Validating Real-Time Behavioral Patterns of Embedded Controllers

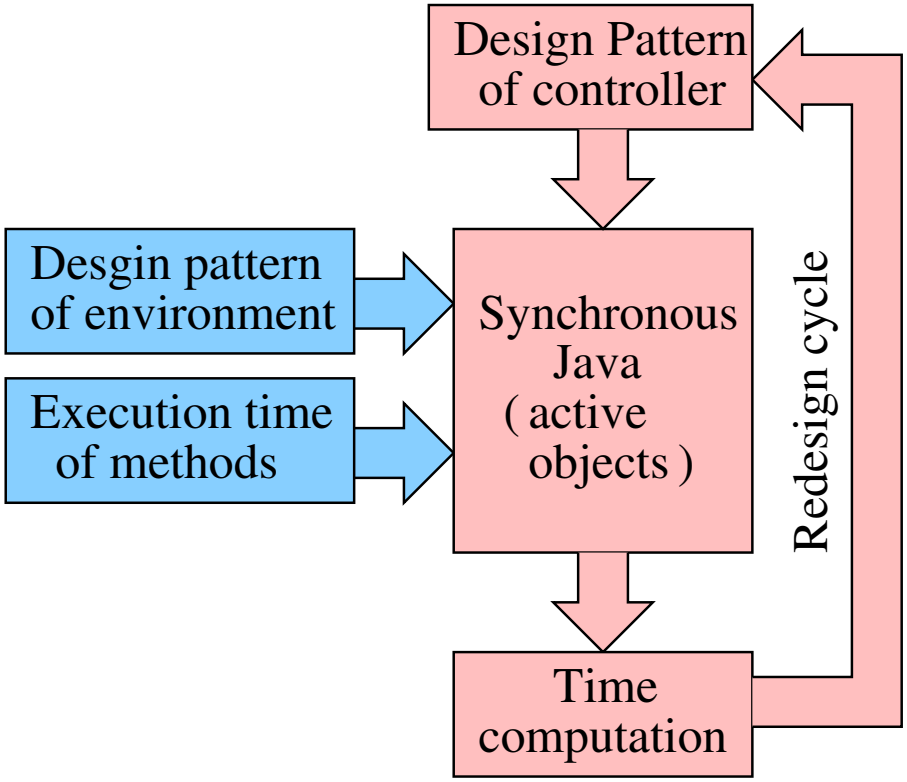
Jagannath Aghav and Claude Petitpierre

Swiss Federal Institute of Technology (EPFL)

OUTLINE...

1. Validation Process Cycle
2. Composition of Gear Controller
3. Timing Requirements
4. Architectural and Behaviroal Patterns
5. Timed Annotations
6. Validation Model
7. Time Computation
8. Discussion

