Verification of BBW system

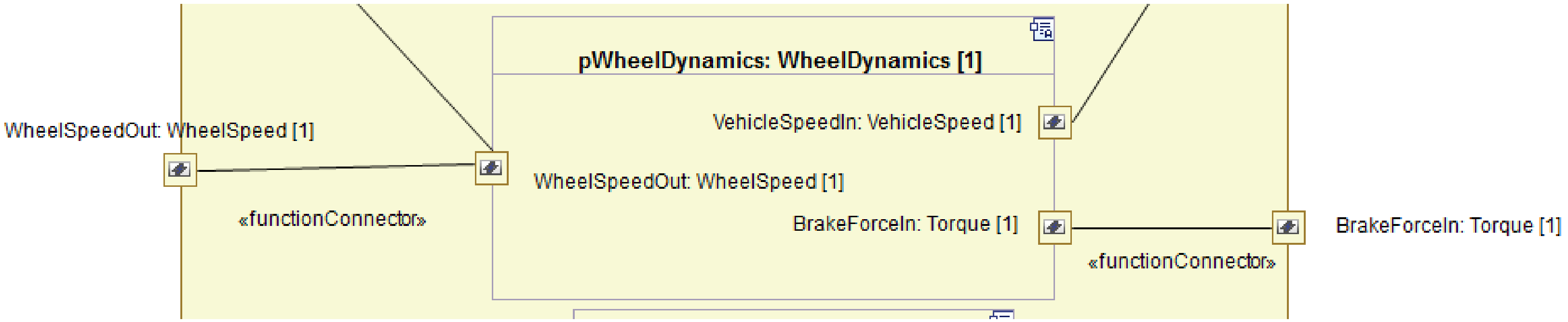
Outline

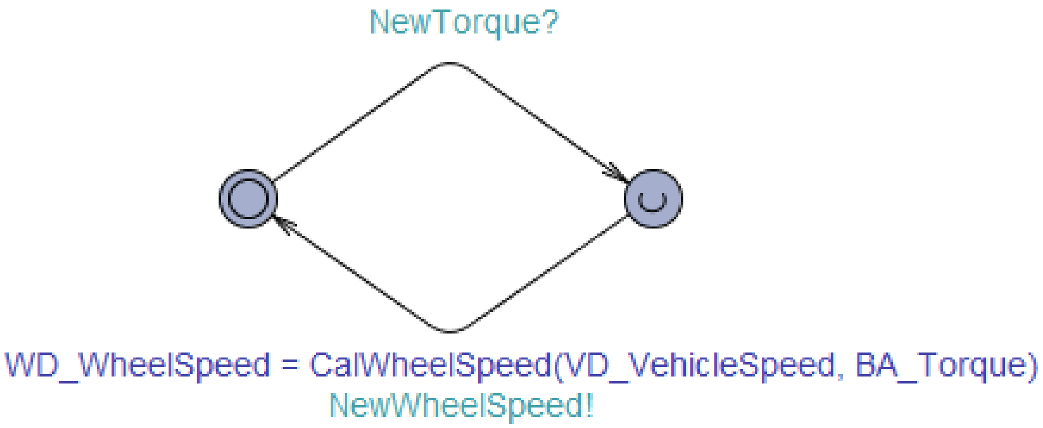
- Build model in UPPAAL
  - ESAT-ADL is NOT a model checker but UPPAAL is
  - ESAT-ADL does NOT contain behaviors inside of function prototypes
- Verify properties

Build model in UPPAAL

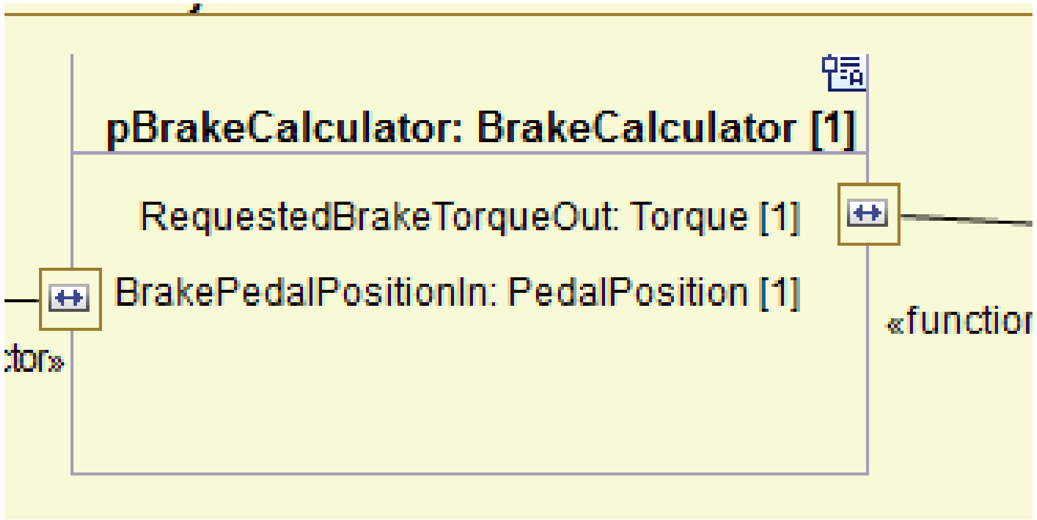
- Use one template to represent one function prototype (box)
- Two location
  - One for idle
  - Another one for running
- Use synchronize channels to represent ports and channels (communication between boxes)
- Use global variable to represent data

