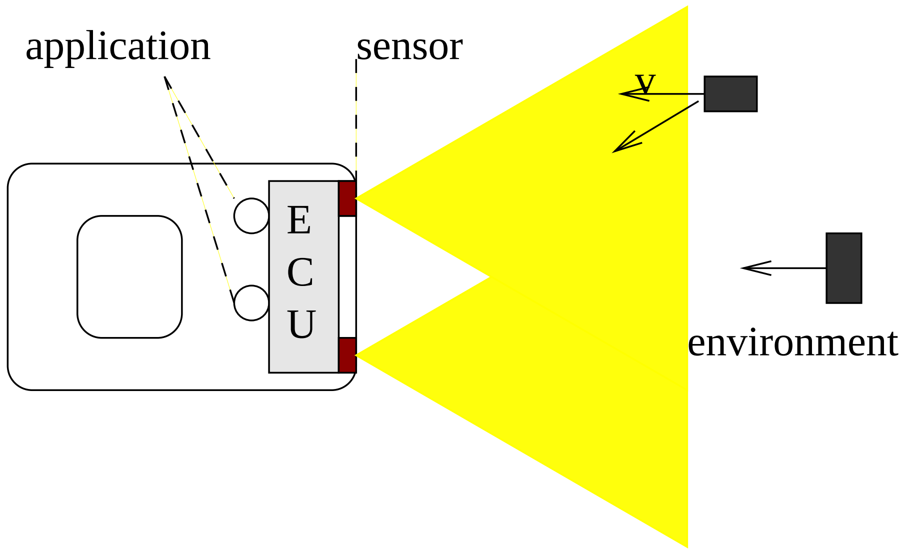
A Formal Analysis of a Car Periphery Supervision System

Biniam Gebremichael
http://www.cs.kun.nl/~biniam
University of Nijmegen, The Netherlands

Together with Tomas Krilavicius and Yaroslav S. Usenko
University of Twente, The Netherlands

will appear in **WODES 2004**

The Car Periphery Supervision (CPS)