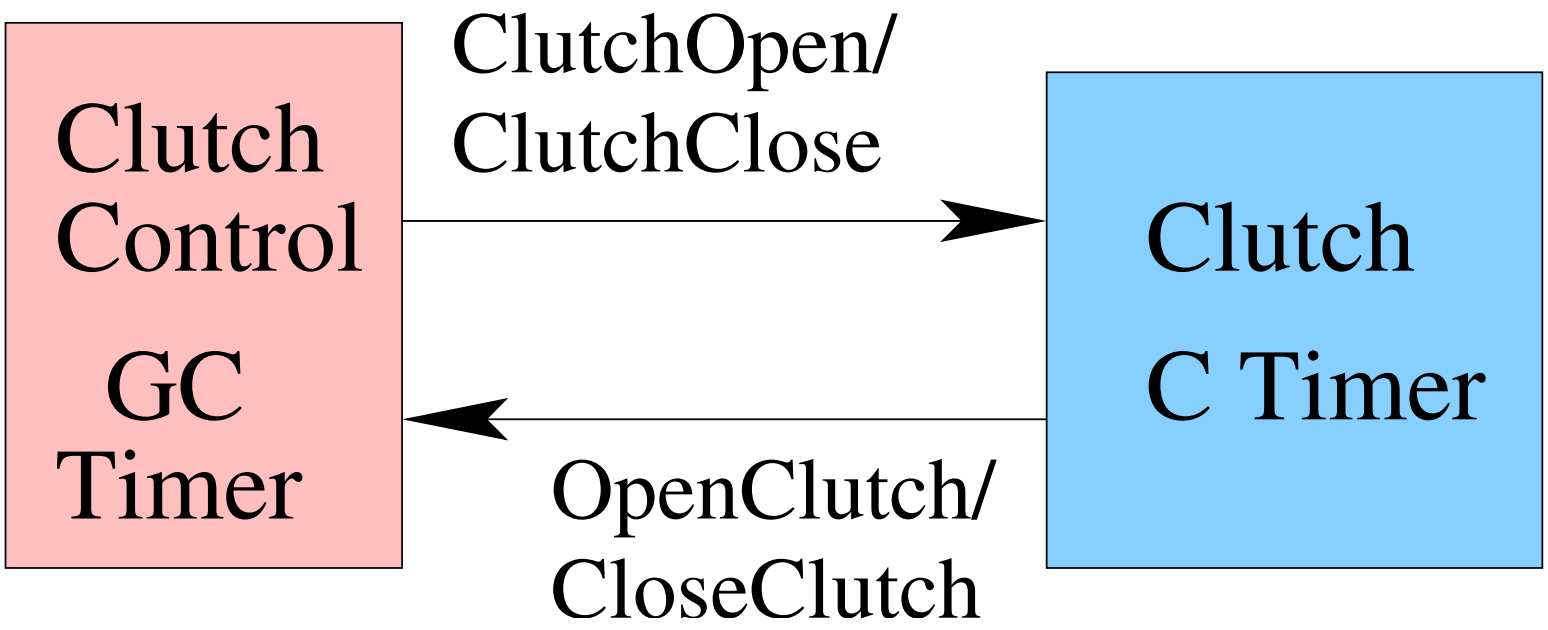
VALIDATION PROCESS CYCLE



Steps of Validation Process

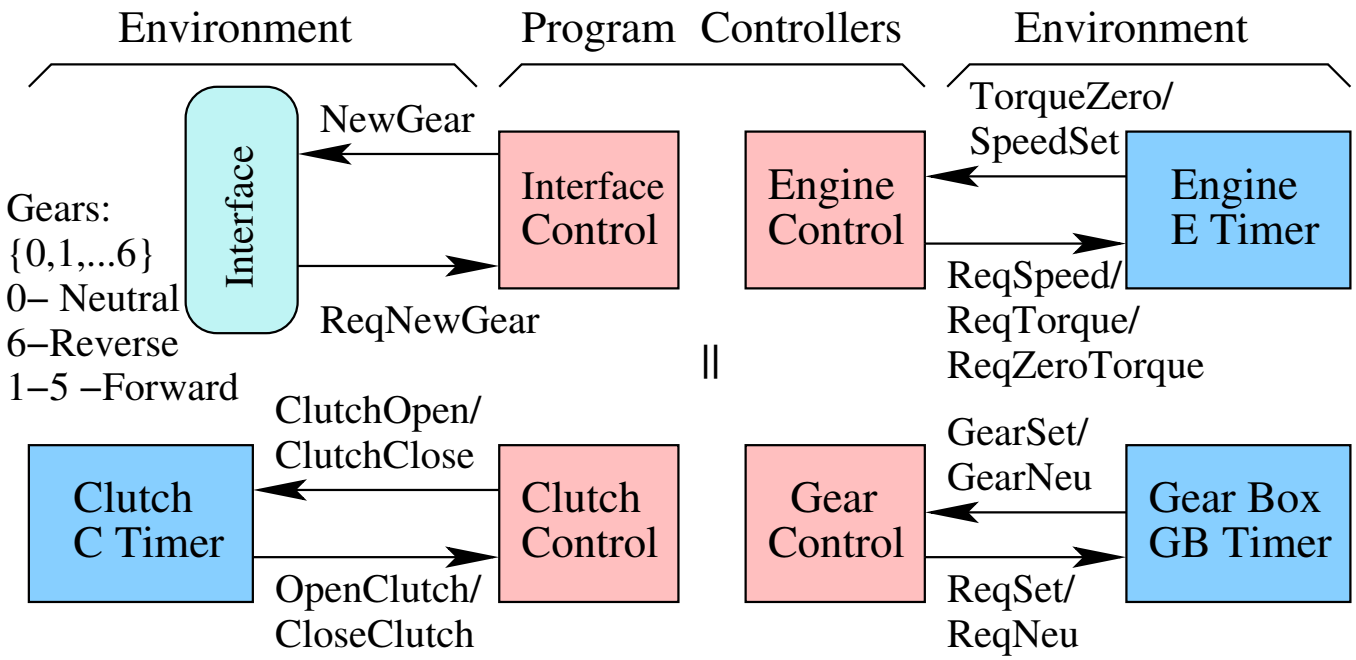
1. Model the behavioral pattern of the program controller.
2. Model the behavioral pattern of corresponding component being controlled.
3. Implement the code from Statecharts diagrams as synchronous active objects.
4. Read execution times in Java code.
5. Construct a finite state automaton.
6. Compute the longest response time.
7. Display the longest time response of all paths.

