Timing verification of automotive communication architecture using quantile estimation

Nicolas NAVET (Uni Lu), Shehnaz LOUVART (Renault), Jose VILLANUEVA (Renault), Sergio CAMPOY-MARTINEZ (Renault) and Jörn MIGGE (RealTime-at-Work).

Early-stage timing verification of wired automotive buses – CAN-based communication architectures

- Schedulability analysis versus simulation
- Performance metrics: the case for quantiles derived by simulation
- 2 typical automotive use-cases
Automotive communication architectures

- Increased bandwidth requirements & timing constraints
- More complex & heterogeneous architectures with black-box ECUs
- Optimized CAN networks for higher bus loads: priorities, frame offsets, gateways, communication stacks, etc
- Verification activity of higher importance today, higher load levels calls for more accurate verification models → no margin for errors
- Main performance metrics: frame response time = communication latency
**Schedulability analysis**

“mathematical model of the worst-case possible situation”

**Simulation**

“program that reproduces the behavior of a system”

\[ K_i^k(t) \overset{\text{def}}{=} \left\lfloor \frac{J_i^k + \phi_i^k(\phi_i)}{T_i^k} \right\rfloor + \left\lfloor \frac{t - \phi_i^k(\phi_i)}{T_i^k} \right\rfloor + 1 \]

- **Upper bounds on the perf. metrics → Safe if model is correct and assumptions met**
- **Often pessimistic → over-dimensioning**
- **Might be a gap between models and real systems! → unpredictably unsafe**

**Models close to real systems**

**Fine grained information**

**Worst-case response times are out of reach! Occasional deadline misses must be acceptable**
RTaW: “enable designers to build provably safe and optimized critical systems”

- Simulation and schedulability analysis for networks and ECU CAN, CAN FD, Arinc825, Ethernet, FlexRay, AFDX, etc...
- OEM customers: Renault, PSA, Eurocopter, Astrium, ABB

- RTaW/Sim Starter edition can be downloaded from www.realtimeatwork.com

- No black box software: all schedulability analysis that are implemented are published

Used in this study RTaW-Sim → CAN simulator with schedulability analysis and configuration algorithms
Metrics for the evaluation of frame latencies: the case for quantiles
Frame response time distribution

Easily observable events
Testbed / Simulation

Infrequent events
Long Simulation

Rare events
Schedulability analysis

Upper-bound with schedulability analysis

(actual) worst-case response time (WCRT)

Simulation max.

Probability

Q1: pessimism of schedulability analysis ?!
Q2: distance between simulation max. and WCRT ?!
Using quantiles means accepting a controlled risk.

Quantile \( Q_n \): \( P[\text{response time} > Q_n] < 10^{-n} \)

- No extrapolation here, won’t help to say anything about what is too rare to be in simulation traces.

ERTSS’2014
Identifying both deadline and tolerable risks

1. Identify frame deadline
2. Decide the tolerable risk → target quantile
3. Simulate “sufficiently” long
4. If target quantile value is below deadline, performance objective is met
1) Quantiles vs average time between deadline misses

<table>
<thead>
<tr>
<th>Quantile</th>
<th>One frame every …</th>
<th>Mean time to failure Frame period = 10ms</th>
<th>Mean time to failure Frame period = 500ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q3</td>
<td>1 000</td>
<td>10 s</td>
<td>8mn 20s</td>
</tr>
<tr>
<td>Q4</td>
<td>10 000</td>
<td>1mn 40s</td>
<td>≈ 1h 23mn</td>
</tr>
<tr>
<td>Q5</td>
<td>100 000</td>
<td>≈ 17mn</td>
<td>≈ 13h 53mn</td>
</tr>
<tr>
<td>Q6</td>
<td>1000 000</td>
<td>≈ 2h 46mn</td>
<td>≈ 5d 19h</td>
</tr>
</tbody>
</table>

Warning: successive failures in some cases might be temporally correlated, this must be assessed!
Use of distributions of successive quantile overshoots, linear and non-linear dependency analysis
2) Determine the minimum simulation length

- time needed for quantile convergence
- reasonable # of values: a few tens ...

Tool support can help here:
- e.g. numbers in gray should not be trusted

Reasonable values for Q5 and Q6 (with periods <500ms) are obtained in a few hours of simulation (with a high-speed simulation engine) – e.g. 2 hours for a typical automotive setup
3

Typical use-cases of quantile-based performance evaluation
Use-case 1: OBD2 request through a gateway

50% load – 500kbit/s

40% load – 500kbit/s

Simulated production delay

Conservative assumptions: FIFO, transmission errors

Time between the OBD2 request frame and reception of the first answer frame must not be greater than 50ms once every 1000 requests
Use-case 1: OBD2 request through a gateway

Time between the OBD2 request frame and reception of the first answer frame must not be greater than 50ms once every 1000 requests.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>OBD response times</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min</td>
<td>31.94</td>
</tr>
<tr>
<td>Average</td>
<td>34.29</td>
</tr>
<tr>
<td>Q3</td>
<td>46.55</td>
</tr>
<tr>
<td>Q4</td>
<td>49.31</td>
</tr>
<tr>
<td>Q5</td>
<td>53.45</td>
</tr>
<tr>
<td>Q6</td>
<td>55.32</td>
</tr>
<tr>
<td>Max</td>
<td>56.57</td>
</tr>
</tbody>
</table>
Use-case 2: end-to-end response time of a 10ms control frame

Functional level impact: less than 1 frame every $10^6$ above deadline=10ms is acceptable

$Q_6 = 8.9$
$\text{max} = 12.1$
Concluding remarks

1. Timing verification techniques & tools should not be trusted blindly

2. Simulation is well suited to systems that requires timing guarantees but
   - Are not well amenable to schedulability analysis
   - Or can tolerate deadline misses with a controlled level of risk

3. Some methodological aspects
   - Determine quantile wrt criticality, and simulation length wrt to quantile
   - Simulator and models validation
   - High-performance simulation engine needed for higher quantiles