

Politecnico di Milano
Formal Methods for Concurrent and
Real-Time Systems

Computer Controller Automatic Transmission
(Mandatory Part and Optional Part)

Alessandra Bonetto
Filippo Sironi
Matteo Villa

2009

Contents

1	CCAT Class	5
2	Vehicle/EngineSpeedSensor Classes	21
3	PlanetaryGearSet Class	24
4	HydraulicSystem Class	30
5	TransmissionControlUnit Class	33
6	Annotations	38
7	Properties	39

List of Figures

1	Computer Controller Automatic Transmission	7
---	--	---

Listings

1	ComputerControlledAutomaticTransmission.trio	5
2	ComputerControlledAutomaticTransmission.trio	8
3	ComputerControlledAutomaticTransmission.lisp	11
4	VehicleSpeedSensor.trio	21
5	EngineSpeedSensor.trio	22
6	PlanetaryGearSet.trio	24
7	HydraulicSystem.trio	30
8	TransmissionControlUnit.trio	33
9	Property 1	39
10	Property 2	39
11	Property 3	39

1 CCAT Class

The *ComputerControlledAutomaticTransmission* class is formalized thanks to the code reported in Listing 1 while Figure 1 shows the *big picture* of our complete designed.

Listing 1: ComputerControlledAutomaticTransmission.trio

```

1  class ComputerControlledAutomaticTransmission
2
3  import :
4      HydraulicSystem ,
5      PlanetaryGearSet ,
6      TransmissionControlUnit ,
7      VehicleSpeedSensor ,
8      EngineSpeedSensor ;
9
10 signature :
11
12 visible :
13     torqueConverterState ,
14     vehicleSpeed ,
15     engineSpeed ;
16
17 temporal domain : real ;
18
19 domains :
20     TorqueConverterState : { Attached , Detached } ;
21
22 items :
23     TD total torqueConverterState : TorqueConverterState ;
24     TD total vehicleSpeed : integer ;
25     TD total engineSpeed : integer ;
26
27 modules :
28     hydraulicSystem : HydraulicSystem ;
29     planetaryGearSet : PlanetaryGearSet ;
30     transmissionControlUnit : TransmissionControlUnit ;
31     vehicleSpeedSensor : VehicleSpeedSensor ;
32     engineSpeedSensor : EngineSpeedSensor ;
33
34 connections :
35     (direct EngineSpeedSensor.actualSpeed , engineSpeed)
36     (direct vehicleSpeedSensor.actualSpeed , vehicleSpeed)

```

```
37 (direct planetaryGearSet.transmissionShaftState ,
38     torqueConverterState)
39 (direct planetaryGearSet.gearShift ,
40     hydraulicSystem.gearShift)
41 (direct planetaryGearSet.gearDrive ,
42     hydraulicSystem.gearDrive)
43 (direct planetaryGearSet.gearPark ,
44     hydraulicSystem.gearPark)
45 (direct planetaryGearSet.gearReverse ,
46     hydraulicSystem.gearReverse)
47 (direct hydraulicSystem.controlGearShift ,
48     transmissionControlUnit.controlGearShift)
49 (direct transmissionControlUnit.receiveEngineSpeed ,
50     engineSpeedSensor.sendSpeed)
51 (direct transmissionControlUnit.receiveVehicleSpeed ,
52     vehicleSpeedSensor.sendSpeed)
53 end
```

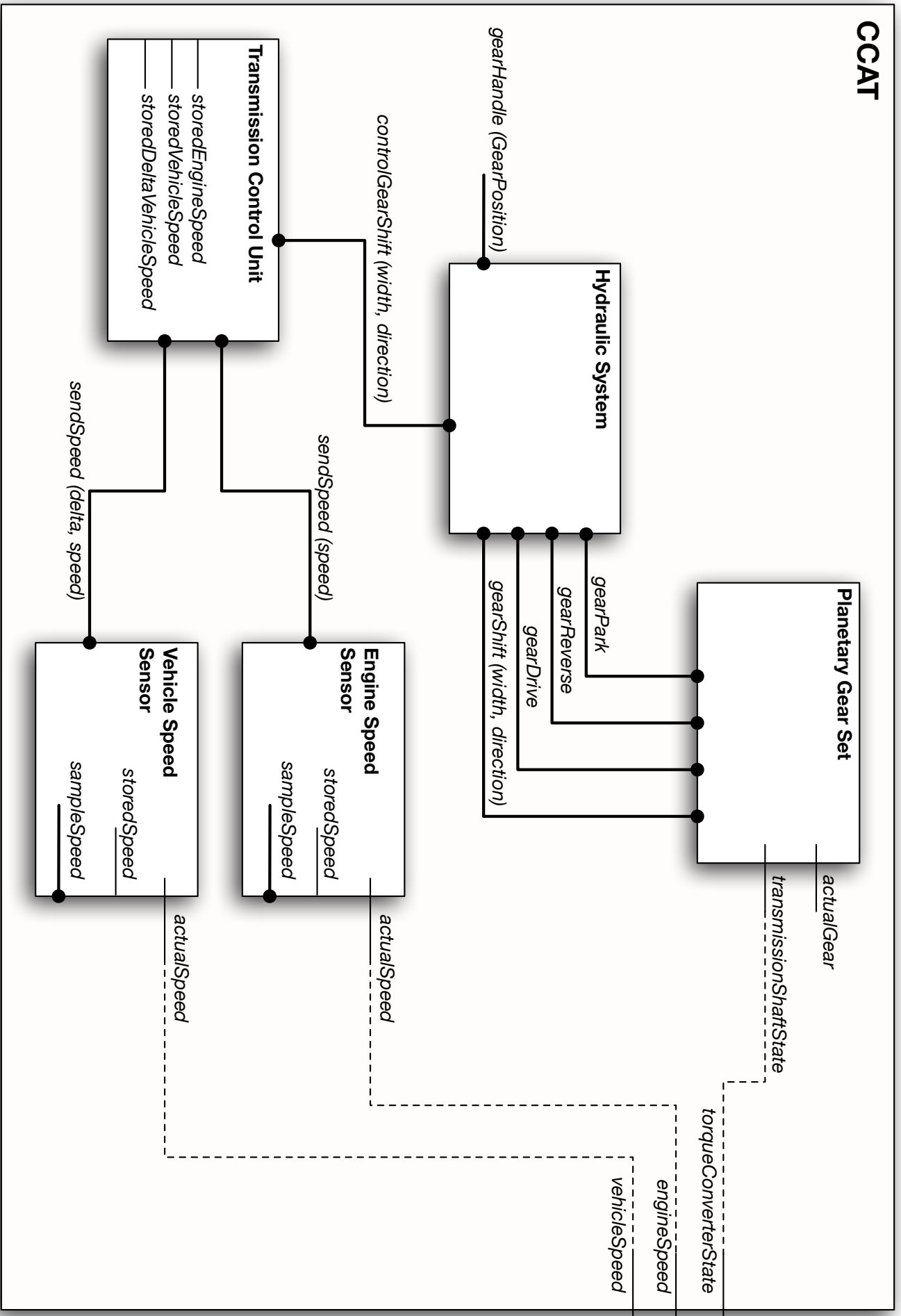


Figure 1: Computer Controller Automatic Transmission

Due to the fact that a TRIO specification is not decidable we have decided to focus our verification process only on the Hydraulic System, described in Section 4, and on the Planetary Gear Set, described in Section 3 and we have used a decidable subset of the TRIO language.