Clutch Controller



- Electronic Controller

Composition of Mecel's Gear Controller



GEAR CHANGING ALGORITHM

1. Wait until request for new gear.
2. Obtain zero torque over transmission.
3. Bring gear box in neutral gear.
4. Set the required speed of engine.
5. Set new gear.
6. Set the required torque and go to step 1.

TIMING REQUIREMENTS

(a) Gear box sets a gear in 100 to 300 ms. Otherwise Error state.

(b) Gear box releases gear in 100 to 200 ms. Otherwise Error state.

(c) Clutch changes state from open to close or vice versa in 100 to 150 ms otherwise returns to error state.

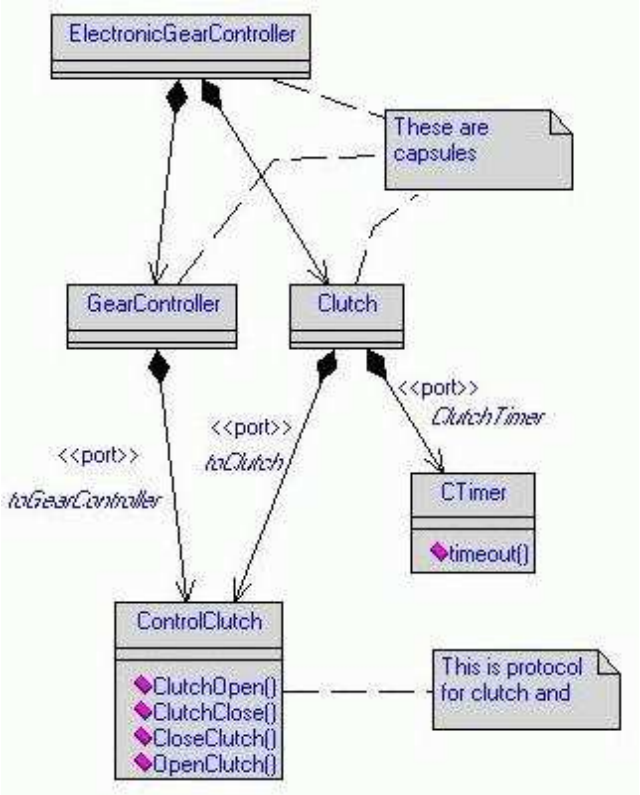
(d) The maximum time bound to obtain a zero torque for engine is 400 ms.

(e) For engine the maximum time bound to obtain a synchronous speed is 500 ms otherwise engine enters into error state.

