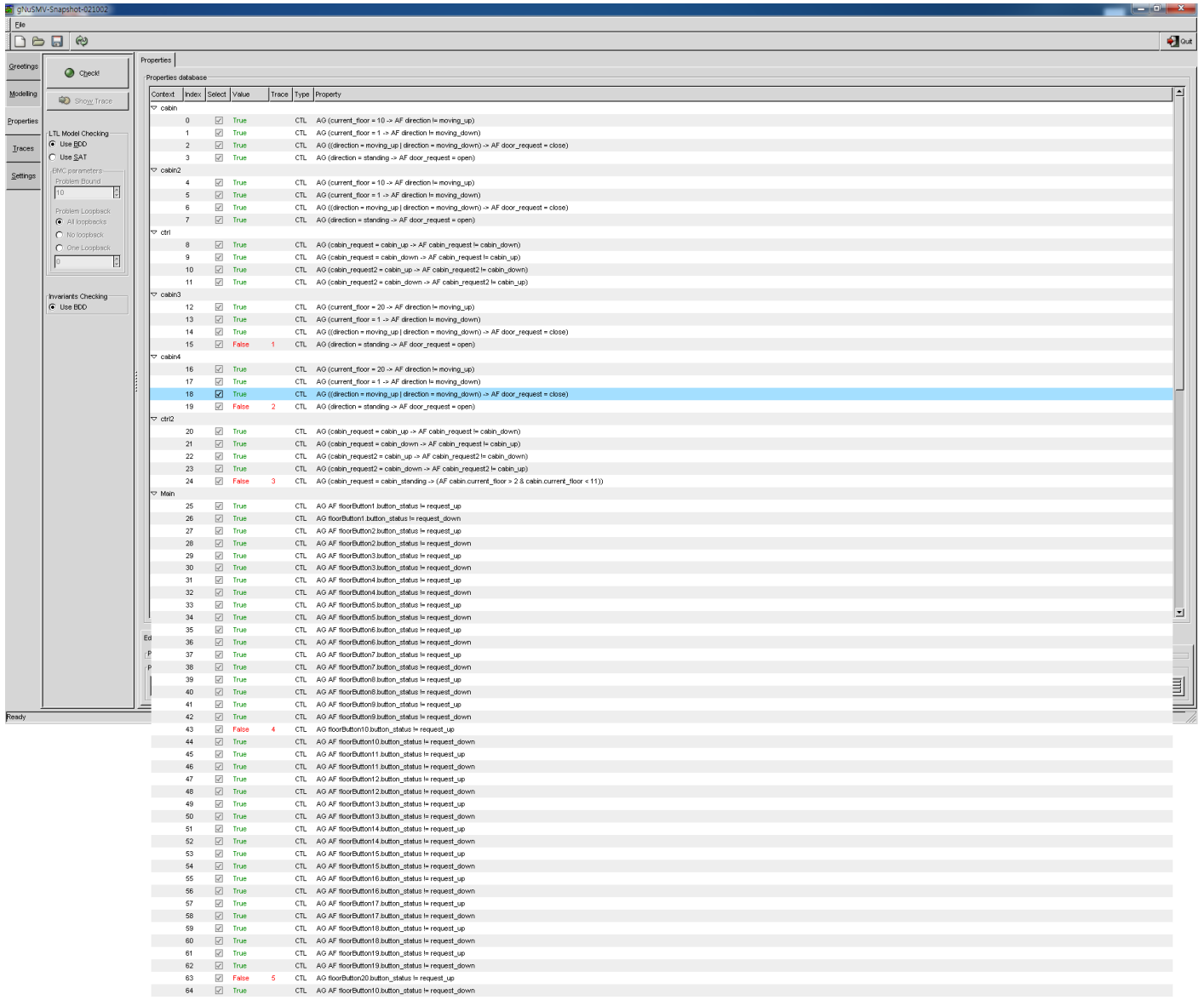
State : Control(저층/고층)



Variable

- Input
  - Floor button : up, down , off
  - Cabin inner button : 1…20
- Output
  - Cabin : direction, current_floor, door_request
  - Control : cabin_request
- Define
  - Current_on : 해당 칸이 floor button 누른 층에 있음
  - Pending_up : floor button 누른 층이 위에 있음
  - Pending_down : foor button 누른 층이 아래에 있음
  - Serv_up : cabin 내부 버튼을 눌렀을 때 해당 층이 cabin 기준 위에 있음
  - Serv_down : cabin 내부 버튼을 눌렀을 때 해당 층이 cabin 기준 아래에 있음