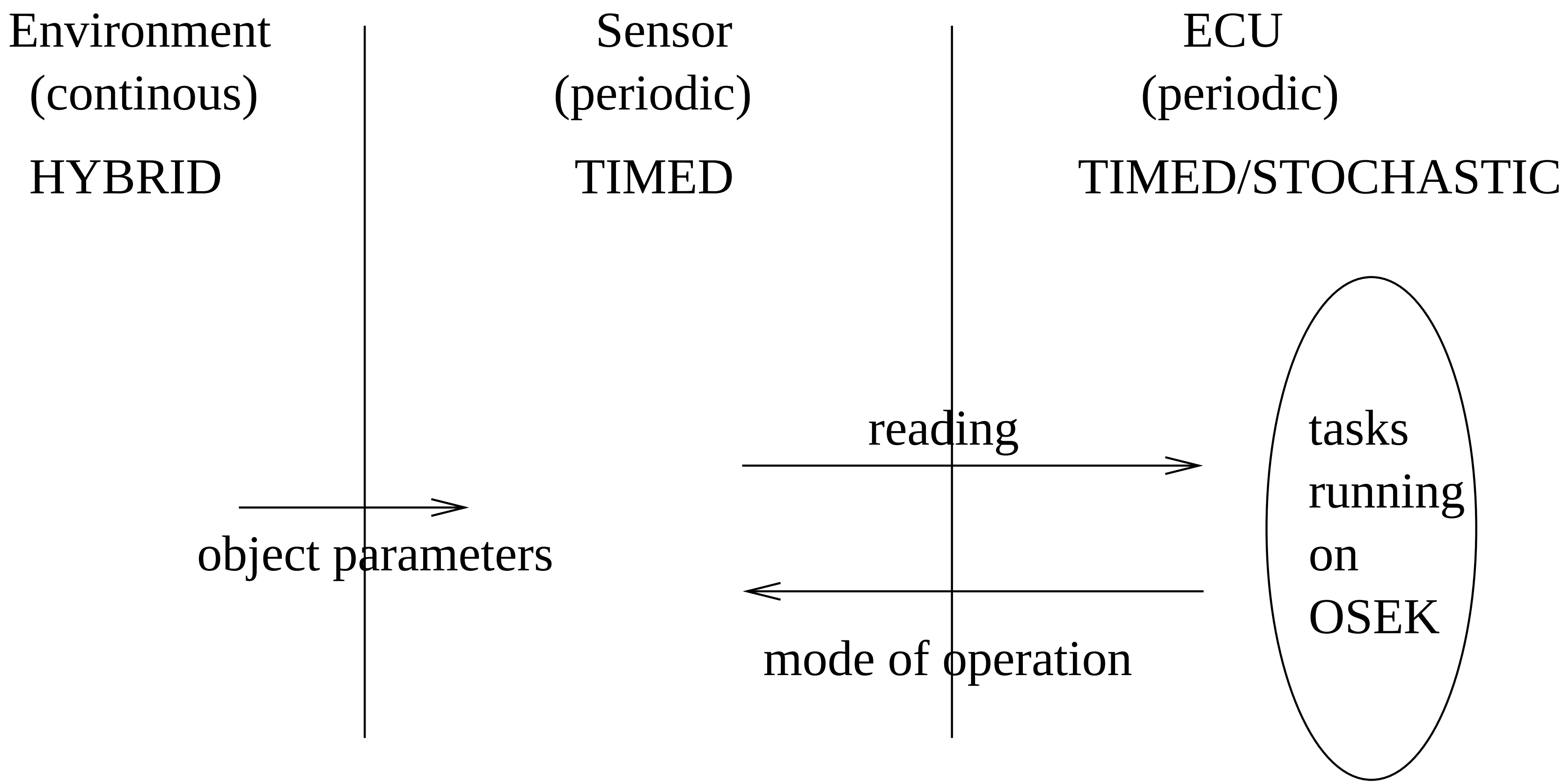


- Sensors scan the environment and transfer data to ECU.
- ECU provide information for the applications,
- ECU controls how sensors operate.
- Applications: airbag in¤ation, belt tensioner, parking assistance, HMI ... etc

Requirement definition

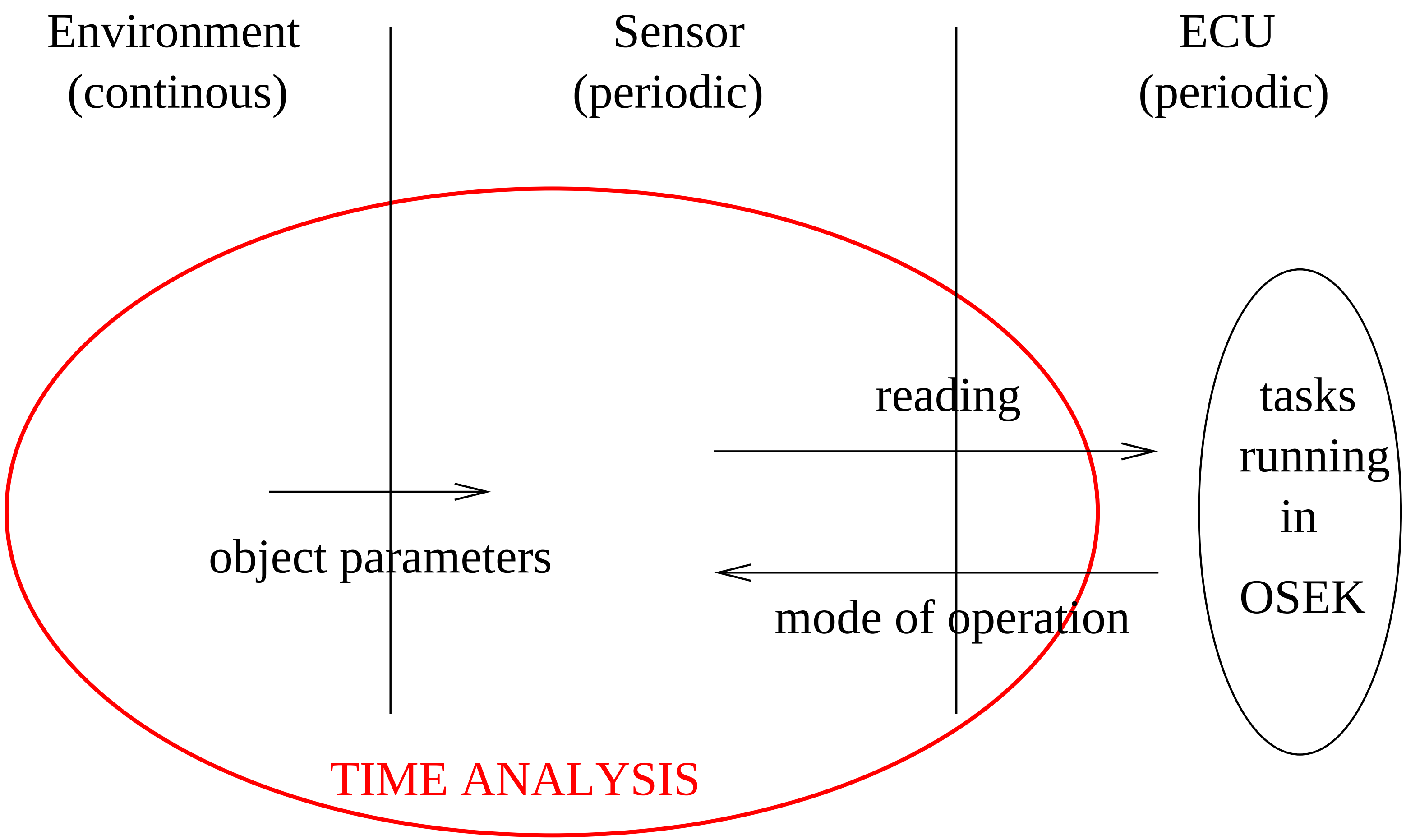
- Deliver accurate and on-time information to applications
- Avoid false alarm
- No deadlock