The specification is reported in Listing 2.

Listing 2: ComputerControlledAutomaticTransmission.trio

```

1  variables
2      controlGearShift: [0..2],
3      gearHandle: [0..3],
4      gearShift: [0..5],
5      actualGear: [0..3],
6      transmissionShaftState: [0..1]
7
8  constants
9      Nothing = 0,
10     TCUShiftOneUp = 1, TCUShiftOneDown = 2,
11     HandleShiftDrive = 1, HandleShiftPark = 2,
12     HandleShiftReverse = 3,
13     ShiftOneUp = 1, ShiftOneDown = 2, ShiftDrive = 3,
14     ShiftPark = 4, ShiftReverse = 5,
15     First = 0, Second = 1, Park = 2, Reverse = 3,
16     Detached = 0, Attached = 1,
17     FluidDelay = 1, ShiftDelay = 1
18
19  axioms
20  Mechanic:
21      (actualGear = First ->
22          gearShift = Nothing | gearShift = ShiftOneUp |
23          gearShift = ShiftPark | gearShift =
24          ShiftReverse
25      ) &
26      (actualGear = Second ->
27          gearShift = Nothing | gearShift = ShiftOneDown
28      ) &
29      (actualGear = Park ->
30          gearShift = Nothing | gearShift = ShiftDrive |
31          gearShift = ShiftReverse
32      ) &
33      (actualGear = Reverse ->
34          gearShift = Nothing | gearShift = ShiftDrive |
35          gearShift = ShiftPark
36      ) &

```



```

31      (gearShift = ShiftOneUp -> transmissionShaftState
32        = Attached) &
33      (gearShift = ShiftDrive | gearShift = ShiftPark |
34        gearShift = ShiftReverse ->
35        transmissionShaftState = Detached
36      ) &
37      (transmissionShaftState = Attached -> actualGear =
38        First | actualGear = Second | actualGear =
39        Reverse) &
40      (actualGear = Park -> transmissionShaftState =
41        Detached);
42
43  GearShiftCommand:
44      (controlGearShift = TCUShiftOneUp ->
45        Lasts_ii(gearHandle = Nothing, FluidDelay) &
46        Lasts_ei(controlGearShift = Nothing,
47          FluidDelay) &
48        Futr(gearShift = ShiftOneUp, FluidDelay)
49      ) &
50      (controlGearShift = TCUShiftOneDown ->
51        Lasts_ii(gearHandle = Nothing, FluidDelay) &
52        Lasts_ei(controlGearShift = Nothing,
53          FluidDelay) &
54        Futr(gearShift = ShiftOneDown, FluidDelay)
55      );
56
57  GearHandleCommand:
58      (gearHandle = HandleShiftDrive ->
59        Lasts_ii(controlGearShift = Nothing &
60          transmissionShaftState = Detached,
61          FluidDelay) &
62        Lasts_ei(gearHandle = Nothing, FluidDelay) &
63        Futr(gearShift = ShiftDrive, FluidDelay)
64      ) &
65      (gearHandle = HandleShiftPark ->
66        Lasts_ii(controlGearShift = Nothing &
67          transmissionShaftState = Detached,
68          FluidDelay) &
69        Lasts_ei(gearHandle = Nothing, FluidDelay) &
70        Futr(gearShift = ShiftPark, FluidDelay)
71      ) &
72      (gearHandle = HandleShiftReverse ->

```

```

62         Lasts_ii(controlGearShift = Nothing &
                  transmissionShaftState = Detached,
                  FluidDelay) &
63         Lasts_ei(gearHandle = Nothing, FluidDelay) &
64         Futr(gearShift = ShiftReverse, FluidDelay)
65     );
66
67     GearShiftFirst:
68         (actualGear = First & gearShift = ShiftOneUp ->
69         Lasts_ei(gearShift = Nothing, ShiftDelay) &
70         Futr(actualGear = Second, ShiftDelay)
71         ) &
72         (actualGear = First & gearShift = ShiftPark ->
73         Lasts_ii(transmissionShaftState = Detached,
74         ShiftDelay) &
75         Lasts_ei(gearShift = Nothing, ShiftDelay) &
76         Futr(actualGear = Park, ShiftDelay)
77         ) &
78         (actualGear = First & gearShift = ShiftReverse ->
79         Lasts_ii(transmissionShaftState = Detached,
80         ShiftDelay) &
81         Lasts_ei(gearShift = Nothing, ShiftDelay) &
82         Futr(actualGear = Reverse, ShiftDelay)
83         );
84
85     GearShiftSecond:
86         (actualGear = Second & gearShift = ShiftOneDown ->
87         Lasts_ei(gearShift = Nothing, ShiftDelay) &
88         Futr(actualGear = First, ShiftDelay)
89         );
90
91     GearShiftPark:
92         (actualGear = Park & gearShift = ShiftDrive ->
93         Lasts_ii(transmissionShaftState = Detached,
94         ShiftDelay) &
95         Lasts_ei(gearShift = Nothing, ShiftDelay) &
96         Futr(actualGear = First, ShiftDelay)
97         ) &
98         (actualGear = Park & gearShift = ShiftReverse ->
99         Lasts_ii(transmissionShaftState = Detached,
100        ShiftDelay) &
101        Lasts_ei(gearShift = Nothing, ShiftDelay) &
102        Futr(actualGear = Reverse, ShiftDelay)
103        );

```

```

97         );
98
99     GearShiftReverse:
100         (actualGear = Reverse & gearShift = ShiftDrive ->
101           Lasts_ii(transmissionShaftState = Detached,
102                   ShiftDelay) &
103           Lasts_ei(gearShift = Nothing, ShiftDelay) &
104           Futr(actualGear = First, ShiftDelay)
105         ) &
106         (actualGear = Reverse & gearShift = ShiftPark ->
107           Lasts_ii(transmissionShaftState = Detached,
108                   ShiftDelay) &
109           Lasts_ei(gearShift = Nothing, ShiftDelay) &
110           Futr(actualGear = Park, ShiftDelay)
111         );

```

The same specification reported in Listings 2 has been ported also in Zot and is listed in Listings 3.

