# Timing verification of automotive communication architecture using quantile estimation

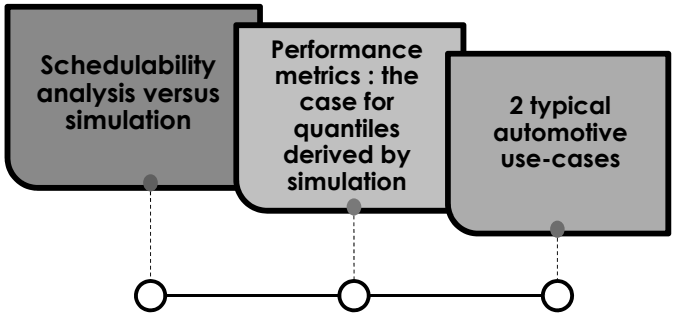
**Nicolas NAVET** (Uni Lu), Shehnaz LOUVART (Renault), Jose VILLANUEVA (Renault), Sergio CAMPOY-MARTINEZ (Renault) and Jörn MIGGE (RealTime-at-Work).

ERTSS'2014 - Toulouse, February 5-7, 2014.



## 1 Outline

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





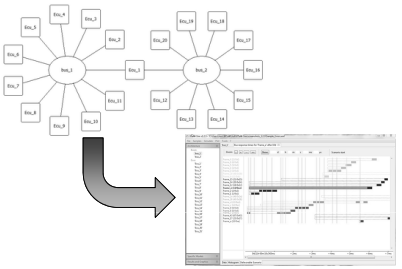

## 2 Automotive communication architectures

- ✓ 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** *"mathematic model of the worst-case possible situation"* VS **Simulation** *"program that reproduces the behavior of a system"*

$$K_i^k(t) \stackrel{\text{def}}{=} \underbrace{\left\lfloor \frac{J_i^k + \varphi_i^k(\phi^i)}{T_i^k} \right\rfloor}_{\text{max number of instances that can accumulate at critical instants}} + \underbrace{\left\lfloor \frac{t - \varphi_i^k(\phi^i)}{T_i^k} \right\rfloor + 1}_{\text{max number of instances arriving after critical instants}}$$



☺ 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 then

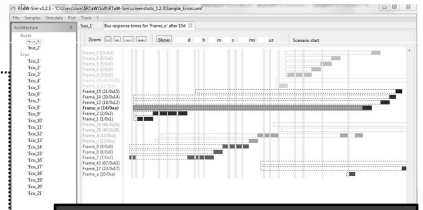
☺ Models close to real systems

☺ 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**

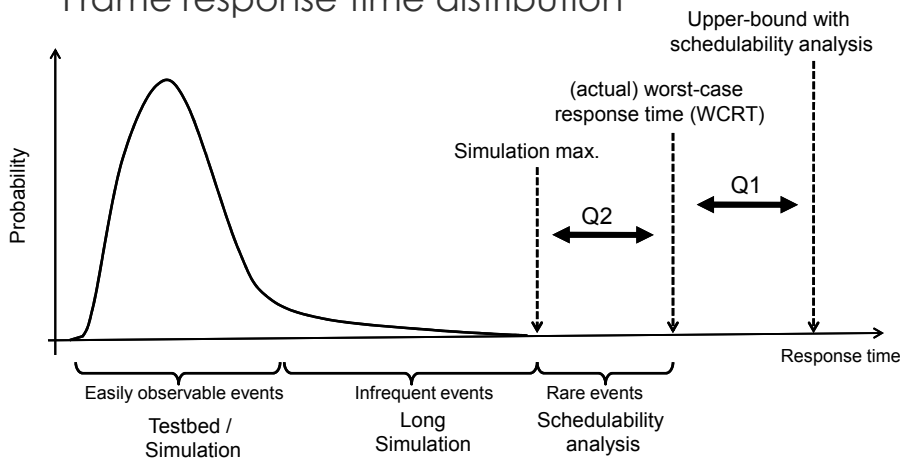
**Used in this study**
***RTaW-Sim*** → CAN simulator with schedulability analysis and configuration algorithms