gNuSMV-Snapshot-021002
File
Quit
Greetings
Modelling
Properties
Traces
Settings
Check!
Show Trace
LTL Model Checking
Use BDD
Use SAT
BMC parameters
Problem Bound
10
Problem Loopback
All loopbacks
No loopback
One Loopback
0
Invariants Checking
Use BDD
Properties
Properties database
Context | Index | Select | Value | Trace | Type | Property
cabin
0 True CTL AG (current_floor = 10 -> AF direction != moving_up)
1 True CTL AG (current_floor = 1 -> AF direction != moving_down)
2 True CTL AG ((direction = moving_up | direction = moving_down) -> AF door_request = close)
3 True CTL AG (direction = standing -> AF door_request = open)
cabin2
4 True CTL AG (current_floor = 10 -> AF direction != moving_up)
5 True CTL AG (current_floor = 1 -> AF direction != moving_down)
6 True CTL AG ((direction = moving_up | direction = moving_down) -> AF door_request = close)
7 True CTL AG (direction = standing -> AF door_request = open)
ctrl
8 True CTL AG (cabin_request = cabin_up -> AF cabin_request != cabin_down)
9 True CTL AG (cabin_request = cabin_down -> AF cabin_request != cabin_up)
10 True CTL AG (cabin_request2 = cabin_up -> AF cabin_request2 != cabin_down)
11 True CTL AG (cabin_request2 = cabin_down -> AF cabin_request2 != cabin_up)
cabin3
12 True CTL AG (current_floor = 20 -> AF direction != moving_up)
13 True CTL AG (current_floor = 1 -> AF direction != moving_down)
14 True CTL AG ((direction = moving_up | direction = moving_down) -> AF door_request = close)
15 True CTL AG (direction = standing -> AF door_request = open)
16 True CTL AG ((current_floor > 2 & current_floor < 10) -> AF door_request = close)
cabin4
17 True CTL AG (current_floor = 20 -> AF direction != moving_up)
18 True CTL AG (current_floor = 1 -> AF direction != moving_down)
19 True CTL AG ((direction = moving_up | direction = moving_down) -> AF door_request = close)
20 True CTL AG (direction = standing -> AF door_request = open)
21 True CTL AG ((current_floor > 2 & current_floor < 10) -> AF door_request = close)
ctrl2
22 True CTL AG (cabin_request = cabin_up -> AF cabin_request != cabin_down)
23 True CTL AG (cabin_request = cabin_down -> AF cabin_request != cabin_up)
24 True CTL AG (cabin_request2 = cabin_up -> AF cabin_request2 != cabin_down)
25 True CTL AG (cabin_request2 = cabin_down -> AF cabin_request2 != cabin_up)
26 True CTL AG (cabin_request = cabin_standing -> AF (!(cabin.current_floor > 2 & cabin.current_floor < 11)))
Main
27 True CTL AG AF floorButton1.button_status != request_up
28 True CTL AG floorButton1.button_status != request_down
29 True CTL AG AF floorButton2.button_status != request_up
30 True CTL AG AF floorButton2.button_status != request_down
31 True CTL AG AF floorButton3.button_status != request_up
Editor
Messages
Property editor
<Select type>
Property Editor Helper
Ready