Listing 3: ComputerControlledAutomaticTransmission.lisp

```

1  (asdf:operate 'asdf:load-op 'bezot)
2  (use-package :trio-utils)
3
4  ; Constants
5  (defvar Nothing 0)
6
7  (defvar TCUShiftOneUp 1)
8  (defvar TCUShiftOneDown 2)
9
10 (defvar HandleDrive 1)
11 (defvar HandlePark 2)
12 (defvar HandleReverse 3)
13
14 (defvar ShiftOneUp 1)
15 (defvar ShiftOneDown 2)
16 (defvar ShiftDrive 3)
17 (defvar ShiftPark 4)
18 (defvar ShiftReverse 5)
19
20 (defvar First 0)
21 (defvar Second 1)
22 (defvar Park 2)
23 (defvar Reverse 3)
24

```

```

25 (defvar Detached 0)
26 (defvar Attached 1)
27
28 (defvar FluidDelay 1)
29 (defvar ShiftDelay 1)
30
31 ; Domains
32 (defvar ControlGearShiftDomain (loop for i from 0 to 2
    collect i))
33 (defvar GearHandleDomain (loop for i from 0 to 3 collect
    i))
34 (defvar GearShiftDomain (loop for i from 0 to 5 collect i))
35 (defvar ActualGearDomain (loop for i from 0 to 3 collect
    i))
36 (defvar TransmissionShaftStateDomain (loop for i from 0 to
    1 collect i))
37
38 ; Variables
39 (define-variable controlGearShift ControlGearShiftDomain)
40 (define-variable gearHandle GearHandleDomain)
41 (define-variable gearShift GearShiftDomain)
42 (define-variable actualGear ActualGearDomain)
43 (define-variable transmissionShaftState
    TransmissionShaftStateDomain)
44
45 ; Axioms
46 (defvar ControlGearShiftMutualExclusion
47   (&&
48     (-E- x '(0 1 2) (-P- controlGearShift x))
49     (-A- x '(0 1 2)
50       (->
51         (-P- controlGearShift x)
52         (-A- y '(0 1 2) (-> (!! (= x y)) (!! (-P-
            controlGearShift y))))))
53   )
54 )
55 )
56 )
57
58 (defvar GearHandleMutualExclusion
59   (&&
60     (-E- x '(0 1 2 3) (-P- gearHandle x))
61     (-A- x '(0 1 2 3)

```

```

62         (->
63         (-P- gearHandle x)
64         (-A- y '(0 1 2 3) (-> (!! (= x y)) (!!
        (-P- gearHandle y))))))
65     )
66 )
67 )
68 )
69
70 (defvar GearShiftMutualExclusion
71   (&&
72     (-E- x '(0 1 2 3 4 5) (-P- gearShift x))
73     (-A- x '(0 1 2 3 4 5)
74       (->
75         (-P- gearShift x)
76         (-A- y '(0 1 2 3 4 5) (-> (!! (= x y))
        (!! (-P- gearShift y))))))
77     )
78   )
79 )
80 )
81
82 (defvar ActualGearMutualExclusion
83   (&&
84     (-E- x '(0 1 2 3) (-P- actualGear x))
85     (-A- x '(0 1 2 3)
86       (->
87         (-P- actualGear x)
88         (-A- y '(0 1 2 3) (-> (!! (= x y)) (!!
        (-P- actualGear y))))))
89     )
90   )
91 )
92 )
93
94 (defvar TransmissionShaftStateMutualExclusion
95   (&&
96     (-E- x '(0 1) (-P- transmissionShaftState x))
97     (-A- x '(0 1)
98       (->
99         (-P- transmissionShaftState x)
100        (-A- y '(0 1) (-> (!! (= x y)) (!! (-P-
        transmissionShaftState y))))))

```

```

101         )
102     )
103 )
104 )
105
106 (defvar Mechanic
107     (&&
108         (->
109             (actualGear-is First)
110             (||
111                 (gearShift-is Nothing)
112                 (gearShift-is ShiftOneUp)
113                 (gearShift-is ShiftPark)
114                 (gearShift-is ShiftReverse)
115             )
116         )
117         (->
118             (actualGear-is Second)
119             (|| (gearShift-is Nothing) (gearShift-is
120                 ShiftOneDown))
121         )
122         (->
123             (actualGear-is Park)
124             (|| (gearShift-is Nothing) (gearShift-is
125                 ShiftDrive) (gearShift-is ShiftReverse))
126         )
127         (->
128             (actualGear-is Reverse)
129             (|| (gearShift-is Nothing) (gearShift-is
130                 ShiftDrive) (gearShift-is ShiftPark))
131         )
132         (-> (gearShift-is ShiftOneUp)
133             (transmissionShaftState-is Attached))
134         (->
135             (||
136                 (gearShift-is ShiftDrive)
137                 (gearShift-is ShiftPark)
138                 (gearShift-is ShiftReverse)
139             )
140             (transmissionShaftState-is Detached)
141         )
142         (->
143             (transmissionShaftState-is Attached)

```

```

140         (|| (actualGear-is First) (actualGear-is
141             Second) (actualGear-is Reverse))
142     )
143     (-> (actualGear-is Park)
144         (transmissionShaftState-is Detached))
145     (->
146         (&&
147             (controlGearShift-is Nothing)
148             (gearHandle-is Nothing)
149             )
150         (Futr (gearShift-is Nothing) FluidDelay)
151     )
152     (-A- x '(0 1 2 3)
153         (->
154             (&& (-P- actualGear x) (gearShift-is
155                 Nothing))
156             (Lasts_ii (-P- actualGear x) ShiftDelay)
157         )
158     )
159 )
160 (defvar GearShiftCommand
161     (&&
162         (->
163             (controlGearShift-is TCUShiftOneUp)
164             (Futr (gearShift-is ShiftOneUp) FluidDelay)
165         )
166         (->
167             (controlGearShift-is TCUShiftOneDown)
168             (Futr (gearShift-is ShiftOneDown) FluidDelay)
169         )
170     )
171 )
172 (defvar GearHandleCommand
173     (&&
174         (->
175             (gearHandle-is HandleDrive)
176             (&&
177                 (Lasts_ii (&& (controlGearShift-is
178                     Nothing) (transmissionShaftState-is
179                         Detached)) FluidDelay)
180             )
181         )
182     )
183 )

