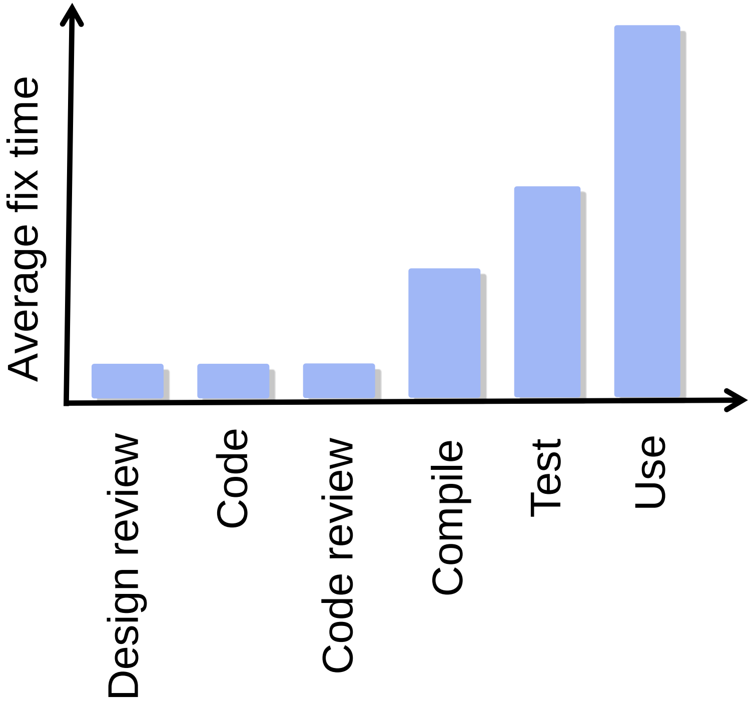
Transducer FSMs in System Design

In this lecture we go through examples of transducer FSMs in the specification of larger systems.

In the process we will discuss system design lifecycles and the role of specification at different lifecycle stages.