gNuSMV-Snapshot-021002
File
Quit
Greetings
Modelling
Properties
Traces
Settings
Check!
Show Trace
LTL Model Checking
Use BDD
Use SAT
BMC parameters
Problem Bound
10
Problem Loopback
All loopbacks
No loopback
One Loopback
0
Invariants Checking
Use BDD
Properties
Properties database
Context
Index
Select
Value
Trace
Type
Property
cabin
0 True CTL AG (current_floor = 10 -> AF direction != moving_up)
1 True CTL AG (current_floor = 1 -> AF direction != moving_down)
2 True CTL AG ((direction = moving_up | direction = moving_down) -> AF door_request = close)
3 True CTL AG (direction = standing -> AF door_request = open)
cabin2
4 True CTL AG (current_floor = 10 -> AF direction != moving_up)
5 True CTL AG (current_floor = 1 -> AF direction != moving_down)
6 True CTL AG ((direction = moving_up | direction = moving_down) -> AF door_request = close)
7 True CTL AG (direction = standing -> AF door_request = open)
ctrl
8 True CTL AG (cabin_request = cabin_up -> AF cabin_request != cabin_down)
9 True CTL AG (cabin_request = cabin_down -> AF cabin_request != cabin_up)
10 True CTL AG (cabin_request2 = cabin_up -> AF cabin_request2 != cabin_down)
11 True CTL AG (cabin_request2 = cabin_down -> AF cabin_request2 != cabin_up)
cabin3
12 True CTL AG (current_floor = 20 -> AF direction != moving_up)
13 True CTL AG (current_floor = 1 -> AF direction != moving_down)
14 True CTL AG ((direction = moving_up | direction = moving_down) -> AF door_request = close)
15 False 1 CTL AG (direction = standing -> AF door_request = open)
cabin4
16 True CTL AG (current_floor = 20 -> AF direction != moving_up)
17 True CTL AG (current_floor = 1 -> AF direction != moving_down)
18 True CTL AG ((direction = moving_up | direction = moving_down) -> AF door_request = close)
19 False 2 CTL AG (direction = standing -> AF door_request = open)
ctrl2
20 True CTL AG (cabin_request = cabin_up -> AF cabin_request != cabin_down)
21 True CTL AG (cabin_request = cabin_down -> AF cabin_request != cabin_up)
22 True CTL AG (cabin_request2 = cabin_up -> AF cabin_request2 != cabin_down)
23 True CTL AG (cabin_request2 = cabin_down -> AF cabin_request2 != cabin_up)
24 False 3 CTL AG (cabin_request = cabin_standing -> (AF cabin.current_floor > 2 & cabin.current_floor < 11))
Main
25 True CTL AG AF floorButton1.button_status != request_up
26 True CTL AG floorButton1.button_status != request_down
27 True CTL AG AF floorButton2.button_status != request_up
28 True CTL AG AF floorButton2.button_status != request_down
29 True CTL AG AF floorButton3.button_status != request_up
30 True CTL AG AF floorButton3.button_status != request_down
31 True CTL AG AF floorButton4.button_status != request_up
32 True CTL AG AF floorButton4.button_status != request_down
33 True CTL AG AF floorButton5.button_status != request_up
34 True CTL AG AF floorButton5.button_status != request_down
35 True CTL AG AF floorButton6.button_status != request_up
36 True CTL AG AF floorButton6.button_status != request_down
37 True CTL AG AF floorButton7.button_status != request_up
38 True CTL AG AF floorButton7.button_status != request_down
39 True CTL AG AF floorButton8.button_status != request_up
40 True CTL AG AF floorButton8.button_status != request_down
41 True CTL AG AF floorButton9.button_status != request_up
42 True CTL AG AF floorButton9.button_status != request_down
43 False 4 CTL AG floorButton10.button_status != request_up
44 True CTL AG AF floorButton10.button_status != request_down
45 True CTL AG AF floorButton11.button_status != request_up
46 True CTL AG AF floorButton11.button_status != request_down
47 True CTL AG AF floorButton12.button_status != request_up
48 True CTL AG AF floorButton12.button_status != request_down
49 True CTL AG AF floorButton13.button_status != request_up
50 True CTL AG AF floorButton13.button_status != request_down
51 True CTL AG AF floorButton14.button_status != request_up
52 True CTL AG AF floorButton14.button_status != request_down
53 True CTL AG AF floorButton15.button_status != request_up
54 True CTL AG AF floorButton15.button_status != request_down
55 True CTL AG AF floorButton16.button_status != request_up
56 True CTL AG AF floorButton16.button_status != request_down
57 True CTL AG AF floorButton17.button_status != request_up
58 True CTL AG AF floorButton17.button_status != request_down
59 True CTL AG AF floorButton18.button_status != request_up
60 True CTL AG AF floorButton18.button_status != request_down
61 True CTL AG AF floorButton19.button_status != request_up
62 True CTL AG AF floorButton19.button_status != request_down
63 False 5 CTL AG floorButton20.button_status != request_up
64 True CTL AG AF floorButton10.button_status != request_down
Ready

Trace 1 | Trace 2 | Trace 3 | Trace 4 | Trace 5

CTL property 15: AG (direction = standing -> AF door_request = open)

Loop	Step	cabin.currentfloor	cabin.destinationbutton	cabin.direction	cabin.door.status	cabin.doorrequest	cabin2.currentfloor	cabin2.destinationbutton	cabin2.direction	cabin2.door.status	cabin2.doorrequest	cabin3.currentfloor	cabin3.destinationbutton	cabin3.direction	cabin3.door.status	cabin3.doorrequest
	0	8	8	standing	open	close	8	8	standing	open	close	8	18	standing	open	close
	1	8	8	standing	close	open	8	8	standing	close	open	8	18	standing	close	close
	2	8	8	standing	open	open	8	8	standing	open	open	8	18	standing	close	close
	3	8	8	standing	open	open	8	8	standing	open	open	8	18	standing	close	close
	4	8	8	standing	open	open	8	8	standing	open	open	8	18	standing	close	close

Property

Property	의미	검증결과
SPEC AG (current_floor = 20 -> AF(direction != moving_up))	20에서는 더 올라갈 수 없음	True
SPEC AG (current_floor = 1 -> AF(direction != moving_down))	1층에서는 더 내려갈 수 없음	True
SPEC AG (direction = standing -> AF(door_request = open))	Cabin이 머물러 있을 때는 문을 오픈함	True
SPEC AG (direction = moving_up | direction = moving_down -> AF(door_request = close))	Cabin이 움직이는 중에는 문이 열리면 안됨	True
SPEC AG ((current_floor > 2 & current_floor < 10) -> AF(door_request = close))	고층의 경우 2층과 10층 사이에 있을 경우 문이 열리면 안됨	True
SPEC AG (cabin_request=cabin_standing -> AF !(cabin.current_floor > 2 & cabin.current_floor <11))	고층용 cabin은 2층과 10층 사이에 머물러 있을 수 없음	True
SPEC AG (AF floorButton1.button_status!=request_up)	Floor 버튼이 무한정 업 상태로만 있을 수 없음	True
SPEC AG (floorButton1.button_status!=request_down)	Floor 버튼이 무한정 업 상태로만 있을 수 없음	True

향후 계획

- 현재: 엘리베이터 2칸 씩의 저층/고층 Elevator
- 요구사항
  - 대수 증가 및 저층/고층 해제
  - 1층에 로비 버튼 추가하여 칸 위치 비교하여 가까운 칸에 request 처리

감사합니다