Modeling



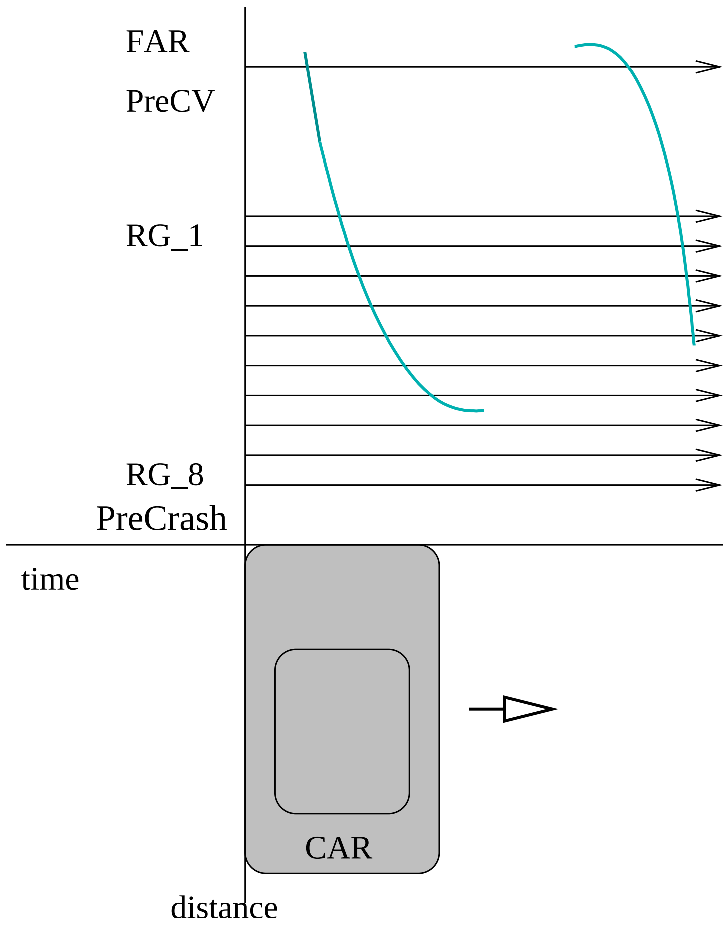
Environment
(continous)
HYBRID
Sensor
(periodic)
TIMED
ECU
(periodic)
TIMED/STOCHASTIC
object parameters
reading
mode of operation
tasks
running
on
OSEK