Why Careful Design Matters

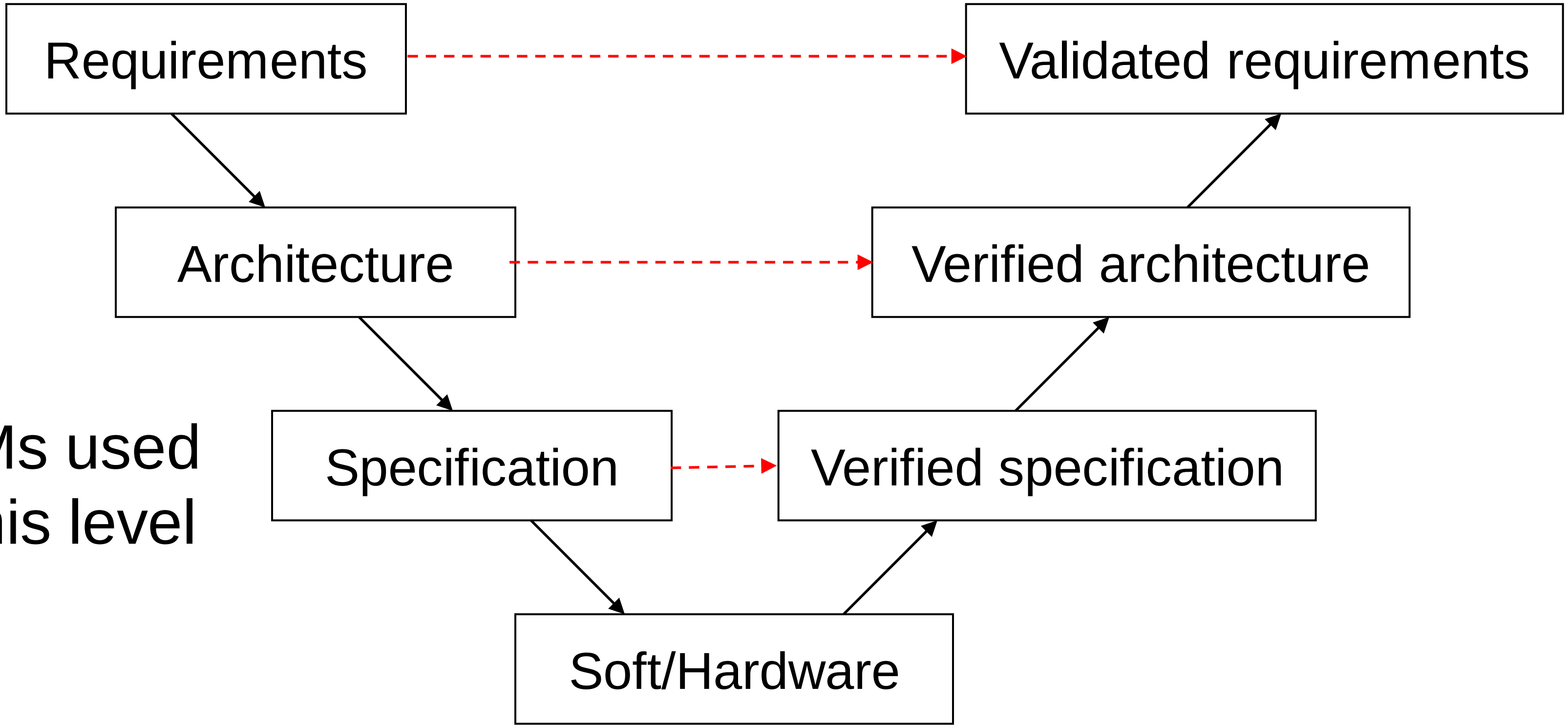


$P = (1 - P_1) \times (1 - P_2) \times \ldots \times (1 – P_n)$

where: P is probability that program is fault free

Pi is probability of fault injection at stage i of n

Example Lifecycle Stages



FSMs used
at this level

Data Projector: Requirements

1. Must be able to control input from either the computer or the video.
2. Should be able to switch between computer and video while the data projector is in operation.
3. Power button must be pressed twice to switch off (to prevent inadvertent shutdown).

Data Projector: Inputs

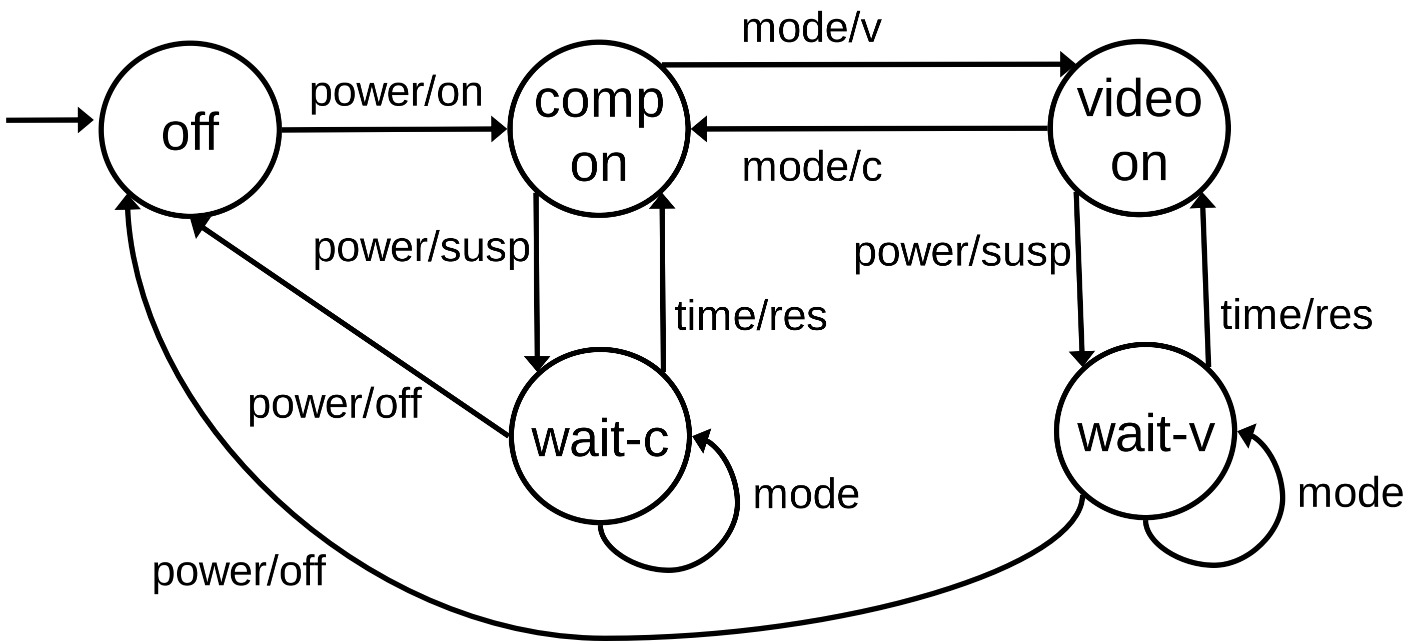
From remote control	
power	Signal from on/off button on remote control
mode	Signal from mode button on remote control