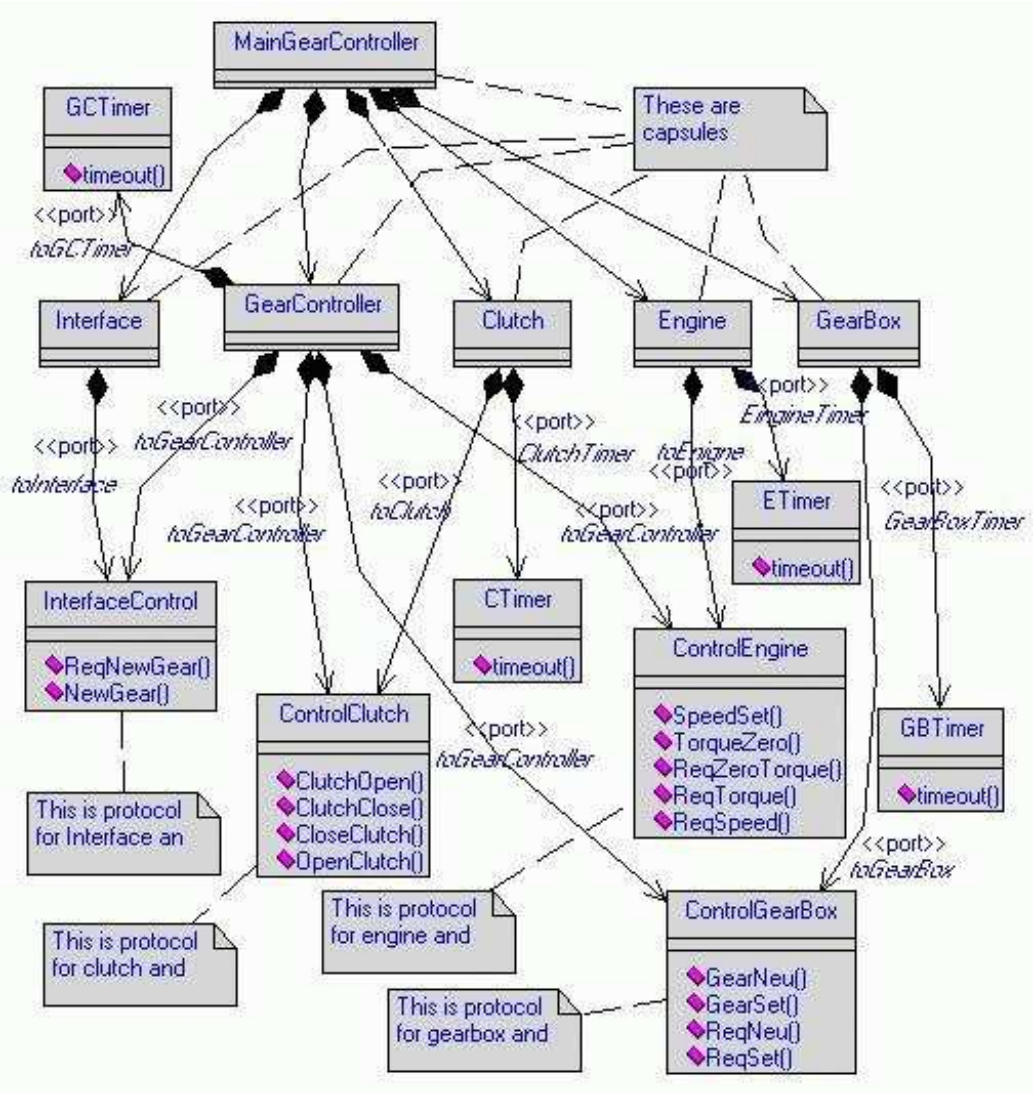
(f) A gear change should be completed within 1.5 seconds.

(g) A gear change under normal conditions should be happen within 1 sec.