# 2
# Metrics for the evaluation of frame latencies: the case for quantiles



## Frame response time distribution

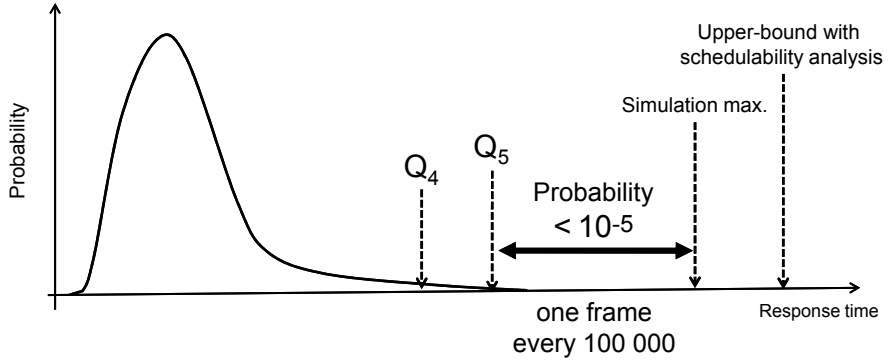



Q1: pessimism of schedulability analysis ?!
Q2: distance between simulation max. and WCRT ?!



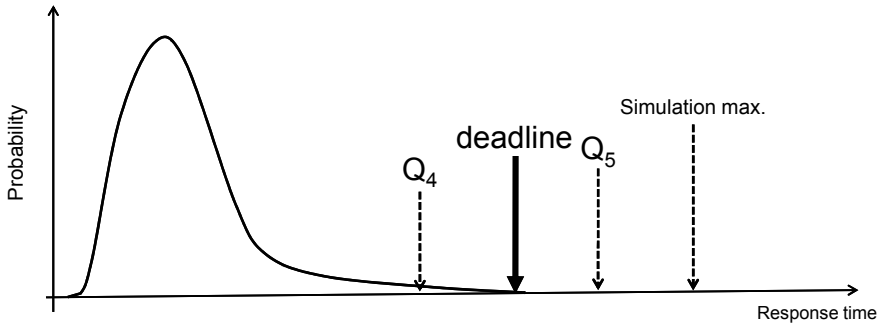
## Using quantiles means accepting a ***controlled*** risk

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

## 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

| Quantile | One frame every … | Mean time to failure Frame period = 10ms | Mean time to failure Frame period = 500ms |
|---|---|---|---|
| Q3 | 1 000 | 10 s | 8mn 20s |
| Q4 | 10 000 | 1mn 40s | ≈ 1h 23mn |
| Q5 | 100 000 | ≈ 17mn | ≈ 13h 53mn |
| Q6 | 1000 000 | ≈ 2h 46mn | ≈ 5d 19h |
| … | … | … | |

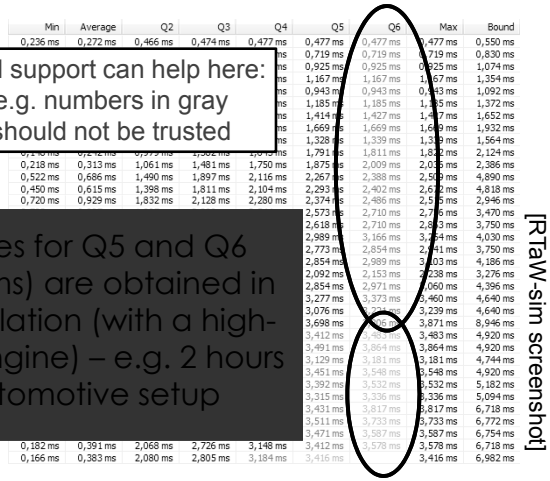
Warning : successive failures in some cases might be temporally correlated, this must be assessed!
Use of distributions of successive quantile overshoots, linear and non-linear dependency analysis



