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 inflation, belt tensioner, parking assistance, HMI ... etc
Requirement definition

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

Environment (continuous) | Sensor (periodic) | ECU (periodic)  
HYBRID | TIMED | TIMED/STOCHASTIC

object parameters ← reading ← tasks running on OSEK

mode of operation
Modeling

Environment (continuous)  Sensor (periodic)  ECU (periodic)

object parameters  reading  tasks running in OSEK

mode of operation

TIME ANALYSIS
Regions and object trajectories

Airbag

B. Gebremichael, A Formal Analysis of a Car Periphery Supervision System
Regions and object trajectories

- Belt tensioner
- Airbag

Diagram showing regions and object trajectories over time and distance.

B. Gebremichael, A Formal Analysis of a Car Periphery Supervision System
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 \(= 56\text{m/s}\)
  - Minimum relative velocity \(= 13\text{m/s}\)
  - One object in CV region
CPS as Network of Timed Automata

Mode switch

\[ d' := d \]

\[ sd1 := d1 \]

\[ sd2 := d2 \]

\[ d := f(sd1, sd2) \]

\[ d' := d \]

ECU | Measurement | Sensors | Environment
---|-------------|---------|--------------
Control |             |         |              

B. Gebremichael, A Formal Analysis of a Car Periphery Supervision System
Correctness property

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

$$A[] (d1 - ECU.i \leq Q)$$

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

$$A[] ((ENV1.PreCrash \text{ and } ENV1.x > P) \text{ imply } (ECU.i >= lastRReg))$$

$\rightarrow$ ECU should avoid false alarm

$$A[] (ECU.i >= firstRReg \text{ imply } (d1 >= ECU.i \text{ or } d2 >= ECU.i))$$

$\rightarrow$ The system is time-deadlock free

$$A[] (\text{not deadlock})$$
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
  
  $P = Sensor_t + Mcontrol_t + ECU_t$

- $Q = P$ in terms of range gate,
  
  $Q = \left\lfloor \frac{P}{CVStep\text{min}} \right\rfloor$

- 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]