Modeling

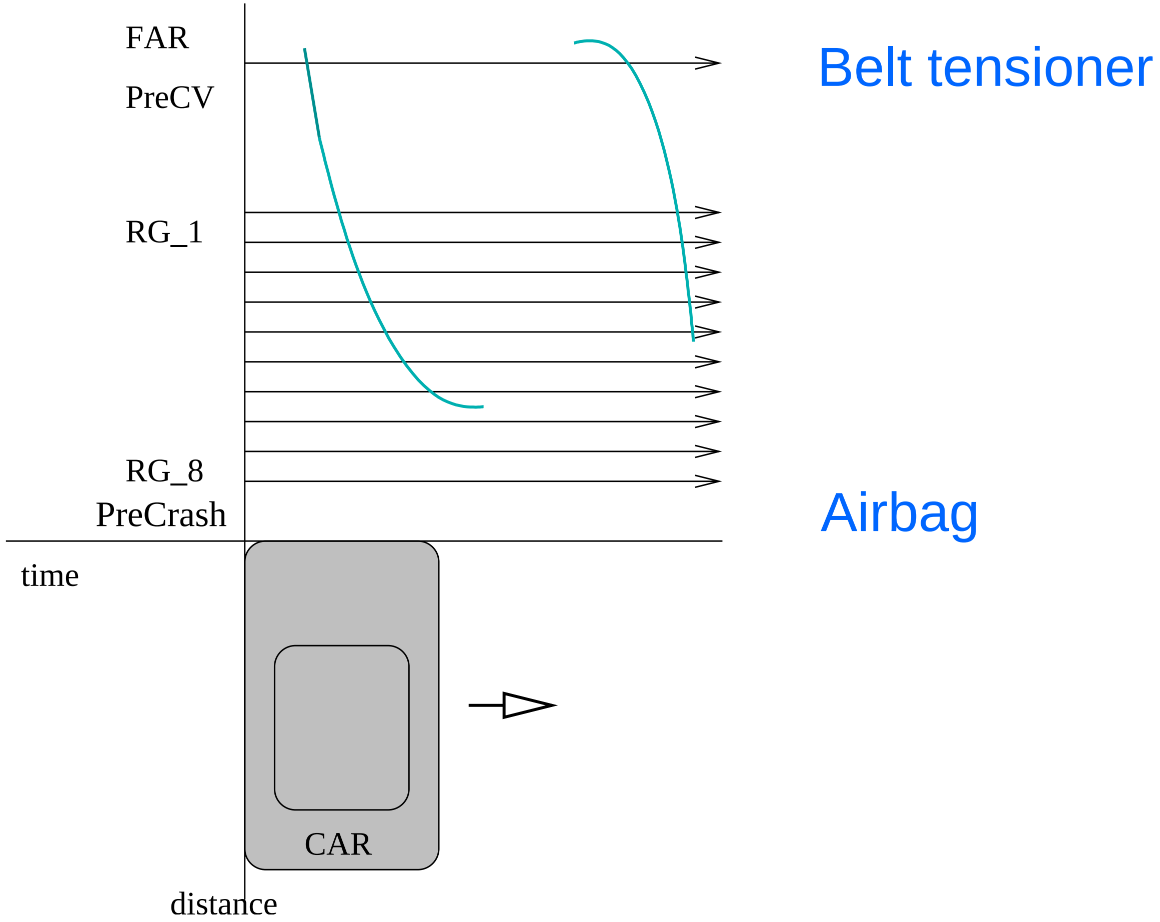


Environment
(continous)
Sensor
(periodic)
ECU
(periodic)
reading
tasks
running
in
OSEK
object parameters
mode of operation
TIME ANALYSIS