From system clock	
time	Timeout signal

Data Projector : Outputs

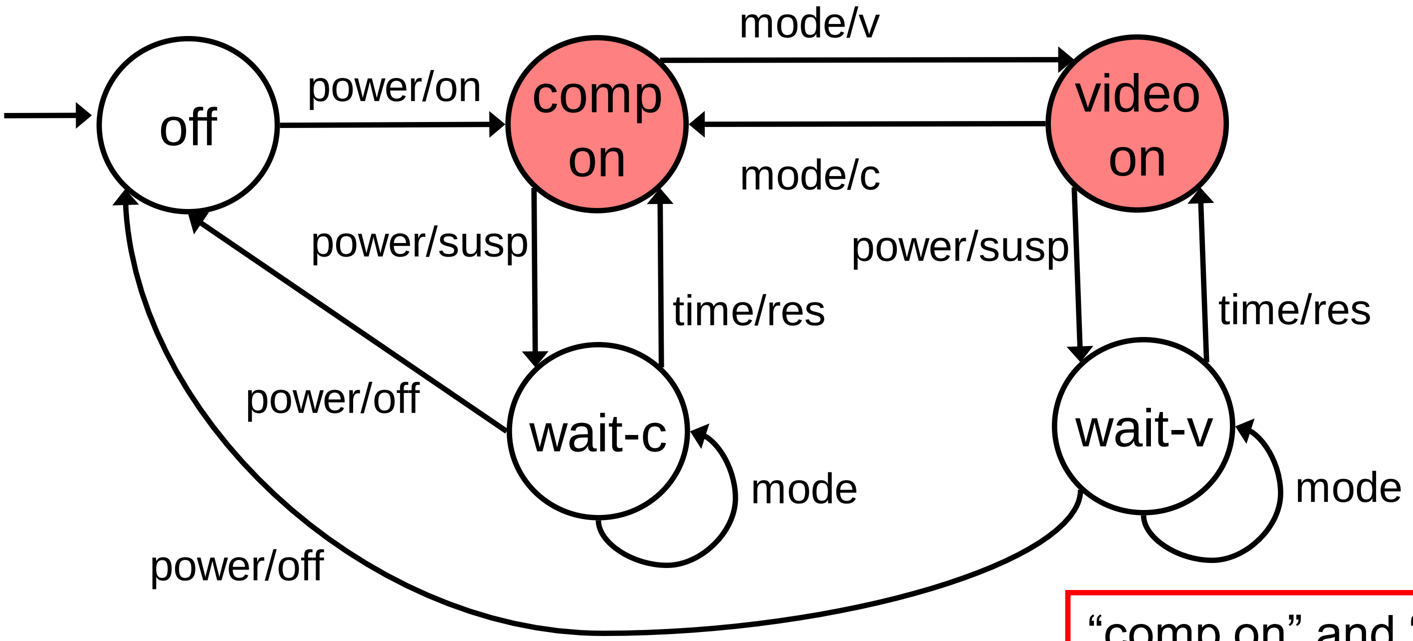
To control system	
on	Signals system to start up
off	Signals system to shut down
c	Take input from computer
v	Take input from video
susp	Signals suspension of normal operation
res	Signals normal operation to resume

Data Projector: Design



Checking Requirement 1

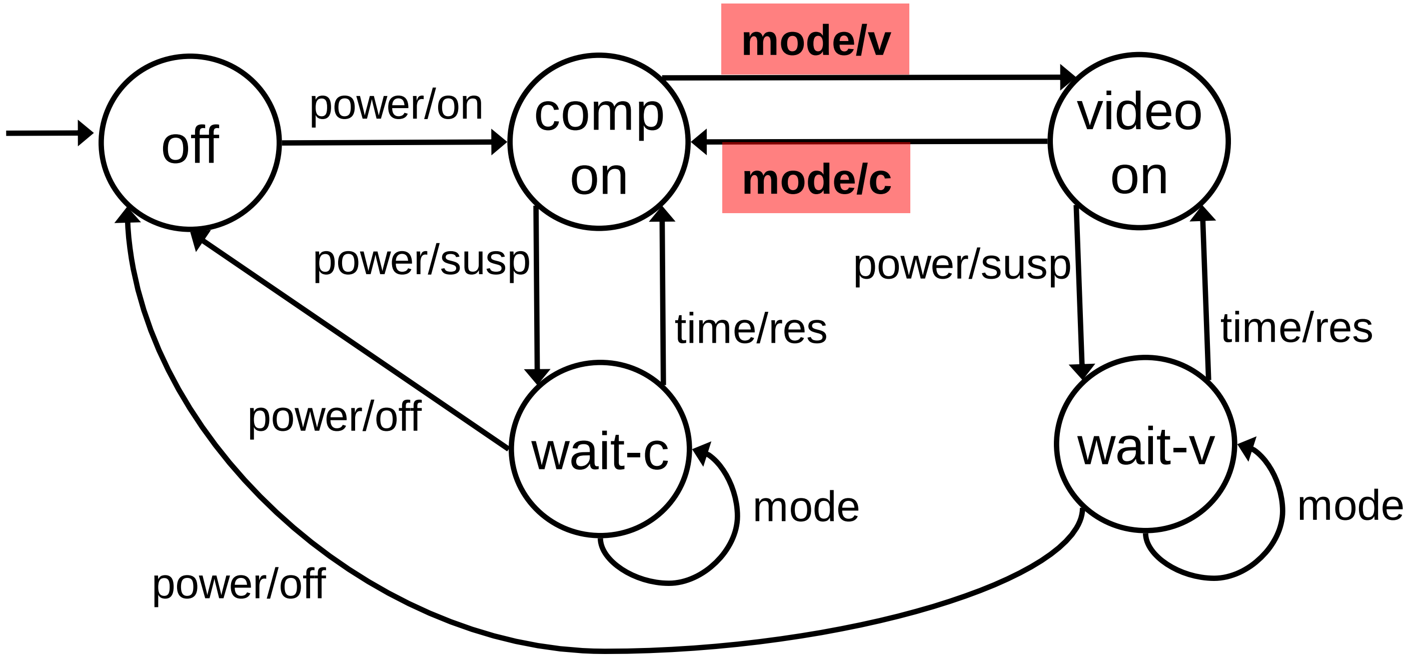
Must be able to control input from either the computer or the video