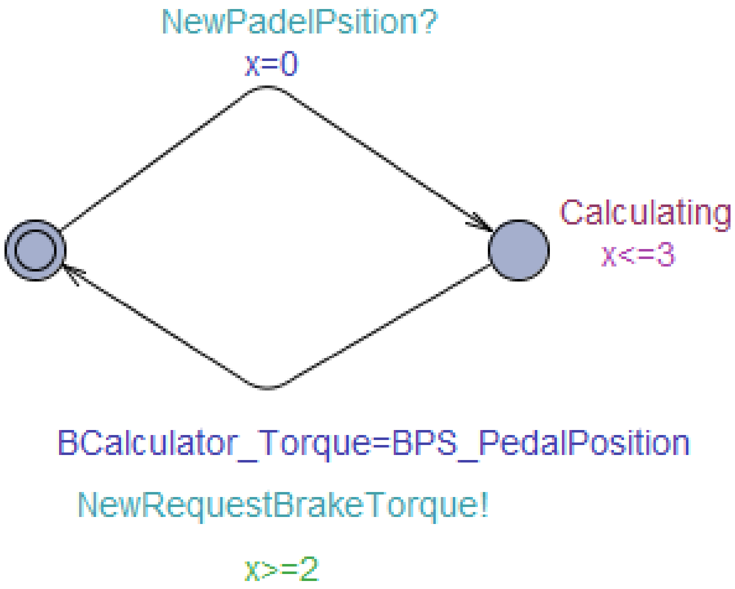
Build model in UPPAAL


pWheelDynamics: WheelDynamics [1]
VehicleSpeedIn: VehicleSpeed [1]
WheelSpeedOut: WheelSpeed [1]
WheelSpeedOut: WheelSpeed [1]
«functionConnector»
BrakeForceIn: Torque [1]
BrakeForceIn: Torque [1]
«functionConnector»