Regions and object trajectories



Regions and object trajectories

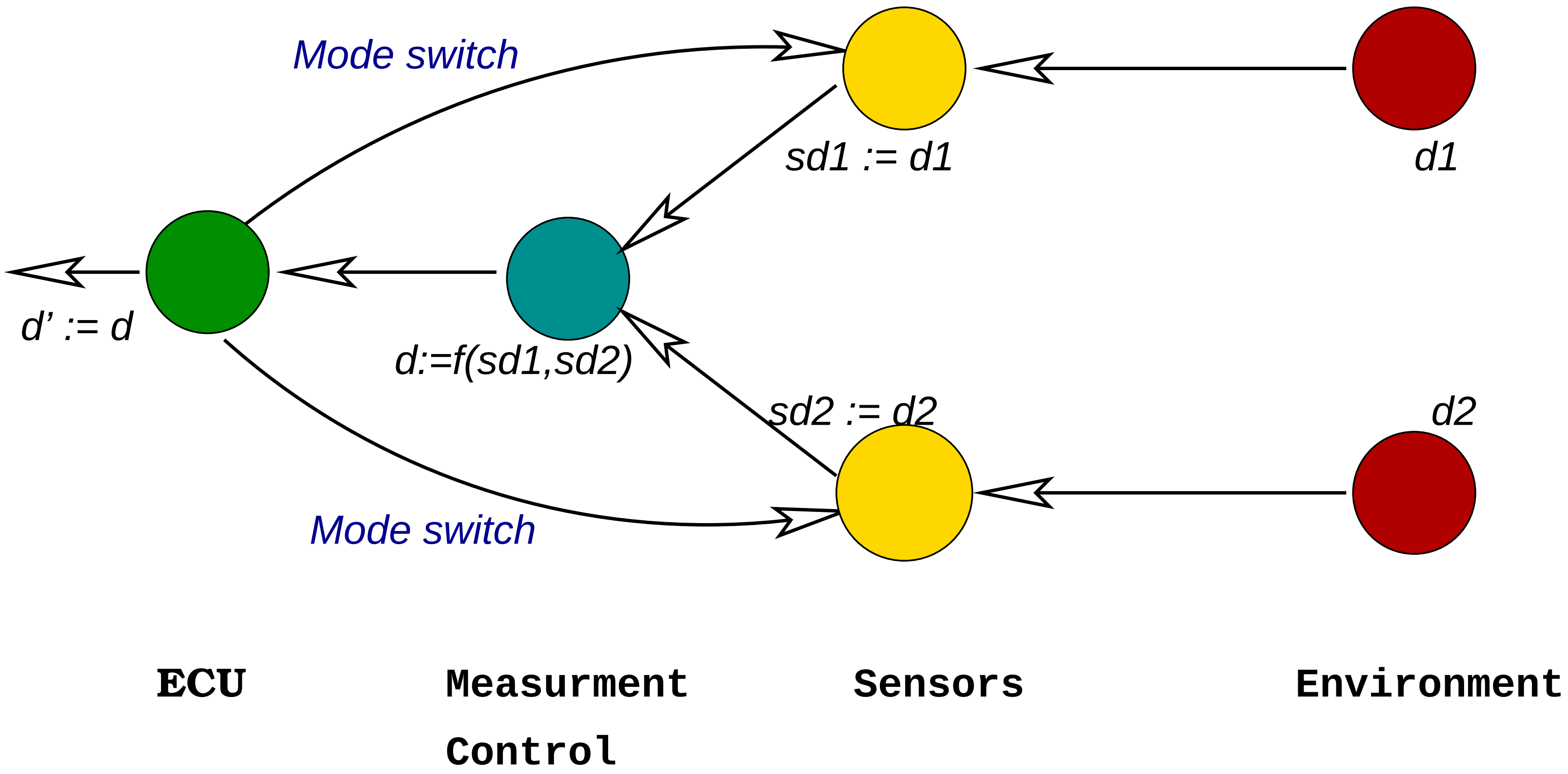


Environment

Object distance (d) is continuous variable.

- Measurement regions: The area in front of the car is divided into 12 regions [Kowalewski and Rittel 02].
  - ➜ FAR $(\infty, 4.77)$
  - ➜ PreCV $[4.77, 1.41)$
  - ➜ Range gates $\forall i : 0 \leq i < 8, [1.41 - 0.09.i, 1.41 - 0.09.(i + 1))$
  - ➜ PreCrash $[0.69, 0]$
- Assumption
  - ➜ Maximum relative velocity $= 56m/s$
  - ➜ Minimum relative velocity $= 13m/s$
  - ➜ One object in CV region

CPS as Network of Timed Automata



Correctness property

- ➜ Q range-gates difference between ECU and ENV (eg. $Q = 3$)

```
A[] (d1 - ECU.i <= Q)
```

- ➜ $P\ ms$ before ECU knows about PreCrash. (eg. $P = 5ms$)

```
A[] ((ENV1.PreCrash and ENV1.x > P) imply (ECU.i >= lastRReg))
```

- ➜ ECU should avoid false alarm

```
A[] (ECU.i >= firstRReg imply (d1 >= ECU.i or d2 >= ECU.i))
```

- ➜ The system is time-deadlock free

```
A[] (not deadlock)
```

Results

- Not scheduled: For $Q \geq 3$ and $P \geq 5ms$ the properties are satisfied.
- Best scheduled: Measurement control scheduled to run before ECU and no communication delay, then $Q \geq 2$ and $P \geq 3ms$
- P = propagation time
  $P = Sensor_t + Mcontrol_t + ECU_t$
  $P = Sensor_t + Mcontrol_t$
- Q = P in terms of range gate,
  $Q = \lceil \frac{P}{CVStepmin} \rceil$
- ECU as several concurrent tasks(T_i) and use OSEK scheduler.

$$P = Sensor_t + OSEK_t(T_1, T_2, ...T_n)$$

- Methods
  - Visibility and timing analysis using Matlab.
  - Uppaal verification using Convex-hull over approximation, possible for two sensors model.
- Future work
  - Multiple objects in RGs.
  - Recovery operation during CVScan→DScan switch.
  - Integration with Belt tensioner, comfort services.
  - Different time scale. Exact acceleration method [Hendriks and Larsen 02] may not work for two sensors model.
  - Abstraction of Hybrid Systems based on the properties to be verified. [Alur et al. 2000], [Henzinger and Ho 95]