“comp on” and “video on” states are reachable from start state and from each other

Checking Requirement 2

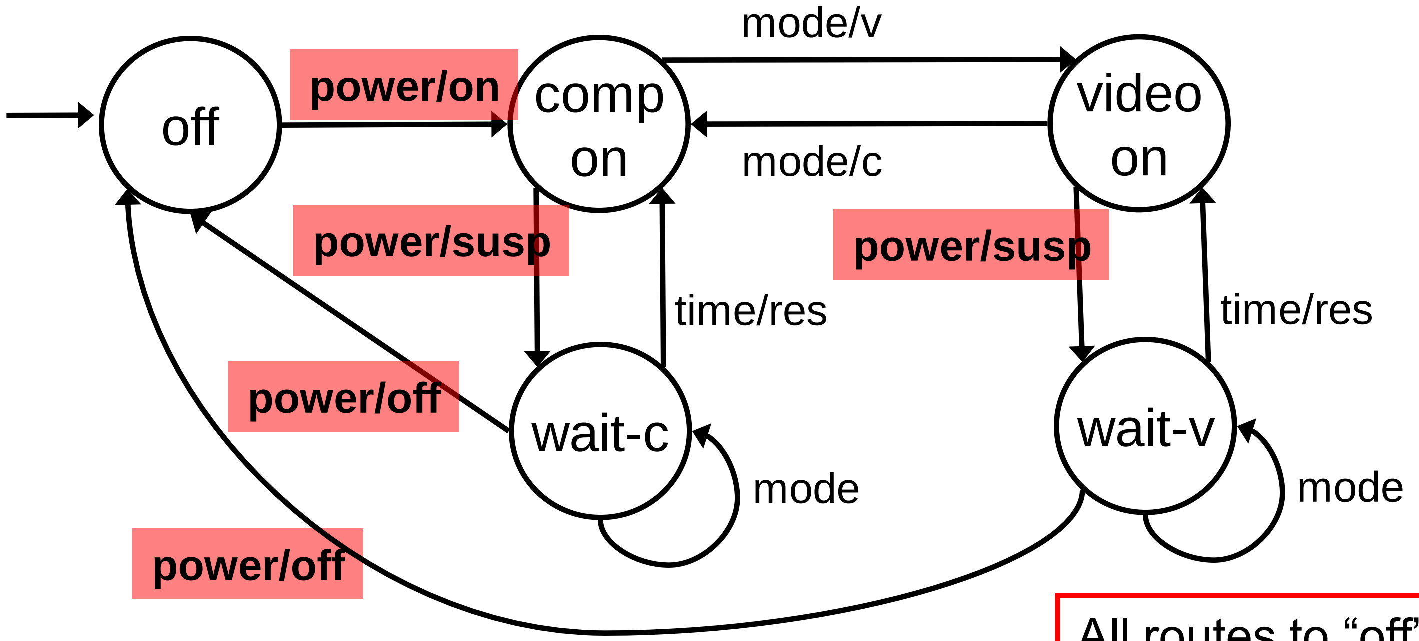
Should be able to switch between computer and video while in operation



“mode” toggles between “comp on” and “video on”, following “on” input.

Checking Requirement 3

Power button must be pressed twice to switch off



All routes to “off” from comp/video on require two consecutive “power” inputs

Cruise Control: Requirements

1. The driver must be able to turn the cruise control system off.
2. The driver must be able to tell the system to maintain the current speed.
3. The cruise control system must not operate after braking.
4. The cruise control system must allow the driver to travel faster than the set speed by using the accelerator.

Cruise Control: Inputs

From driver	
onoff	On/off button
set	Sets cruise to current speed
brake	Brake pressed
accP	Accelerator pressed
accR	Accelerator released
resume	Resume travelling at set speed

From control system	
correct	Car is at correct speed
slow	Car is slower than set speed
fast	Car is faster than set speed