## 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




[RTaW-sim screenshot]

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



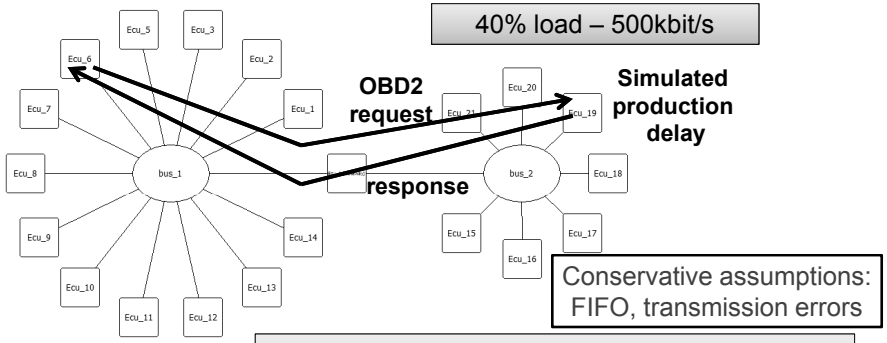
# 3

## Typical use-cases of quantile-based performance evaluation

## Use-case 1: OBD2 request through a gateway

50% load – 500kbit/s

40% load – 500kbit/s




Conservative assumptions: FIFO, transmission errors

[RTaW-sim screenshot]

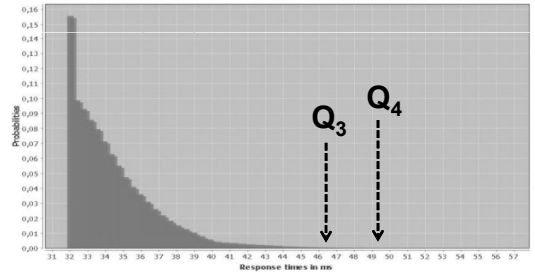
Time between the OBD2 request frame and reception of the first answer frame must not be greater than 50ms once every 1000 requests



## 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

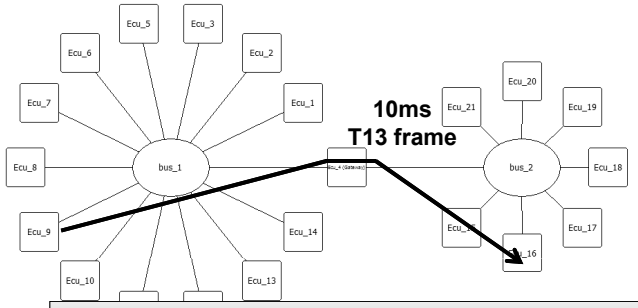
| Metrics | OBD response times |
|---|---|
| Min | 31.94 |
| Average | 34.29 |
| **Q3** | **46.55** |
| **Q4** | **49.31** |
| Q5 | 53.45 |
| Q6 | 55.32 |
| Max | 56.57 |




**Response time distribution**



## 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

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| T10 | 6 | P | 10 | 0 | 0,684 | 0,924 | 2,241 | | | | |
| T11 | 4 | P | 10 | 0 | 0,166 | 0,341 | 1,681 | | | | |
| T12 | 8 | P | 10 | 0 | 0,424 | 0,658 | 2,153 | | | | |
| T13 | 8 | B | | | 0,522 | 0,866 | 2,573 | 4,149 | 6,244 | 7,593 | 8,87 | 12,129 |
| T14 | 8 | P | 20 | 0 | 0,72 | 1,058 | 2,726 | 3,258 | 3,511 | 3,614 | 3,719 | 3,735 |
| T15 | 8 | P | 20 | 0 | 1,168 | 1,588 | 3,094 | 3,511 | 3,741 | 3,784 | 3,962 | 3,977 |

**$Q_6$ = 8.9**
**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