```

```

178         (Lasts_ei (gearHandle-is Nothing)
179                 FluidDelay)
180         (Futr (gearShift-is ShiftDrive) FluidDelay)
181     )
182 (->
183     (gearHandle-is HandlePark)
184     (&&
185         (Lasts_ii (&& (controlGearShift-is
186                     Nothing) (transmissionShaftState-is
187                         Detached)) FluidDelay)
188         (Lasts_ei (gearHandle-is Nothing)
189                 FluidDelay)
190         (Futr (gearShift-is ShiftPark) FluidDelay)
191     )
192 )
193 (->
194     (gearHandle-is HandleReverse)
195     (&&
196         (Lasts_ii (&& (controlGearShift-is
197                     Nothing) (transmissionShaftState-is
198                         Detached)) FluidDelay)
199         (Lasts_ei (gearHandle-is Nothing)
200                 FluidDelay)
201         (Futr (gearShift-is ShiftReverse)
202                 FluidDelay)
203     )
204 )
205 )
206 )
207 )
208 )
209 )
210 )
211
212 (defvar GearShiftFirst
213     (&&
214         (->
215             (&& (actualGear-is First) (gearShift-is
216                 ShiftOneUp))
217             (&&
218                 (Lasts_ei (gearShift-is Nothing)
219                         ShiftDelay)
220                 (Futr (actualGear-is Second) ShiftDelay)
221             )
222         )
223     )
224 )
225 (->

```



```

211         (&& (actualGear-is First) (gearShift-is
212             ShiftPark))
213         (&&
214             (Lasts_ii (transmissionShaftState-is
215                 Detached) ShiftDelay)
216             (Lasts_ei (gearShift-is Nothing)
217                 ShiftDelay)
218             (Futr (actualGear-is Park) ShiftDelay)
219         )
220     )
221     (->
222         (&& (actualGear-is First) (gearShift-is
223             ShiftReverse))
224         (&&
225             (Lasts_ii (transmissionShaftState-is
226                 Detached) ShiftDelay)
227             (Lasts_ei (gearShift-is Nothing)
228                 ShiftDelay)
229             (Futr (actualGear-is Reverse) ShiftDelay)
230         )
231     )
232 )
233 )
234 )
235 )
236 )
237 )
238
239 (defvar GearShiftSecond
240     (->
241         (&& (actualGear-is Second) (gearShift-is
242             ShiftOneDown))
243         (&&
244             (Lasts_ei (gearShift-is Nothing) ShiftDelay)
245             (Futr (actualGear-is First) ShiftDelay)
246         )
247     )
248 )
249
250 (defvar GearShiftPark
251     (&&
252         (->
253             (&& (actualGear-is Park) (gearShift-is
254                 ShiftDrive))
255             (&&
256                 (Lasts_ii (transmissionShaftState-is
257                     Detached) ShiftDelay)

```

```

245         (Lasts_ei (gearShift-is Nothing)
246             ShiftDelay)
247     (Futr (actualGear-is First) ShiftDelay)
248 )
249 (->
250     (&& (actualGear-is Park) (gearShift-is
251         ShiftReverse))
252     (&&
253         (Lasts_ii (transmissionShaftState-is
254             Detached) ShiftDelay)
255         (Lasts_ei (gearShift-is Nothing)
256             ShiftDelay)
257         (Futr (actualGear-is Reverse) ShiftDelay)
258     )
259 )
260 (defvar GearShiftReverse
261     (&&
262         (->
263             (&& (actualGear-is Reverse) (gearShift-is
264                 ShiftDrive))
265             (&&
266                 (Lasts_ii (transmissionShaftState-is
267                     Detached) ShiftDelay)
268                 (Lasts_ei (gearShift-is Nothing)
269                     ShiftDelay)
270                 (Futr (actualGear-is First) ShiftDelay)
271             )
272             (->
273                 (&& (actualGear-is Reverse) (gearShift-is
274                     ShiftPark))
275                 (&&
276                     (Lasts_ii (transmissionShaftState-is
277                         Detached) ShiftDelay)
278                     (Lasts_ei (gearShift-is Nothing)
279                         ShiftDelay)
280                     (Futr (actualGear-is Park) ShiftDelay)
281                 )
282             )
283         )
284     )

```

```

278 |     )
279 | )
280 |
281 | (defvar ComputerControlledAutomaticTransmission
282 |   (Alw
283 |     (&&
284 |       ControlGearShiftMutualExclusion
285 |       GearHandleMutualExclusion
286 |       GearShiftMutualExclusion
287 |       ActualGearMutualExclusion
288 |       TransmissionShaftStateMutualExclusion
289 |       Mechanic
290 |       GearShiftCommand
291 |       GearHandleCommand
292 |       GearShiftFirst
293 |       GearShiftSecond
294 |       GearShiftPark
295 |       GearShiftReverse
296 |     )
297 |   )
298 | )
299 |
300 | (defvar PropertyOne
301 |   (->
302 |     (&& (actualGear-is First) (controlGearShift-is
303 |       TCUShiftOneUp))
304 |     (Futr (actualGear-is Second) (+ FluidDelay
305 |       ShiftDelay))
306 |   )
307 | )
308 |
309 | (defvar PropertyTwo
310 |   (->
311 |     (&& (actualGear-is First) (gearHandle-is
312 |       HandleReverse))
313 |     (&&
314 |       (Futr (actualGear-is Reverse) (+ FluidDelay
315 |         ShiftDelay))
316 |       (Lasts-ii (transmissionShaftState-is Detached)
317 |         (+ FluidDelay ShiftDelay))
318 |     )
319 |   )
320 | )

```

```
316 |
317 | (defvar PropertyThree
318 |   (->
319 |     (&& (actualGear-is First) (gearHandle-is
320 |       HandlePark))
321 |     (&&
322 |       (Futr (actualGear-is Park) (+ FluidDelay
323 |         ShiftDelay))
324 |       (Until (transmissionShaftState-is Detached)
325 |         (!! (gearHandle-is Nothing))))
326 |   )
327 | )
328 |
329 | (bezot:zot 20 ComputerControlledAutomaticTransmission)
330 | ;(bezot:zot 20 (&& ComputerControlledAutomaticTransmission
331 |   (!! (Alw PropertyOne))))
332 | ;(bezot:zot 20 (&& ComputerControlledAutomaticTransmission
333 |   (!! (Alw PropertyTwo))))
334 | ;(bezot:zot 20 (&& ComputerControlledAutomaticTransmission
335 |   (!! (Alw PropertyThree))))
```

2 Vehicle/EngineSpeedSensor Classes

The *VehicleSpeedSensor* is formalized thanks to the code reported in Listing 4 while the *EngineSpeedSensor* is formalized thanks to the code reported in Listing 5.

During the formalization of sensors we decided to simplify the design assuming that every time a `sampleSpeed` event occurs the state variable `actualSpeed` - which is time dependent and total - is automatically updated with the actual measured speed. This means we don't provide any axioms formalizing this behavior.