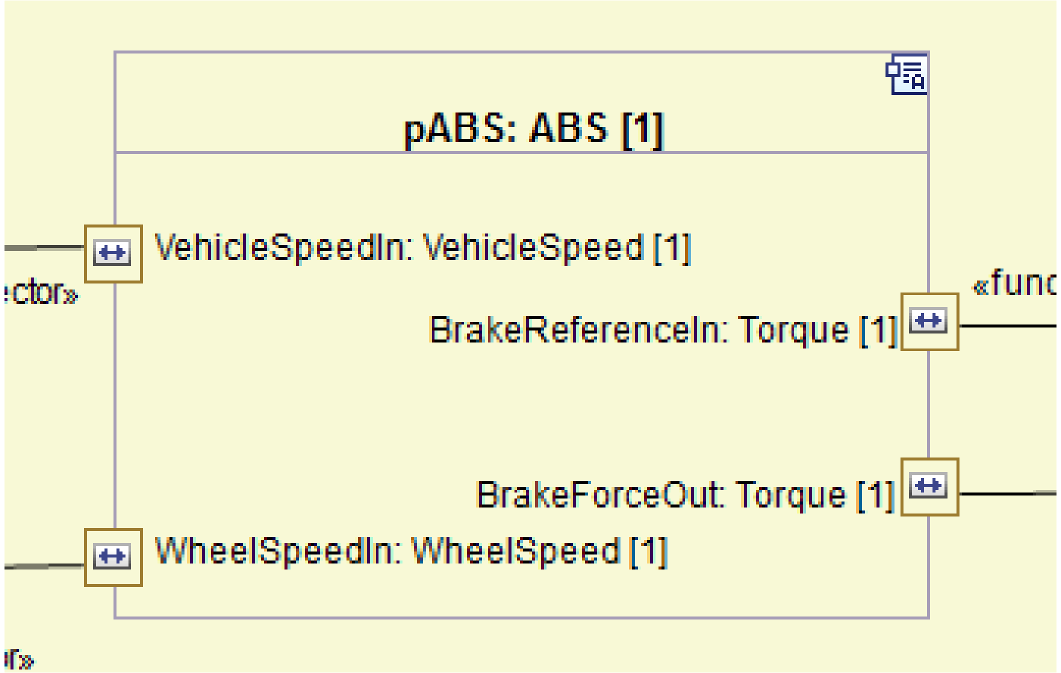


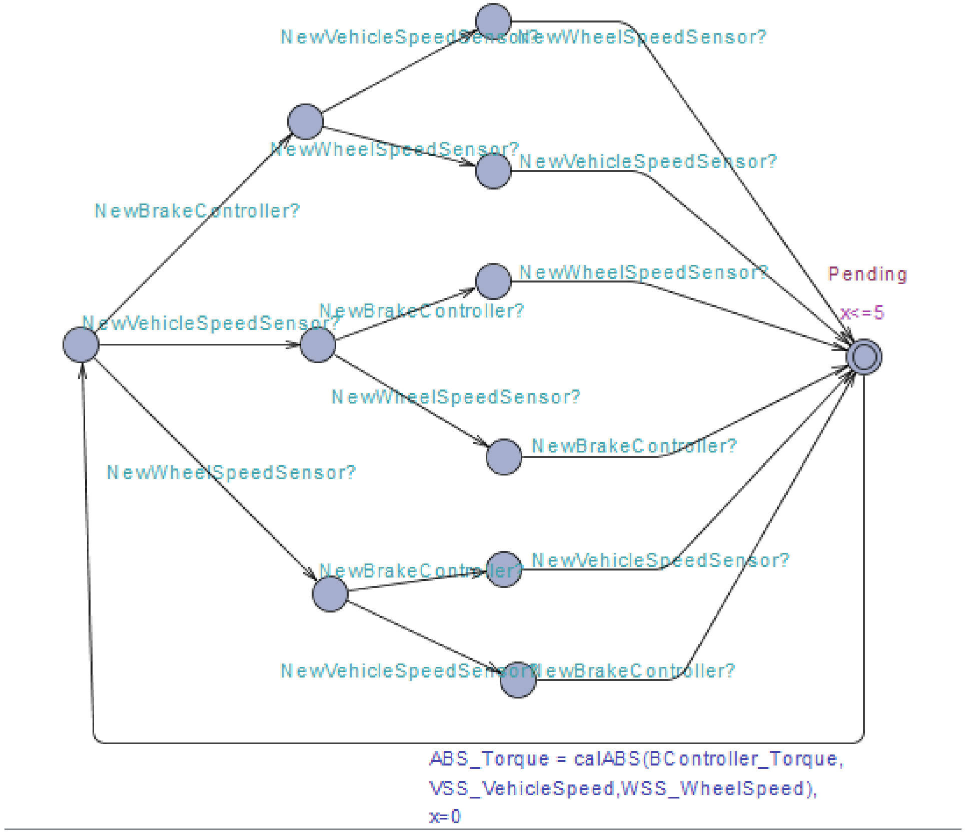
Build model in UPPAAL


pBrakeCalculator: BrakeCalculator [1]
RequestedBrakeTorqueOut: Torque [1]
BrakePedalPositionIn: PedalPosition [1]
«functior
:tor»