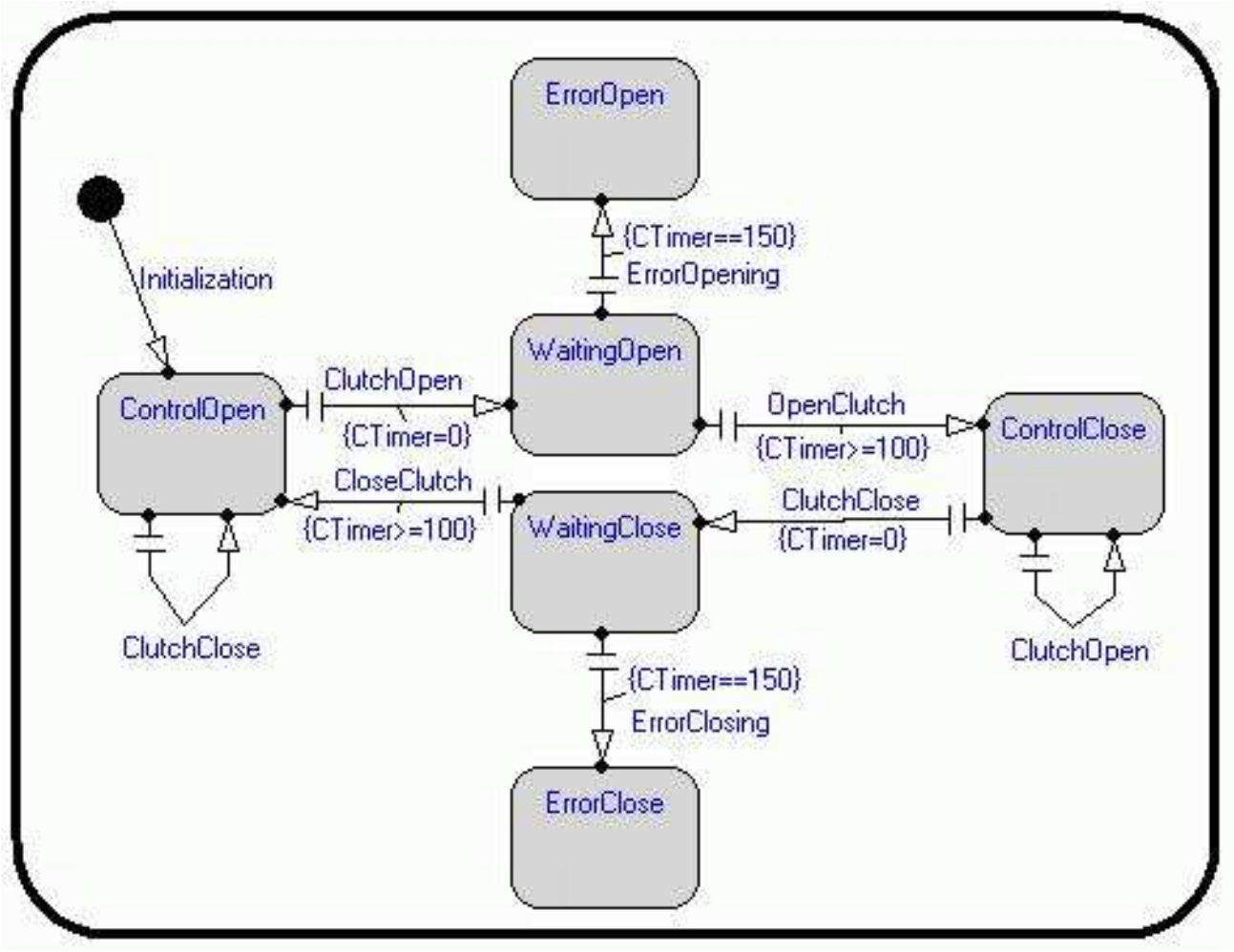
CLASS DIAGRAM OF CLUTCH CONTROLLER



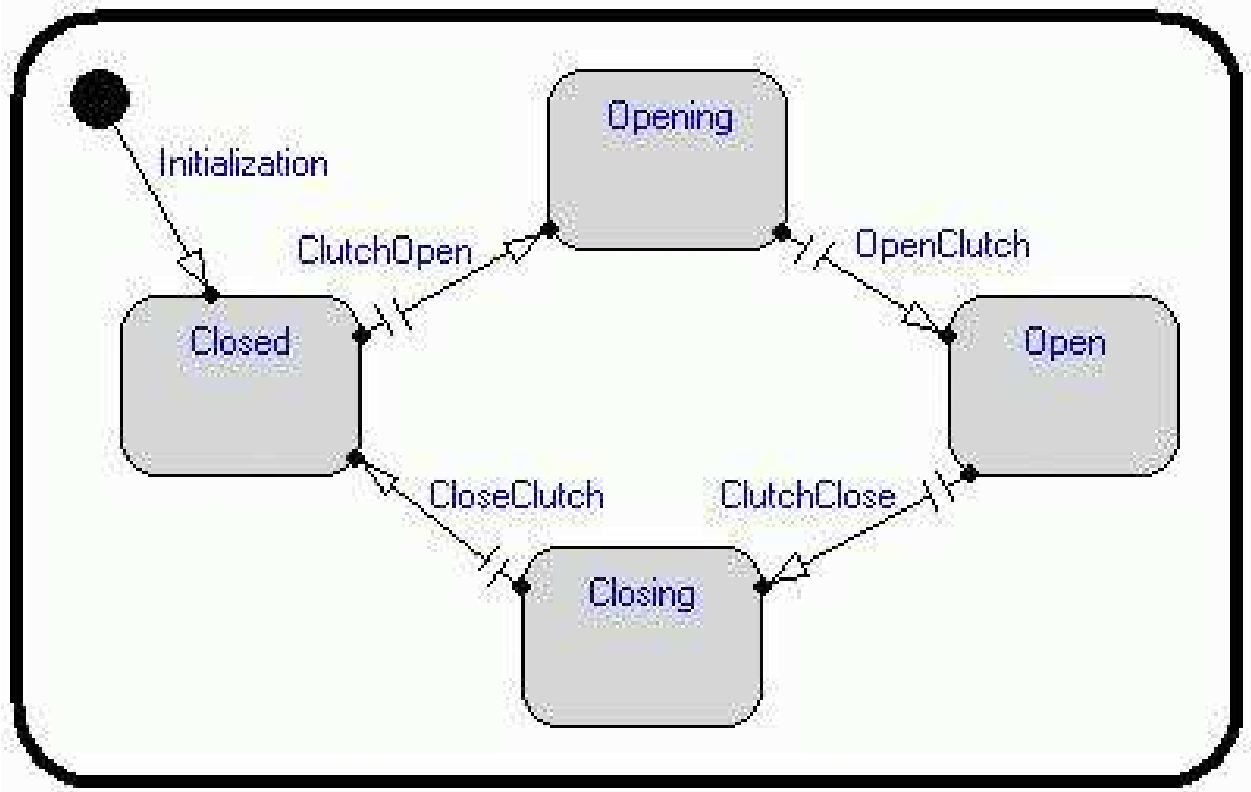
CLASS DIAGRAM OF GEAR CONTROLLER



STATECHART DIAGRAM OF CLUTCH CONTROLLER



STATECHART DIAGRAM OF CLUTCH COMPONENT



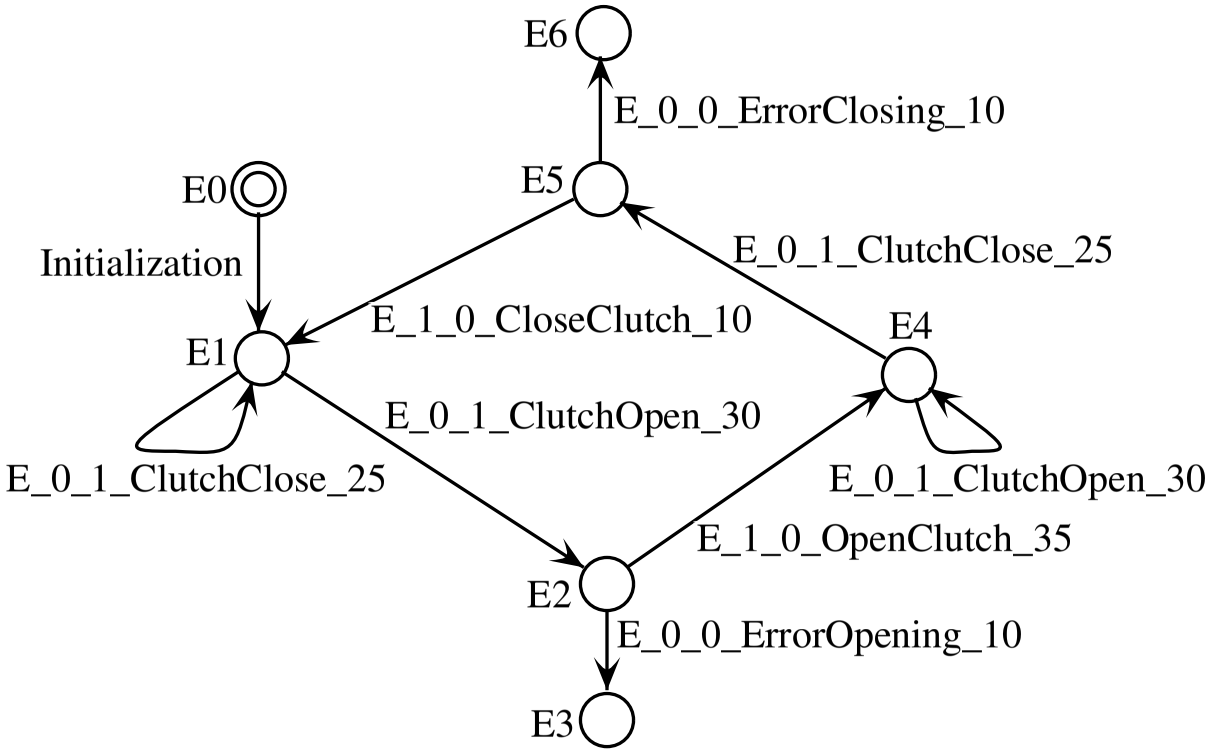
TIME ANNOTATIONS IN THE CODE

- Implementation with Synchronous Active Objects
- Label structure:
  //! { *Calling active object number, receiving active object number, method name, time units* }
- Partition into: *Control* part and *environment* part
- Label generation on `Java method` calls

TIME ANNOTATIONS..CONTD..

```
public class Gear {
      ...
      active class ClutchController{