Moreover, we specified the starting point of the constant frequency sample chain saying that sometimes in the past there was a `sampleSpeed` occurrence. Further more, we guarantee that `sampleSpeed` events will occur at constant frequency. In addition, if the sensor has memory we imposed that the `storedValue` is equal to 0. These can be considered just like the "initial conditions" of the system.

At the end, we guaranteed a sensor performs the needed action if and only if a sample event occurs.

We didn't write any axioms specifying the fact that a `sendSpeed` event is mutually exclusive with itself due to the `total` time dependent parameter it accepts.

Listing 4: *VehicleSpeedSensor.trio*

```

1  class VehicleSpeedSensor (const sampleInterval , const
    sampleDelay)
2
3  signature :
4
5  visible :
6      actualSpeed ,
7      sendSpeed ;
8
9  temporal domain : real ;
10
11 items :
12     TI sampleInterval : real ;
13     TI sampleDelay : real ;
14     TD total storedSpeed : integer ;
15     TD total actualSpeed : integer ;
16     event sendSpeed (integer , integer) ;
17     event sampleSpeed ;
18

```

```

19 axioms:
20 vars:
21     deltaSpeed: integer;
22     speed: integer;
23 formulae:
24     SpeedValues:
25         actualSpeed >= 0 and storedSpeed >= 0;
26
27     BeginSample:
28         SomP (storedSpeed = 0 & sampleSpeed);
29
30     SamplingDefinition:
31         sampleSpeed implies Futr (sampleSpeed ,
32             sampleInterval) and not Lasts (sampleSpeed ,
33             sampleInterval);
34
35     SamplingAction:
36         sampleSpeed implies Futr (deltaSpeed = actualSpeed
37             - storedSpeed and speed = actualSpeed and
38             sendSpeed (deltaSpeed , speed) and Lasts
39             (storedSpeed = actualSpeed , sampleInterval),
40             sampleDelay);
41
42     SendSpeed:
43         deltaSpeed = actualSpeed - storedSpeed and
44         actualSpeed = speed and sendSpeed (deltaSpeed ,
45             speed) implies Past (sampleSpeed , sampleDelay);
46
47 end

```

Listing 5: EngineSpeedSensor.trio

```

1 class EngineSpeedSensor (const sampleInterval , const
2     sampleDelay)
3 signature:
4
5 visible: actualSpeed , sendSpeed;
6
7 temporal domain: real;
8
9 items:
10     TI sampleInterval: real;
11     TI sampleDelay: real;

```

```
12     TD total actualSpeed: integer;  
13     event sendSpeed (integer);  
14     event sampleSpeed;  
15  
16     axioms:  
17     vars:  
18         speed: integer;  
19     formulae:  
20         SpeedValues:  
21             actualSpeed >= 0;  
22  
23         BeginSample:  
24             SomP (sampleSpeed);  
25  
26         SamplingDefinition:  
27             sampleSpeed implies Futr (sampleSpeed ,  
28                 sampleInterval) and not Lasts (sampleSpeed ,  
29                 sampleInterval);  
30  
31         SampleSpeedActions:  
32             sampleSpeed implies Futr (actualSpeed = speed and  
33                 sendSpeed (speed), sampleDelay);  
34  
35         SendSpeed:  
36             actualSpeed = speed and sendSpeed (speed) implies  
37                 Past (sampleSpeed , sampleDelay);  
38  
39     end
```

3 PlanetaryGearSet Class

The *PlanetaryGearSet* class is formalized thanks to the code reported in Listing 6.

The Planetary Gear Set guarantees that every time a gear shift event occurs the `actualGear` will be maintained until the shift is finished.

Inside this component are defined all axioms limiting gear shifts to effective ones only (e.g. it is impossible to shift down a gear if `actualGear` is `First`). The Planetary Gear Set permits to shift up to two gear at the same time (as the specification asks), however, the Transmission Control Unit doesn't use this possibility because in a real Planetary Gear Set this is not possible.

Moreover, through the formalization of the Planetary Gear Set we impose that we can't receive a gear shift event if we are in the middle of a gear shift. Different gear shifting times are defined for different gears and different steps.

The gears `Drive`, `Park`, and `Reverse` can be selected if and only if the transmission shaft is decoupled from the engine.

The state of the Planetary Gear Set changes if and only if an event occurs.

Listing 6: PlanetaryGearSet.trio

```

1  class PlanetaryGearSet (const singleGearShiftDelay , const
    dualGearShiftDelay , const driveGearShiftDelay , const
    parkGearShiftDelay , const reverseGearShiftDelay )
2
3  signature :
4
5  visible :
6      actualGear ,
7      transmissionShaftState ,
8      gearShift ,
9      gearDrive ,
10     gearPark ,
11     gearReverse ,
12
13  temporal domain : real ;
14
15  domains :
16      Gear : {First , Second , Third , Park , Reverse } ;
17      TransmissionShaftState : {Attached , Detached } ;
18      ShiftWidth : 1..2 ;
19      ShiftDirection : {Up , Down } ;
20
21  items :
22      TI singleGearShiftDelay : real ;

```



```

23 TI dualGearShiftDelay: real;
24 TI driveGearShiftDelay: real;
25 TI parkGearShiftDelay: real;
26 TI reverseGearShiftDelay: real;
27 TD total actualGear: Gear;
28 TD total transmissionShaftState:
    TransmissionShaftState;
29 event gearShift (ShiftWidth, ShiftDirection);
30 event gearDrive;
31 event gearPark;
32 event gearReverse;
33
34 axioms:
35 vars:
36     gearShiftWidth: ShiftWidth;
37     gearShiftWidth2: ShiftWidth;
38     gearShiftDirection: ShiftDirection;
39     gearShiftDirection2: ShiftDirection;
40     gear: Gear;
41 formulae:
42     Mechanics:
43         all gearShiftWidth (gearShiftDirection = Up ->
            transmissionShaftState=Attached);
44
45     GearShiftDrive:
46         gearDrive implies transmissionShaftState =
            Detached;
47
48     GearShiftFirst:
49         (actualGear = First implies not gearDrive and not
            ex gearShiftWidth (gearShiftDirection = Down
            and gearShift (gearShiftWidth,
            gearShiftDirection))) and
50         (actualGear = First implies SomF (gearPark or
            gearReverse or ex gearShiftWidth,
            gearShiftDirection (gearShift (gearShiftWidth,
            gearShiftDirection)))) and
51         (actualGear = First and gearShiftWidth = 1 and
            gearShiftDirection = Up and gearShift
            (gearShiftWidth, gearShiftDirection) implies
            Lasts (actualGear = First,
            singleGearShiftDelay) and Futr (actualGear =
            Second, singleGearShiftDelay)) and