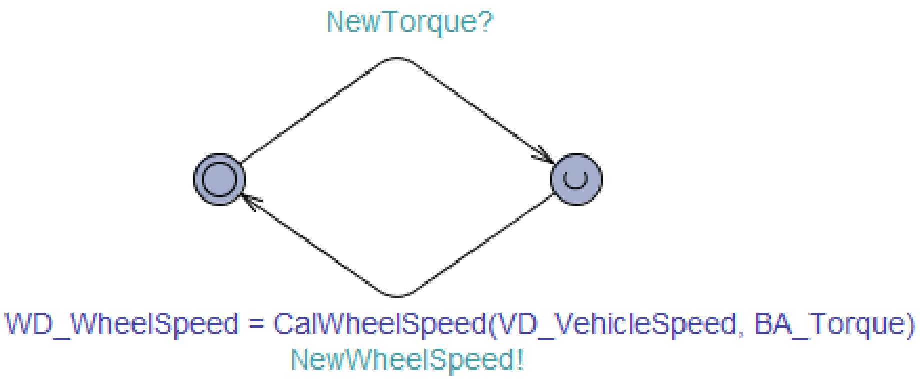


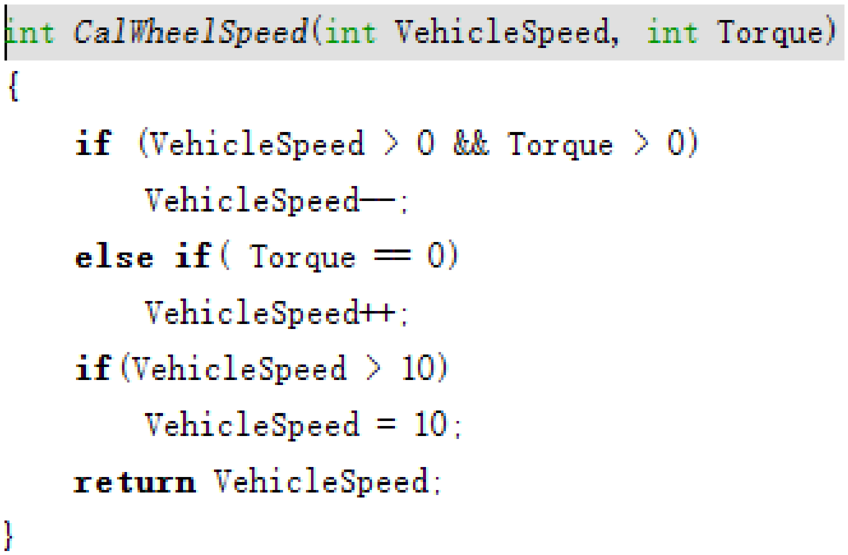
Build model in UPPAAL


pABS: ABS [1]
VehicleSpeedIn: VehicleSpeed [1]
BrakeReferenceIn: Torque [1]
BrakeForceOut: Torque [1]
WheelSpeedIn: WheelSpeed [1]
ctor»
«func
r»



Build model in UPPAAL



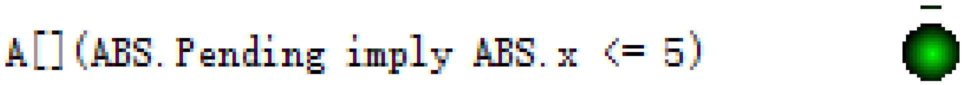


```
int CalWheelSpeed(int VehicleSpeed, int Torque)
{
    if (VehicleSpeed > 0 && Torque > 0)
        VehicleSpeed--;
    else if( Torque == 0)
        VehicleSpeed++;
    if(VehicleSpeed > 10)
        VehicleSpeed = 10;
    return VehicleSpeed;
}
```

Verify Properties

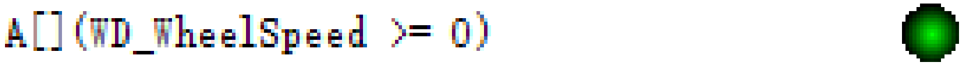
- Find Properties based on your model

- ABS should finish in 5 time units



```
A[](ABS.Pending imply ABS.x <= 5)             ●
```

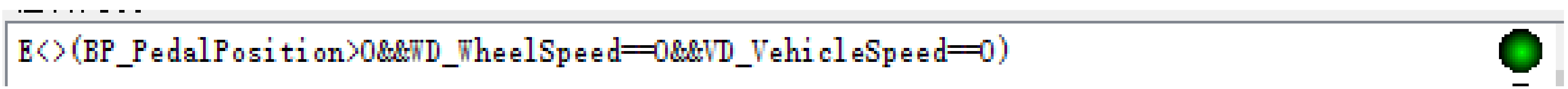
- Speed should be larger or equal to 0 (not negative)



```
A[](WD_WheelSpeed >= 0)                        ●
```

Verify Properties

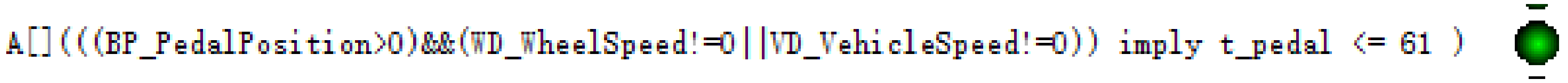
- Press down pedal, vehicle should stop



```
E<>(BP_PedalPosition>0&&WD_WheelSpeed==0&&VD_VehicleSpeed==0)
```

●

- Press down pedal, vehicle should stop in 61 time unit



```
A[](((BP_PedalPosition>0)&&(WD_WheelSpeed!=0||VD_VehicleSpeed!=0)) imply t_pedal <= 61 )
```

●

Thank You!