Transducer FSMs in System Design

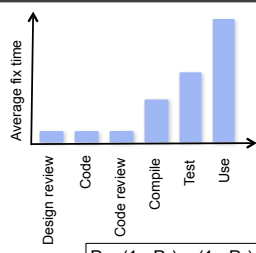In this lecture we go through examples of transducer FSMs in the specification of larger systems.

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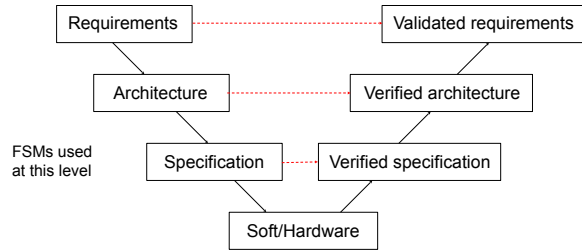
Why Careful Design Matters

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

where: P is probability that program is fault free

Pi is probability of fault injection at stage i of n

Example Lifecycle Stages

Requirements ┄┄┄┄┄┄┄ Validated requirements

Architecture ┄┄┄┄┄┄┄ Verified architecture

FSMs used
at this level

Specification ┄┄┄┄┄┄┄ Verified specification

Soft/Hardware

Data Projector: Requirements

1. Must be able to take 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
spd	Signals suspension of normal operation
res	Signals normal operation to resume

Data Projector: Design

State transition diagram:

- off → comp on : power/on
- comp on → video on : mode/v
- video on → comp on : mode/c
- comp on → wait-c : power/susp
- wait-c → comp on : time/res
- video on → wait-v : power/susp
- wait-v → video on : time/res
- wait-c → off : power/off
- wait-v → off : power/off
- wait-c → wait-v : mode
- wait-v → wait-c : mode
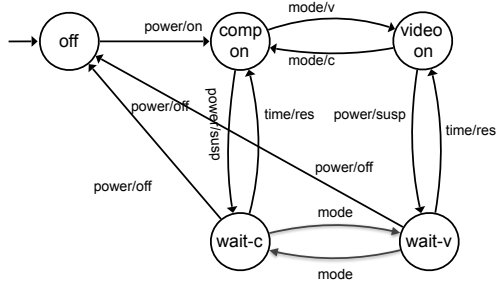
Checking
Requirement 1

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


```
          power/on        mode/v
  off ────────────► com ◄──────────► vid
                    on   ──────────►  on
                         mode/c
```
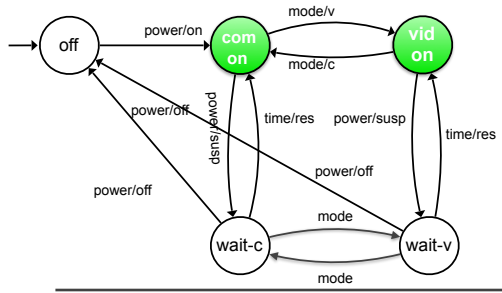
"comp on"
and "video
on" states are
reachable
from start
state and
from each
other

power/off

power/susp

time/res   power/susp   time/res

power/off

power/off

wait-c ◄── mode ──► wait-v
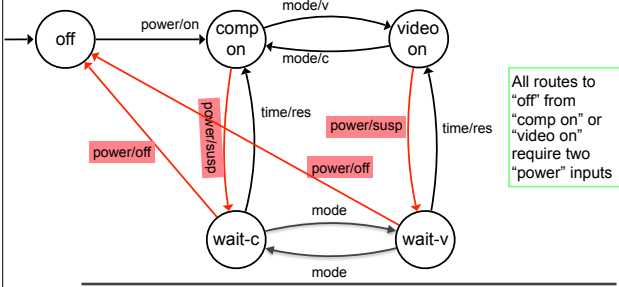   ◄── mode ──

Checking Requirement 2

Should be able to switch between computer and video while in operation
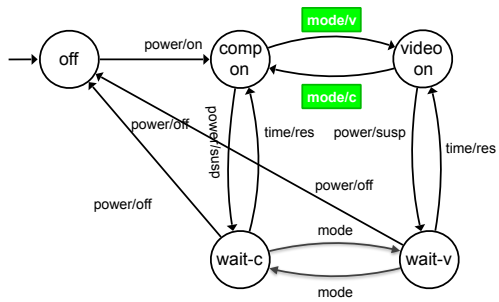
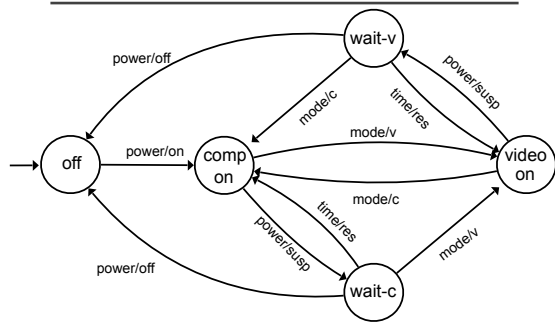"mode" toggles between "comp on" and "video on", following "on" input.

Checking Requirement 3

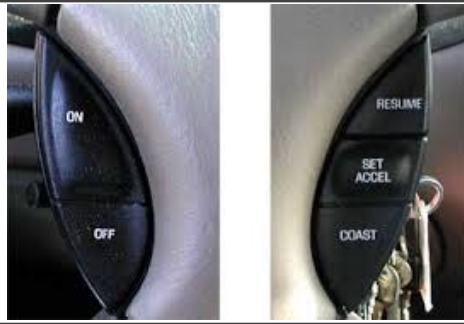Power button must be pressed twice to switch off

All routes to "off" from "comp on" or "video on" require two "power" inputs

An Alternative Design

Wyoming Highway Patrol believes bus that crashed was on cruise control

Three people were killed in an eight-vehicle collision …