```

```

52      (actualGear = First and gearShiftWidth = 2 and
        gearShiftDirection = Up and gearShift
        (gearShiftWidth, gearShiftDirection) implies
        Lasts (actualGear = First, dualGearShiftDelay)
        and Futr (actualGear = Third,
        dualGearShiftDelay) and
53      (actualGear = First and gearPark implies Lasts
        (actualGear = First, parkGearShiftDelay) and
        Futr (actualGear = Park, parkGearShiftDelay))
        and
54      (actualGear = First and gearReverse implies Lasts
        (actualGear = First, reverseGearShiftDelay) and
        Futr (actualGear = Reverse,
        reverseGearShiftDelay));

55  GearShiftSecond:
56
57      (actualGear = Second implies not gearDrive and not
        gearPark and not gearReverse and not ex
        gearShiftDirection (gearShiftWidth = 2 and
        gearShift (gearShiftWidth,
        gearShiftDirection))) and
58      (actualGear = Second implies SomF (ex
        gearShiftDirection (gearShiftWidth = 1 and
        gearShift (gearShiftWidth,
        gearShiftDirection)))) and
59      (actualGear = Second and gearShiftWidth = 1 and
        gearShiftDirection = Up and gearShift
        (gearShiftWidth, gearShiftDirection) implies
        Lasts (actualGear = Second,
        singleGearShiftDelay) and Futr (actualGear =
        Third, singleGearShiftDelay)) and
60      (actualGear = Second and gearShiftWidth = 1 and
        gearShiftDirection = Down and gearShift
        (gearShiftWidth, gearShiftDirection) implies
        Lasts (actualGear = Second,
        singleGearShiftDelay) and Futr (actualGear =
        First, singleGearShiftDelay));

61  GearShiftThird:
62
63      (actualGear = Third implies not gearDrive and not
        gearPark and not gearReverse and not ex
        gearShiftWidth (gearShiftDirection = Up and
        gearShift (gearShiftWidth,

```

```

64         gearShiftDirection))) and
        (actualGear = Third implies SomF (ex
          gearShiftWidth (gearShiftDirection = Down and
            gearShift (gearShiftWidth ,
              gearShiftDirection)))) and
65        (actualGear = Third and gearShiftWidth = 1 and
          gearShiftDirection = Down and gearShift
            (gearShiftWidth , gearShiftDirection) implies
              Lasts (actualGear = Third ,
                singleGearShiftDelay) and Futr (actualGear =
                Second , singleGearShiftDelay)) and
66        (actualGear = Third and gearShiftWidth = 2 and
          gearShiftDirection = Down and gearShift
            (gearShiftWidth , gearShiftDirection) implies
              Lasts (actualGear = Third , dualGearShiftDelay)
              and Futr (actualGear = First ,
                dualGearShiftDelay));
67
68    GearShiftReverse:
69        (actualGear = Reverse implies not gearReverse and
          all gearShiftWidth , gearShiftDirection (not
            gearShift (gearShiftWidth ,
              gearShiftDirection))) and
70        (actualGear = Reverse implies SomF (gearDrive or
          gearPark)) and
71        (actualGear = Reverse and gearDrive implies Lasts
          (actualGear = Reverse , driveGearShiftDelay) and
            Futr (actualGear = First , driveGearShiftDelay))
          and
72        (actualGear = Reverse and gearPark implies Lasts
          (actualGear = Reverse , parkGearShiftDelay) and
            Futr (actualGear = Park , parkGearShiftDelay))
          and
73        (gearReverse implies transmissionShaftState =
          Detached);
74
75    GearShiftPark:
76        (actualGear = Park implies not gearPark and all
          gearShiftWidth , gearShiftDirection (not
            gearShift (gearShiftWidth ,
              gearShiftDirection))) and
77        (actualGear = Park implies SomF (gearDrive or
          gearReverse)) and

```

```

78      (actualGear = Park and gearDrive implies Lasts
        (actualGear = Park, reverseGearShiftDelay) and
        Futr (actualGear = First, driveGearShiftDelay))
        and
79      (actualGear = Park and gearReverse implies Lasts
        (actualGear = Park, reverseGearShiftDelay) and
        Futr (actualGear = Reverse,
        reverseGearShiftDelay)) and
80      (actualGear = Park implies transmissionShaftState
        = Detached) and
81      (gearPark implies transmissionShaftState =
        Detached);
82
83      GearShiftTimings:
84      all gearShiftDirection ((actualGear = First or
        actualGear = Second or actualGear = Third) and
        gearShiftWidth = 1 and gearShift
        (gearShiftWidth, gearShiftDirection) implies
        not Lasts (gearDrive or gearPark or gearReverse
        or ex gearShiftWidth2, gearShiftDirection2
        (gearShift (gearShiftWidth2,
        gearShiftDirection2)), singleGearShiftDelay))
        and
85      all gearShiftDirection ((actualGear = First or
        actualGear = Third) and gearShiftWidth = 2 and
        gearShift (gearShiftWidth, gearShiftDirection)
        implies not Lasts (gearDrive or gearPark or
        gearReverse or ex gearShiftWidth2,
        gearShiftDirection2 (gearShift
        (gearShiftWidth2, gearShiftDirection2)),
        dualGearShiftDelay)) and
86      ((actualGear = Reverse and gearDrive) implies not
        Lasts (gearDrive or gearPark or gearReverse or
        ex gearShiftWidth2, gearShiftDirection2
        (gearShift (gearShiftWidth2,
        gearShiftDirection2)), driveGearShiftDelay)) and
87      ((actualGear = Reverse and gearPark) implies not
        Lasts (gearDrive or gearPark or gearReverse or
        ex gearShiftWidth2, gearShiftDirection2
        (gearShift (gearShiftWidth2,
        gearShiftDirection2)), parkGearShiftDelay)) and
88      ((actualGear = Park and gearDrive) implies not
        Lasts (gearDriver or gearPark or gearReverse or

```

```
89      ex gearShiftWidth2, gearShiftDirection2
      (gearShift (gearShiftWidth2,
      gearShiftDirection2)), driveGearShiftDelay)) and
90      ((actualGear = Park and gearReverse) implies not
      Lasts (gearDrive or gearPark or gearReverse or
91      ex gearShiftWidth2, gearShiftDirection2
      (gearShift (gearShiftWidth2,
      gearShiftDirection2)), reverseGearShiftDelay));
92      Nothing:
      all gear (actualGear = gear and not (all
      gearShiftWidth, gearShiftDirection (gearShift
      (gearShiftWidth, gearShiftDirection)) or
      gearDrive or gearPark or gearReverse) implies
      UpToNow (actualGear = gear) and NowOn
      (actualGear = gear));
93
94 end
```

4 HydraulicSystem Class

The *HydraulicSystem* class is formalized thanks to the code reported in Listing 7.