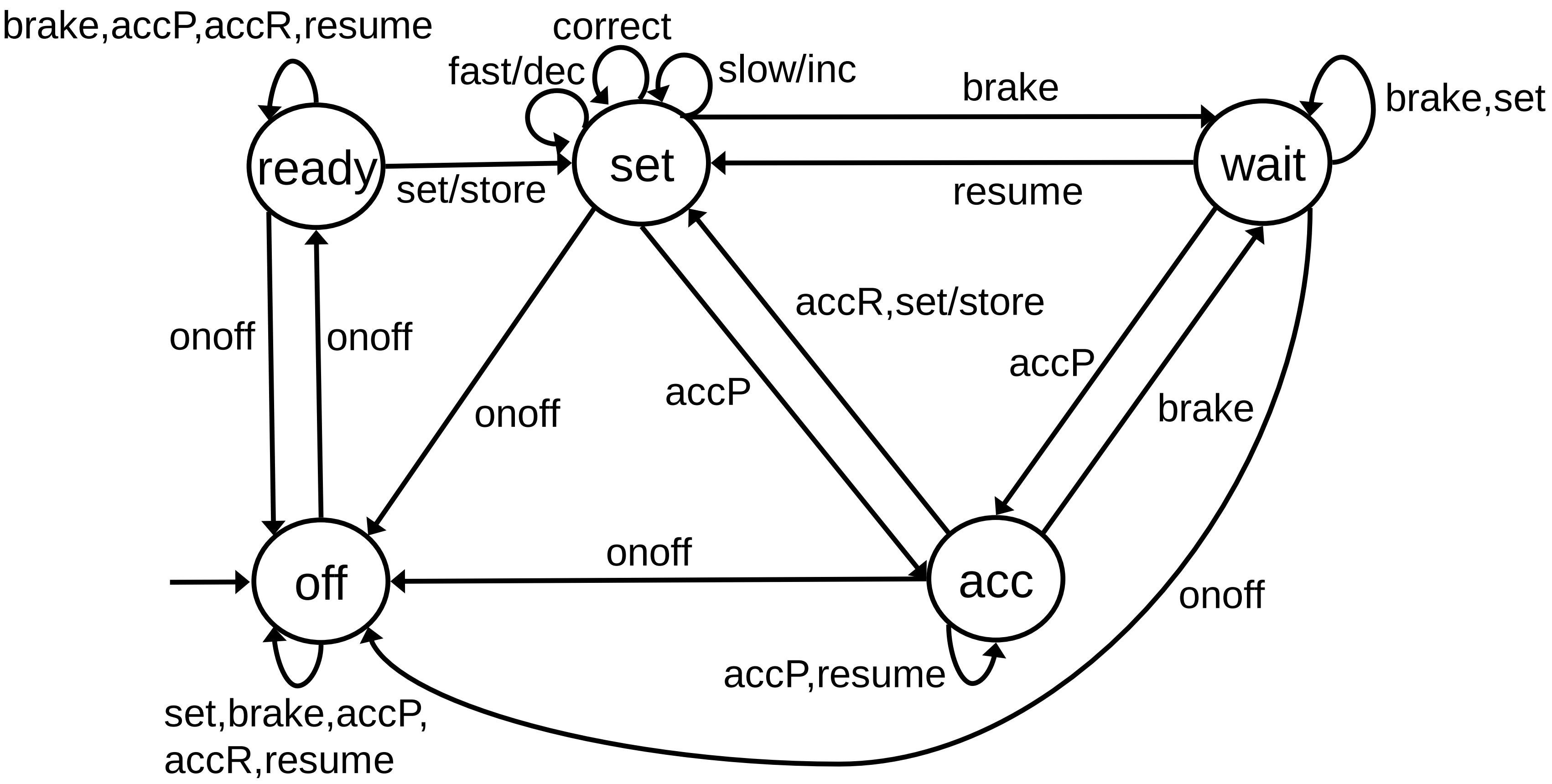
Cruise Control: Outputs

To control system	
store	Store current speed
inc	Increase the throttle
dec	Decrease the throttle

