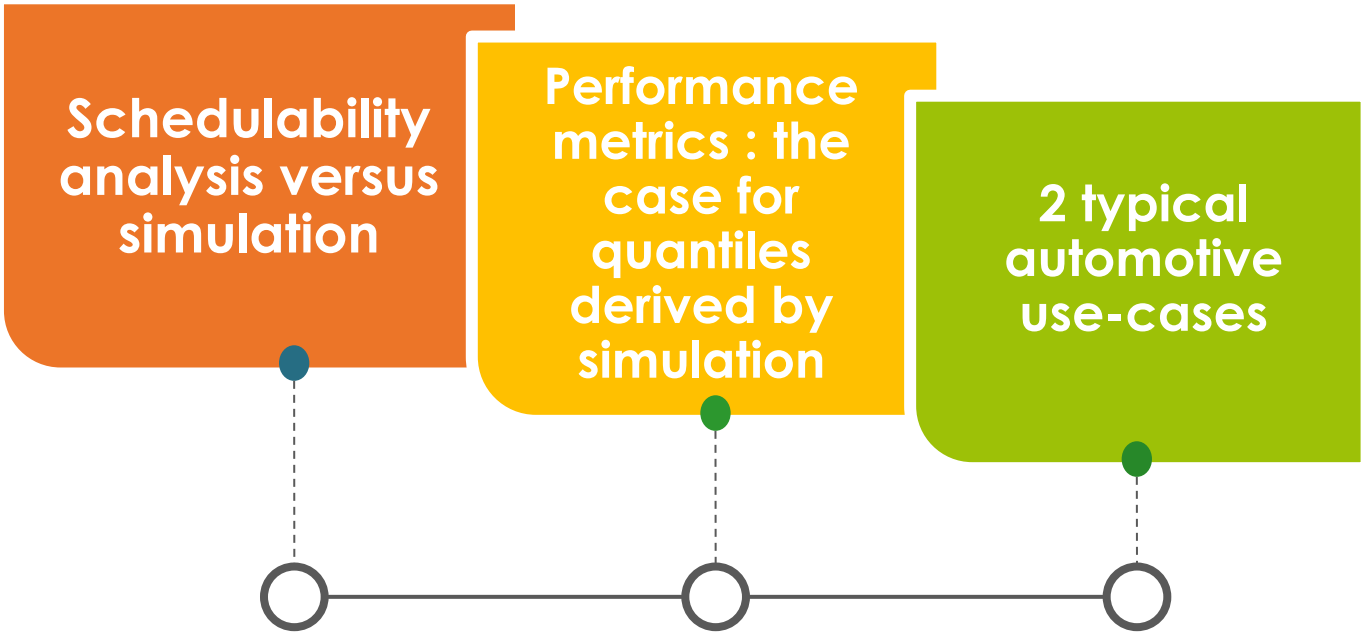
Timing verification of automotive communication architecture using quantile estimation

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

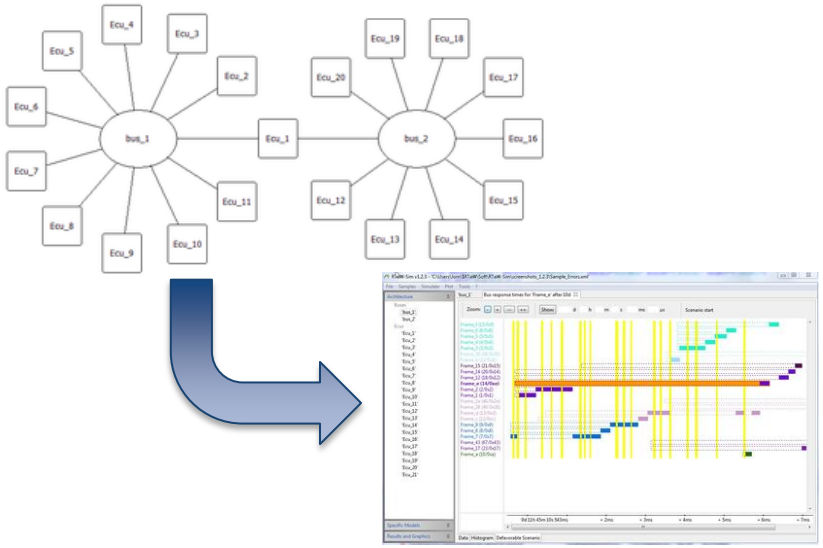
- ✓ Increased bandwidth requirements & timing constraints
- ✓ More complex & heterogeneous architectures with black-box ECUs
- ✓ Optimized CAN networks for higher bus loads: priorities, frame offsets, gateways, communication stacks, etc
- ✓ Verification activity of higher importance today, higher load 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