      ...
      accept OpenClutch;
      //! {1, 0, OpenClutch, 35}
      ...
      }
      active class Clutch{
      ...
      accept ClutchOpen;
      //! {0, 1, ClutchOpen, 30}
      ...
      }
```

FINITE STATE MODEL FOR CLUTCH CONTROLLER



TIME COMPUTATION ALGORITHM

{ P: *program* controller, E: *environment* and }

{ $(P \uparrow E)$: edge with transition from P to E.}

Input: *File description of finite state model.*

Output: *Sum of execution times of all possible paths.*

1. Read the labels, edges and vertices.
2. Search the new edge $(E \uparrow P)$.
3. From the sinking vertex of the selected edge find all possible paths ending on next new edge $(E \uparrow P)$. All the paths are terminating with either $(P \uparrow E)$ or $(P \uparrow P)$ type of edge.
4. Compute the time on all the paths by summing up the execution times specified on the labels.
5. Display the transition that takes longest time response into Statechart diagram of controller.

VALIDATION..CONTD..

$E_1 \rightarrow E_2$:

Time(E_1_0_CloseClutch_10 + E_0_1_ClutchOpen_30) = 40 units

Time(E_1_0_CloseClutch_10 + E_0_1_ClutchClose_25
+ E_0_1_ClutchOpen_30) = 65 units

$E_1 \rightarrow E_3$:

Time(E_1_0_CloseClutch_10 + E_0_1_ClutchClose_25
+ E_0_1_ClutchOpen_30 + E_0_0_ErrorOpening_10) = 75 units

$E_4 \rightarrow E_5$:

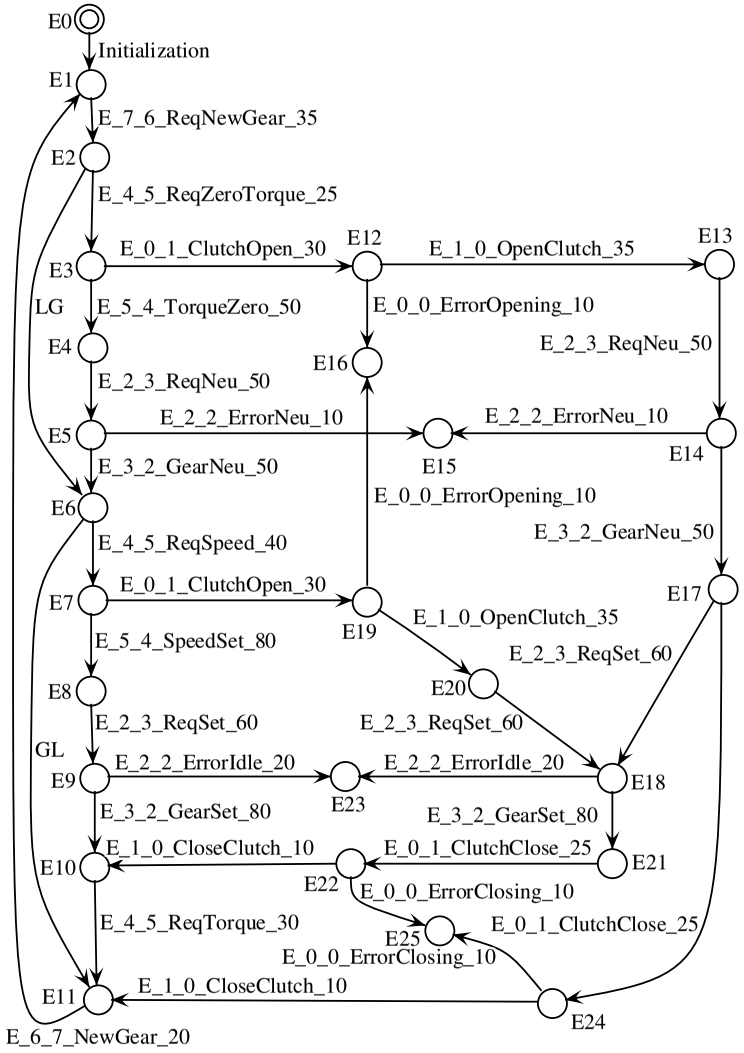
Time(E_1_0_OpenClutch_35 + E_0_1_ClutchOpen_30
+ E_0_1_ClutchClose_25) = 90 units

Time(E_1_0_OpenClutch_35 + E_0_1_ClutchClose_25) = 60 units

$E_4 \rightarrow E_6$:

Time(E_1_0_OpenClutch_35 + E_0_1_ClutchOpen_30
+ E_0_1_ClutchClose_25 + E_0_0_ErrorClosing_10) = 100 units

FINITE STATE MODEL FOR GEAR CONTROLLER



VALIDATION..CONTD..

$E_2 \rightarrow E_3$:

Time(E_7_6_ReqNewGear_35 + E_4_5_ReqZeroTorque_25) = 60 units

...

$E_8 \rightarrow E_9$:

Time(E_5_4_SpeedSet_80 + E_2_3_ReqSet_60) = 140 units

...

$E_{10} \rightarrow E_1$:

Time(E_3_2_GearSet_80 + E_4_5_ReqTorque_30
+ E_6_7_NewGear_20) = 130 units

...

$E_{21} \rightarrow E_{25}$:

Time(E_3_2_GearSet_80 + E_0_1_ClutchClose_25
+ E_0_0_ErrorClosing_10) = 115 units

$E_8 \rightarrow E_{23}$:

Time(E_5_4_SpeedSet_80 + E_2_3_ReqSet_60
+ E_2_2_ErrorIdle_20) = 160 units

DISCUSSION

- Real-time behavioral patterns.
- Architectural patterns.
- Integration into the design phase.
- Internal inconsistencies.

THANK YOU!