The first assumption we made before modelling the Hydraulic System was that every valve and electrovalve configuration imposes the same fluid propagation delay; this means that for every command that the Hydraulic System propagates the delay will always be the same. This behavior is formalized with the time independent constant `fluidPropagationDelay`.

The *manual valve*, which permit the driver to manually select the gear mode, is modelled thanks to the `gearHandle` event and the `GearHandle` axiom. During the time in which the Hydraulic System propagate a command there can be no `gearHandle` event which somehow means the fluid propagation is faster then the driver reaction time (which is a realistic assumption).

Moreover, thanks to the `MutualExclusion` axiom, it's impossible to generate two `gearHandle` event at the same time which means that the gear handle can't be for example in Park and Drive mode at the same instant.

Listing 7: HydraulicSystem.trio

```

1  class HydraulicSystem (const fluidPropagationDelay)
2
3  signature :
4
5  visible :
6      gearHandle ,
7      gearShift ,
8      gearDrive ,
9      gearPark ,
10     gearReverse ,
11     controlGearShift ;
12
13 temporal domain : real ;
14
15 domains :
16     GearPosition : {Drive , Park , Reverse} ;
17     ShiftWidth : 1..2 ;
18     ShiftDirection : {Up, Down} ;
19
20 items :
21     TI fluidPropagationDelay : real ;
22     event gearHandle (GearPosition) ;
23     event gearShift (ShiftWidth , ShiftDirection) ;
24     event gearDrive ;

```



```
45         gearShiftDirection2)), fluidPropagationDelay)
46         and Futr (gearShift (gearShiftWidth,
47         gearShiftDirection), fluidPropagationDelay));
48
49     MutualExclusions:
47         all gear (gearHandle (gear) implies all gear2
48         (gear  $\diamond$  gear2 implies not gearHandle (gear2)));
49 end
```


5 TransmissionControlUnit Class

The *TransmissionControlUnit* class is formalized thanks to the code reported in Listing 8.

Our first formalization of the Transmission Control Unit didn't take in account the possibility to have asynchronous sensors; the latest version of the Transmission Control Unit permits to manage asynchronous sensors thanks to internal memory modelled with three time dependent total values.

When handle the necessity to scale gears till the First with the assumption that the human reaction is way slower than sampling frequency and mechanical reactions, so, when the vehicle stops, the axiom which handle the gear scale manage to be "active" the necessary amount of times to scale all the gears.

The Transmission Control Unit guarantees that it doesn't raise more than one gear shift event per instant and it receives at most one event per instant from each sensor (this is described also in Section 2 and so guaranteed in VehicleSpeedSensor and EngineSpeedSensor class).

Listing 8: TransmissionControlUnit.trio

```

1  class TransmissionControlUnit
2
3  signature:
4
5  visible:
6      controlGearShift ,
7      receiveEngineSpeed ,
8      receiveVehicleSpeed ;
9
10 temporal domain: real;
11
12 domains:
13     ShiftWidth: 1..2;
14     ShiftDirection: {Up, Down};
15
16 items:
17     TD total storedEngineSpeed: integer;
18     TD total storedDeltaVehicleSpeed: integer;
19     TD total storedVehicleSpeed: integer;
20     event controlGearShift (ShiftWidth, ShiftDirection);
21     event receiveEngineSpeed (integer);
22     event receiveVehicleSpeed (integer, integer);
23
24 axioms:
25 vars:

```

```

26     engineSpeed: integer;
27     engineSpeed1: integer;
28     engineSpeed2: integer;
29     deltaVehicleSpeed: integer;
30     deltaVehicleSpeed1: integer;
31     deltaVehicleSpeed2: integer;
32     vehicleSpeed: integer;
33     vehicleSpeed1: integer;
34     vehicleSpeed2: integer;
35     gearShiftWidth1: ShiftWidth;
36     gearShiftWidth2: ShiftWidth;
37     gearShiftDirection1: ShiftDirection;
38     gearShiftDirection2: ShiftDirection;
39 formulae:
40     GearShifts:
41         (receiveEngineSpeed (engineSpeed) and
           receiveVehicleSpeed (deltaVehicleSpeed ,
           vehicleSpeed) and engineSpeed >= 3000 and
           vehicleSpeed > 0 implies gearShiftWidth1 = 1
           and gearShiftDirection1 = Up and
           controlGearShift (gearShiftWidth1 ,
           gearShiftDirection1)) and
42         (receiveEngineSpeed (engineSpeed) and all
           deltaVehicleSpeed , vehicleSpeed (not
           receiveVehicleSpeed (deltaVehicleSpeed ,
           vehicleSpeed)) and engineSpeed >= 3000 and
           storedVehicleSpeed > 0 implies gearShiftWidth1
           = 1 and gearShiftDirection1 = Up and
           controlGearShift (gearShiftWidth1 ,
           gearShiftDirection1)) and
43         (all engineSpeed (not receiveEngineSpeed
           (engineSpeed)) and receiveVehicleSpeed
           (deltaVehicleSpeed , vehicleSpeed) and
           storedEngineSpeed >= 3000 and vehicleSpeed > 0
           implies gearShiftWidth1 = 1 and
           gearShiftDirection1 = Up and controlGearShift
           (gearShiftWidth1 , gearShiftDirection1)) and
44         (receiveEngineSpeed (engineSpeed) and
           receiveVehicleSpeed (deltaVehicleSpeed ,
           vehicleSpeed) and engineSpeed <= 1500 and
           deltaVehicleSpeed <= 0 implies gearShiftWidth1
           = 1 and gearShiftDirection1 = Down and
           controlGearShift (gearShiftWidth1 ,