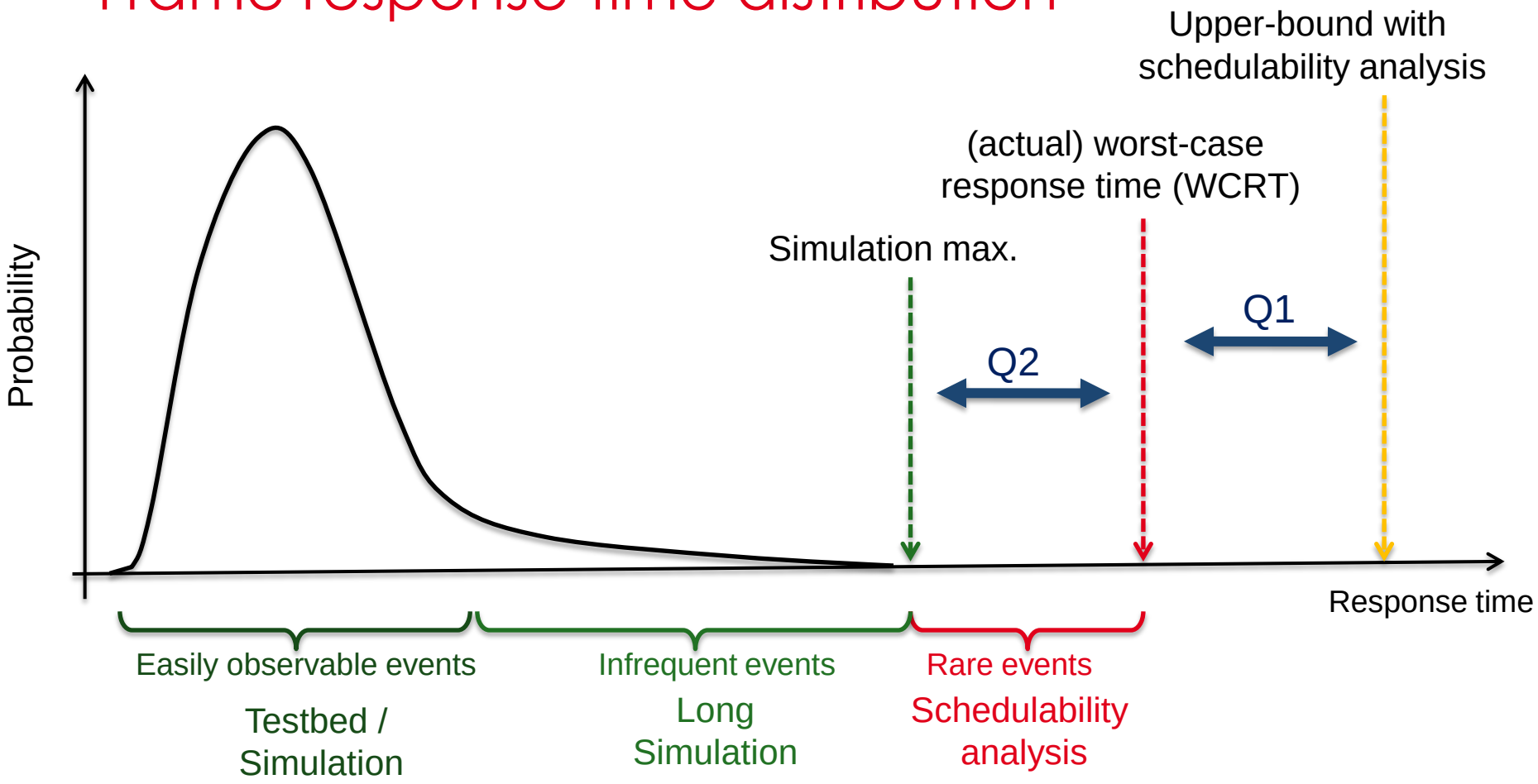
☺ Fine grained information

☹ Worst-case response times are out of reach! Occasional deadline misses must be acceptable

2