Cruise Control: States

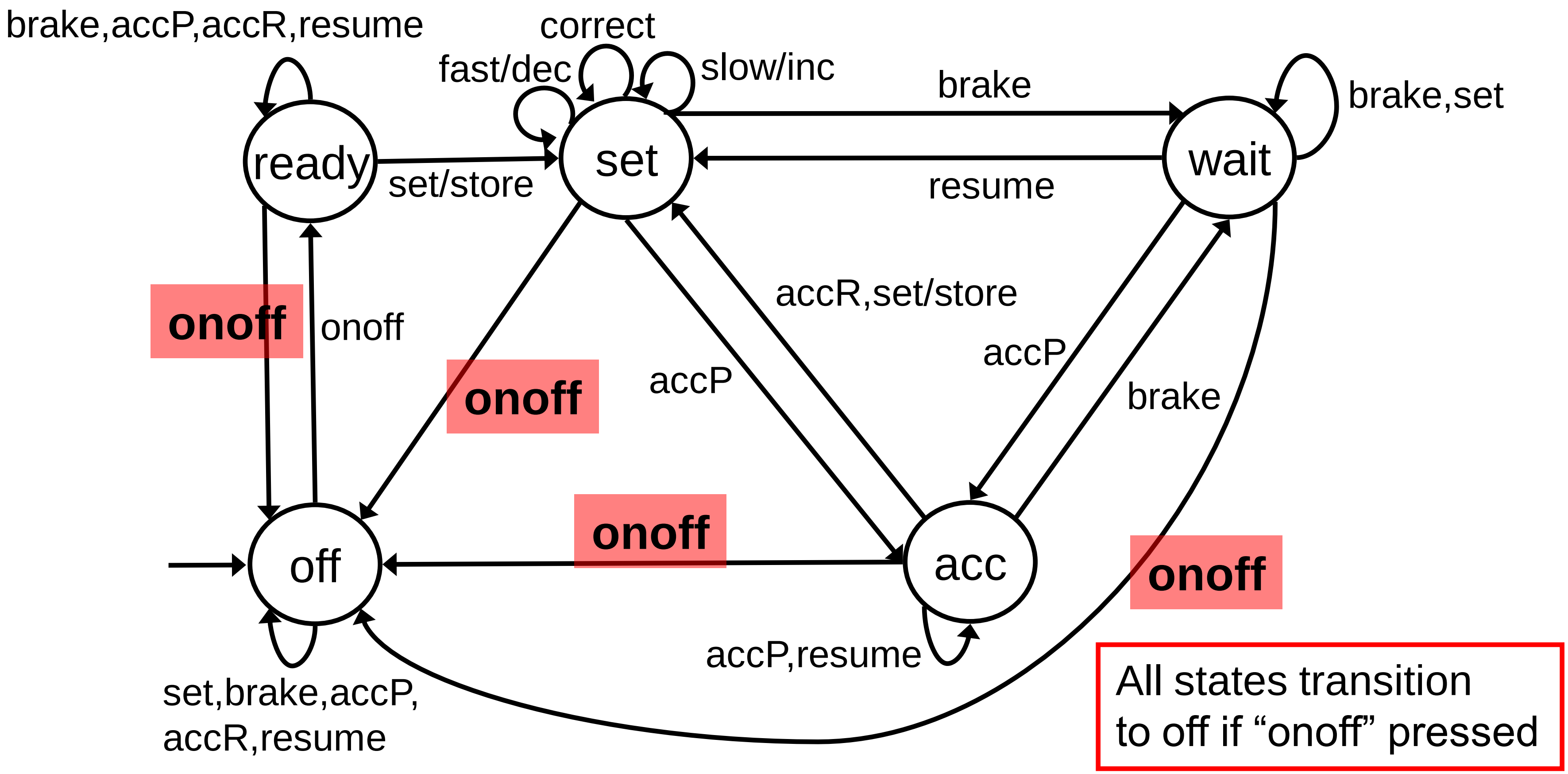
States of cruise control system	
off	System not operational
ready	Switched on but no speed set
set	Speed set and system maintaining it
wait	Speed set but brake pressed so system is waiting until resume is pressed before attempting to maintain speed
acc	Accelerator has been pressed (but not released) to override cruise control

Cruise Control: Design



Checking Requirement 1

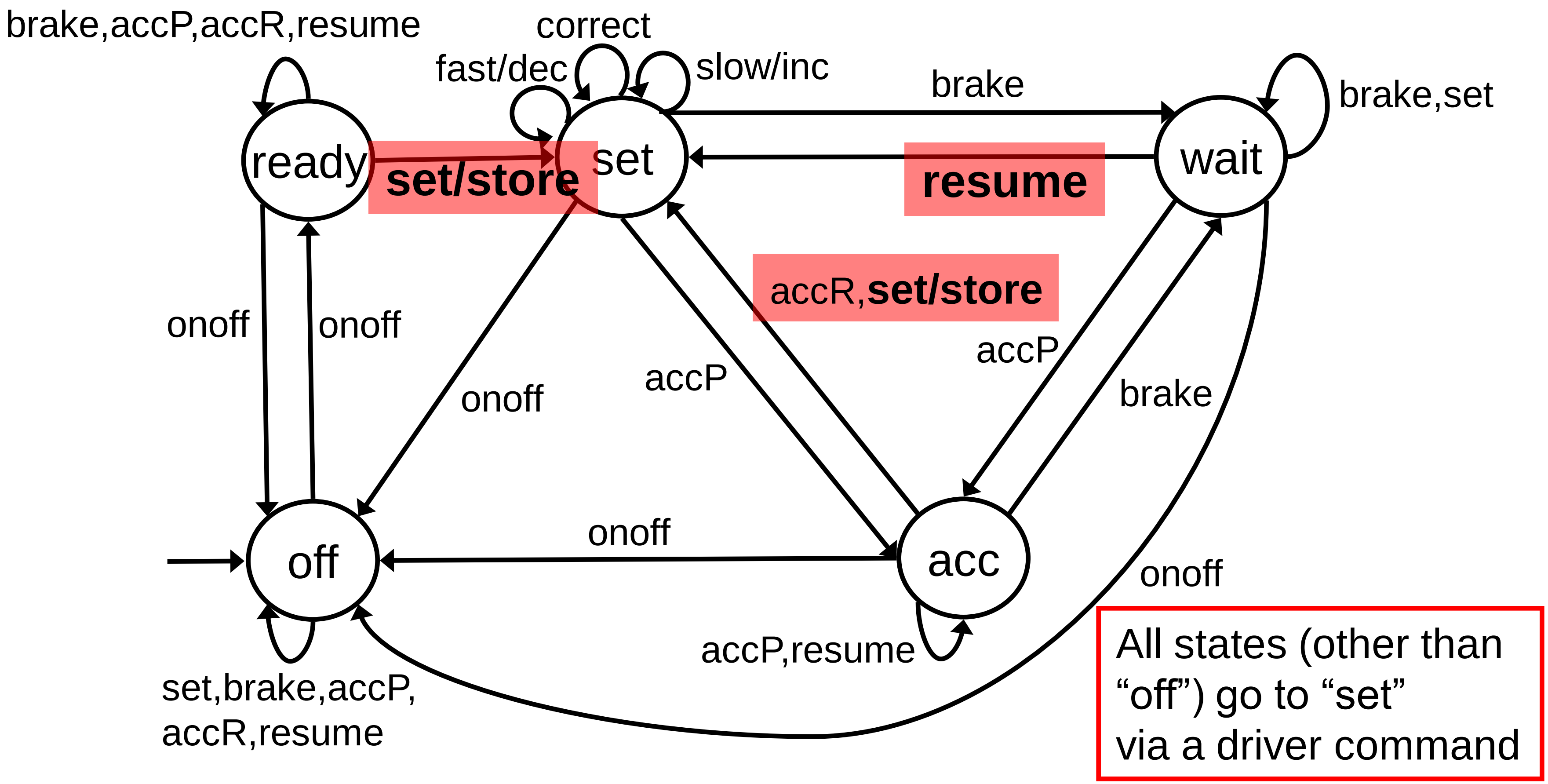
The driver must be able to turn the cruise control system off.