```

```

45      gearShiftDirection1)) and
      (receiveEngineSpeed (engineSpeed) and all
        deltaVehicleSpeed , vehicleSpeed (not
          receiveVehicleSpeed (deltaVehicleSpeed ,
            vehicleSpeed)) and engineSpeed <= 1500 and
            storedDeltaVehicleSpeed <= 0 implies
              gearShiftWidth1 = 1 and gearShiftDirection1 =
                Down and controlGearShift (gearShiftWidth1 ,
146      gearShiftDirection1)) and
      (all engineSpeed (not receiveEngineSpeed
        (engineSpeed)) and receiveVehicleSpeed
          (deltaVehicleSpeed , vehicleSpeed) and
            storedEngineSpeed <= 1500 and
              (deltaVehicleSpeed <= 0 or vehicleSpeed = 0)
                implies gearShiftWidth1 = 1 and
                  gearShiftDirection1 = Down and controlGearShift
                    (gearShiftWidth1 , gearShiftDirection1)) and
47      (receiveEngineSpeed (engineSpeed) and
        receiveVehicleSpeed (deltaVehicleSpeed ,
          vehicleSpeed) and engineSpeed <= 1500 and
            deltaVehicleSpeed > 0 implies all
              gearShiftWidth1 , gearShiftDirection1 (not
                controlGearShift (gearShiftWidth1 ,
148      gearShiftDirection1))) and
      (receiveEngineSpeed (engineSpeed) and all
        deltaVehicleSpeed , vehicleSpeed (not
          receiveVehicleSpeed (deltaVehicleSpeed ,
            vehicleSpeed)) and engineSpeed <= 1500 and
              storedDeltaVehicleSpeed >= 0 and
                storedVehicleSpeed > 0 implies all
                  gearShiftWidth1 , gearShiftDirection1 (not
                    controlGearShift (gearShiftWidth1 ,
49      gearShiftDirection1))) and
      (all engineSpeed (not receiveEngineSpeed
        (engineSpeed)) and receiveVehicleSpeed
          (deltaVehicleSpeed , vehicleSpeed) and
            storedEngineSpeed <= 1500 and deltaVehicleSpeed
              >= 0 and vehicleSpeed > 0 implies all
                gearShiftWidth1 , gearShiftDirection1 (not
                  controlGearShift (gearShiftWidth1 ,
50      gearShiftDirection1))) and
      (receiveEngineSpeed (engineSpeed) and
        receiveVehicleSpeed (deltaVehicleSpeed ,

```

```

51         vehicleSpeed) and engineSpeed >= 1500 and
           engineSpeed < 3000 implies all gearShiftWidth1 ,
           gearShiftDirection1 (not controlGearShift
           (gearShiftWidth1 , gearShiftDirection1))) and
52     (receiveEngineSpeed (engineSpeed) and all
           deltaVehicleSpeed , vehicleSpeed (not
           receiveVehicleSpeed (deltaVehicleSpeed ,
           vehicleSpeed)) and engineSpeed >= 1500 and
           engineSpeed < 3000 implies all gearShiftWidth1 ,
           gearShiftDirection1 (not controlGearShift
           (gearShiftWidth1 , gearShiftDirection1))) and
53     (all engineSpeed (not receiveEngineSpeed
           (engineSpeed)) and receiveVehicleSpeed
           (deltaVehicleSpeed , vehicleSpeed) and
           storedEngineSpeed >= 1500 and storedEngineSpeed
           < 3000 implies all gearShiftWidth1 ,
           gearShiftDirection1 (not controlGearShift
           (gearShiftWidth1 , gearShiftDirection1))) and
54     (all engineSpeed (not receiveEngineSpeed
           (engineSpeed)) and all deltaVehicleSpeed ,
           vehicleSpeed (not receiveVehicleSpeed
           (deltaVehicleSpeed , vehicleSpeed)) implies all
           gearShiftWidth1 , gearShiftDirection1 (not
           controlGearShift (gearShiftWidth1 ,
           gearShiftDirection1))));
55
56 ReceivingEventAction :
57     all deltaVehicleSpeed1 , vehicleSpeed1
           (receiveVehicleSpeed (deltaVehicleSpeed1 ,
           vehicleSpeed1) implies Until
           (storedDeltaVehicleSpeed = deltaVehicleSpeed1
           and storedVehicleSpeed = vehicleSpeed1 , ex
           deltaVehicleSpeed2 , vehicleSpeed2
           (receiveVehicleSpeed (deltaVehicleSpeed2 ,
           vehicleSpeed2)))) and
58     all engineSpeed1 (receiveEngineSpeed
           (engineSpeed1) implies Until (storedEngineSpeed
           = engineSpeed1 , ex engineSpeed2
           (receiveEngineSpeed (engineSpeed2))));
59
60 MutualExclusions :
           all gearShiftWidth1 , gearShiftDirection1
           (controlGearShift (gearShiftWidth1 ,

```

```
        gearShiftDirection1) implies all
        gearShiftWidth2 , gearShiftDirection2
        (gearShiftWidth1  $\Diamond$  gearShiftWidth2 and
        gearShiftDirection1  $\Diamond$  gearShiftDirection2
        implies not controlGearShift (gearShiftWidth2 ,
        gearShiftDirection2))) and
61 all engineSpeed1 (receiveEngineSpeed
        (engineSpeed1) implies all engineSpeed2
        (engineSpeed2  $\Diamond$  engineSpeed1 implies not
        receiveEngineSpeed (engineSpeed2))) and
62 all deltaVehicleSpeed1 , vehicleSpeed1
        (receiveVehicleSpeed (deltaVehicleSpeed1 ,
        vehicleSpeed1) implies all deltaVehicleSpeed2 ,
        vehicleSpeed2 (deltaVehicleSpeed2  $\Diamond$ 
        deltaVehicleSpeed1 and vehicleSpeed2  $\Diamond$ 
        vehicleSpeed1 implies not receiveVehicleSpeed
        (deltaVehicleSpeed2 , vehicleSpeed2)));
63
64 end
```

6 Annotations

During the last phase of our modelling we decided not to formalize the *Torque Converter* and this decision depends on the way the Torque Converter works.

The Torque Converter is a mechanical component that works coupling and decoupling the *Transmission Shaft* and the *Engine Shaft*. It solves its duty without the necessity to receive commands from any component of the system and this is the cause we have decided to remove it from our model.

Anyway, the state of the Torque Converter is really important for the system since it gives information that permits to insert or not to insert some gears and other details that aren't taken into account in this project.

7 Properties

In this Section 7 are reported the three properties we have proved in their decidable TRIO form; these formulae are available in their *Zot* form directly in Listings 3.

In order to verify these three properties we needed to translate them from their “present/future” form to a “present/past” form, because of some inherent limitations of *Spin*. The latter property has been verified only with *Zot* that doesn't need any translation.

Listing 9: Property 1

```
actualGear = First & controlGearShift = TCUShiftOneUp ->  
  Futr(actualGear = Second, FluidDelay + ShiftDelay);
```

Listing 10: Property 2

```
actualGear = First & gearHandle = HandleShiftReverse ->  
  Futr(actualGear = Reverse, FluidDelay + ShiftDelay) &  
  Lasts_ii(transmissionShaftState = Detached, FluidDelay  
    + ShiftDelay));
```

Listing 11: Property 3

```
actualGear = First & gearHandle = HandleShiftPark ->  
  Futr(actualGear = Park, FluidDelay + ShiftDelay) &  
  Until(transmissionShaftState = Detached, gearHandle ◇  
    Nothing));
```

Log files are available at this page <http://code.google.com/p/ccat/source/browse/#svn/trunk/log>.