All states transition to off if "onoff" pressed

Checking Requirement 2

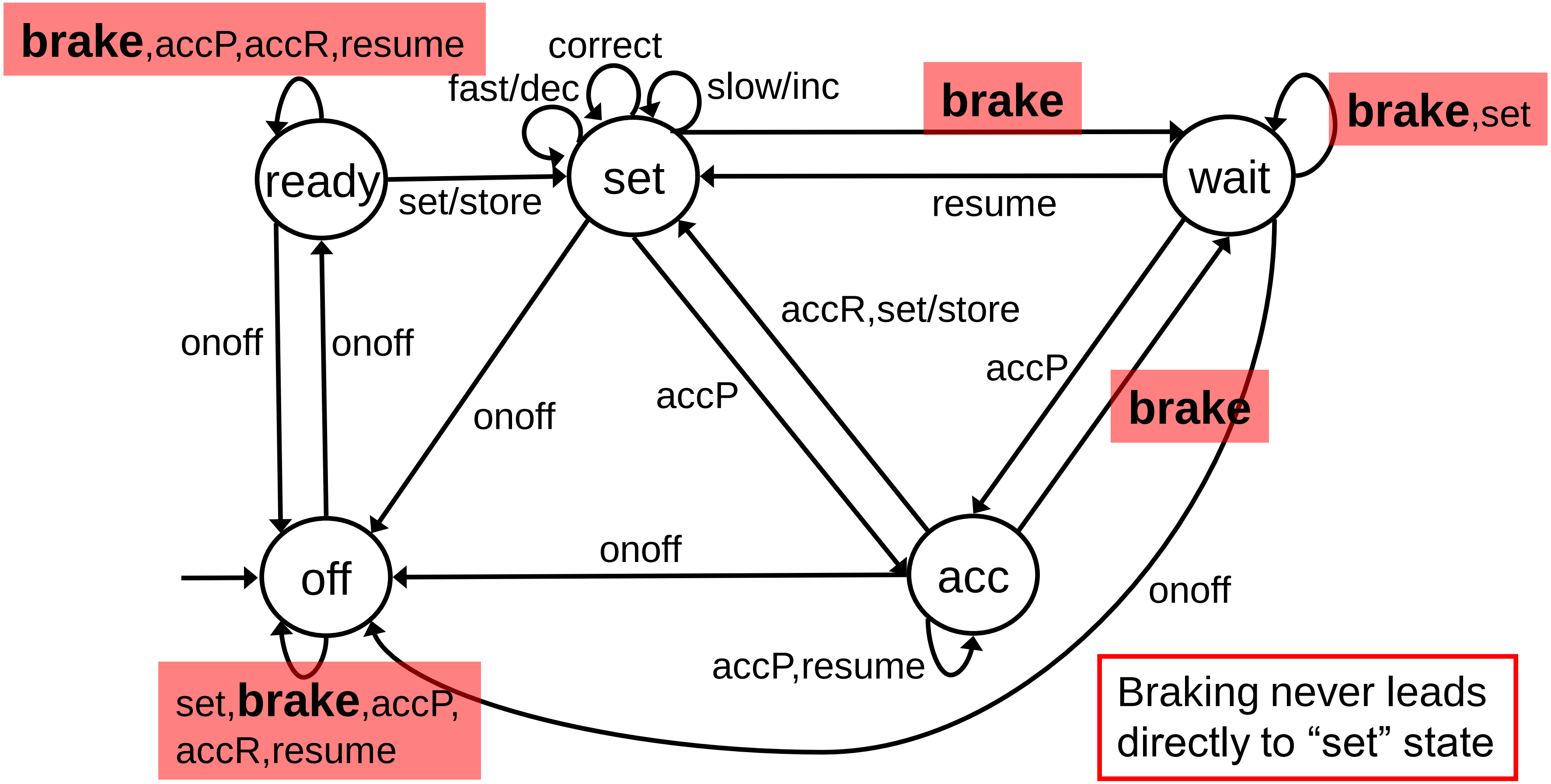
The driver must be able to tell the system to maintain the current speed.



All states (other than “off”) go to “set” via a driver command

Checking Requirement 3

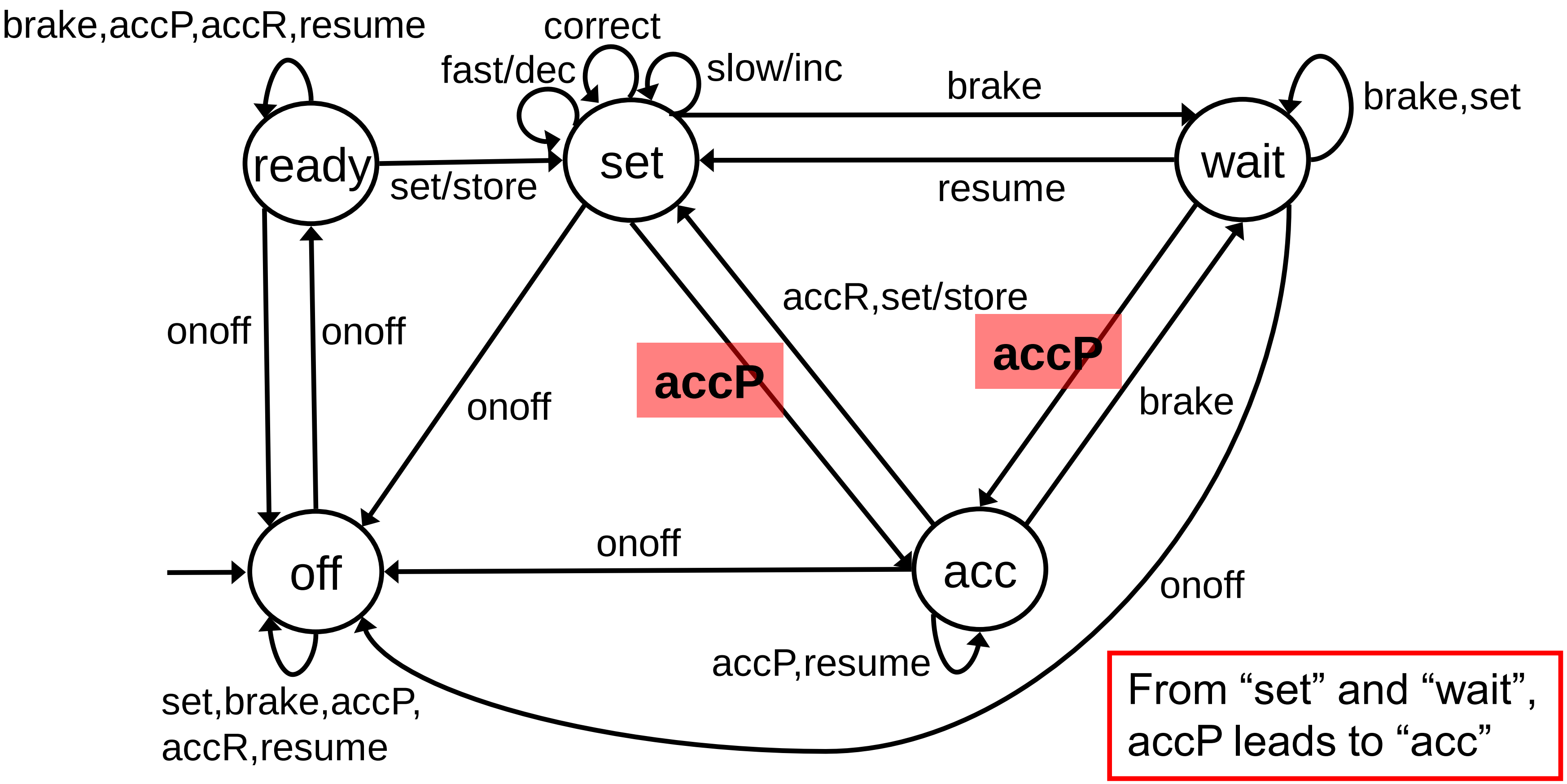
The cruise control system must not operate after braking.



Braking never leads directly to “set” state

Checking Requirement 4

The system must allow the driver to go faster than the set speed using the accelerator.



From “set” and “wait”, accP leads to “acc”