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

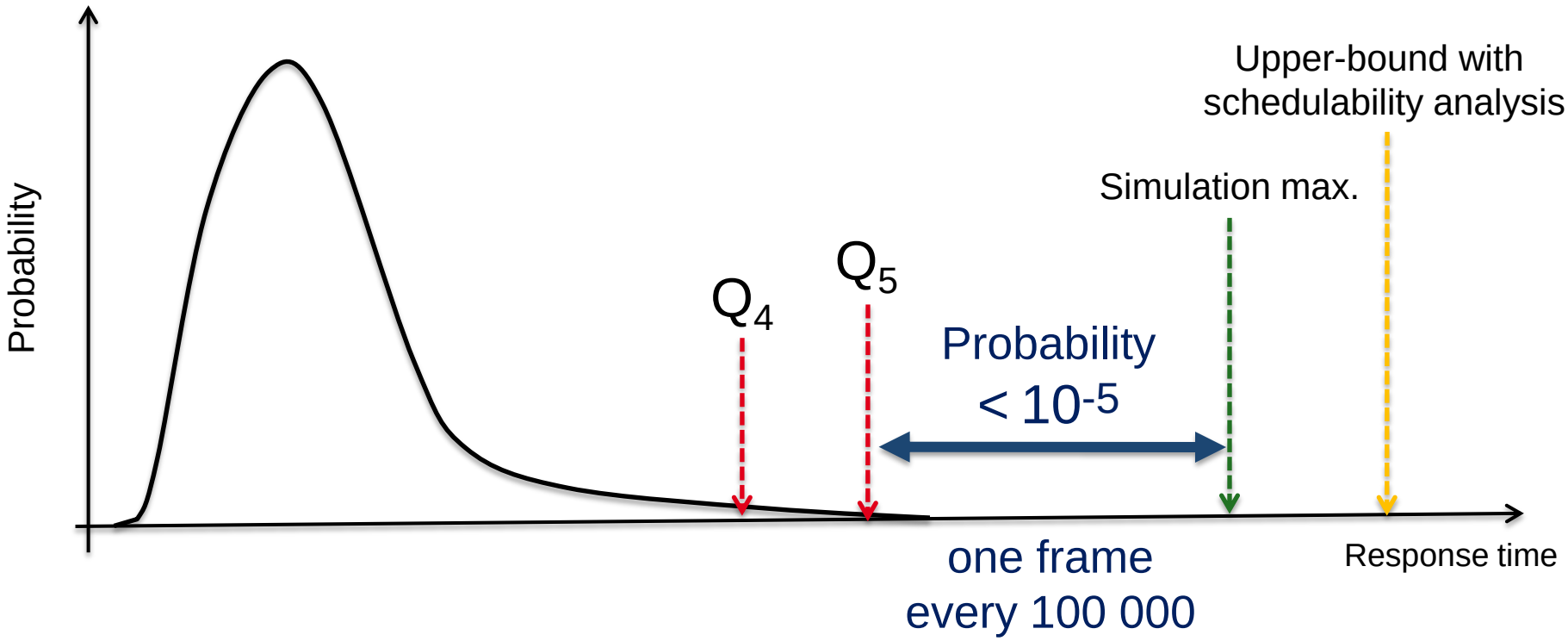
Frame response time distribution



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

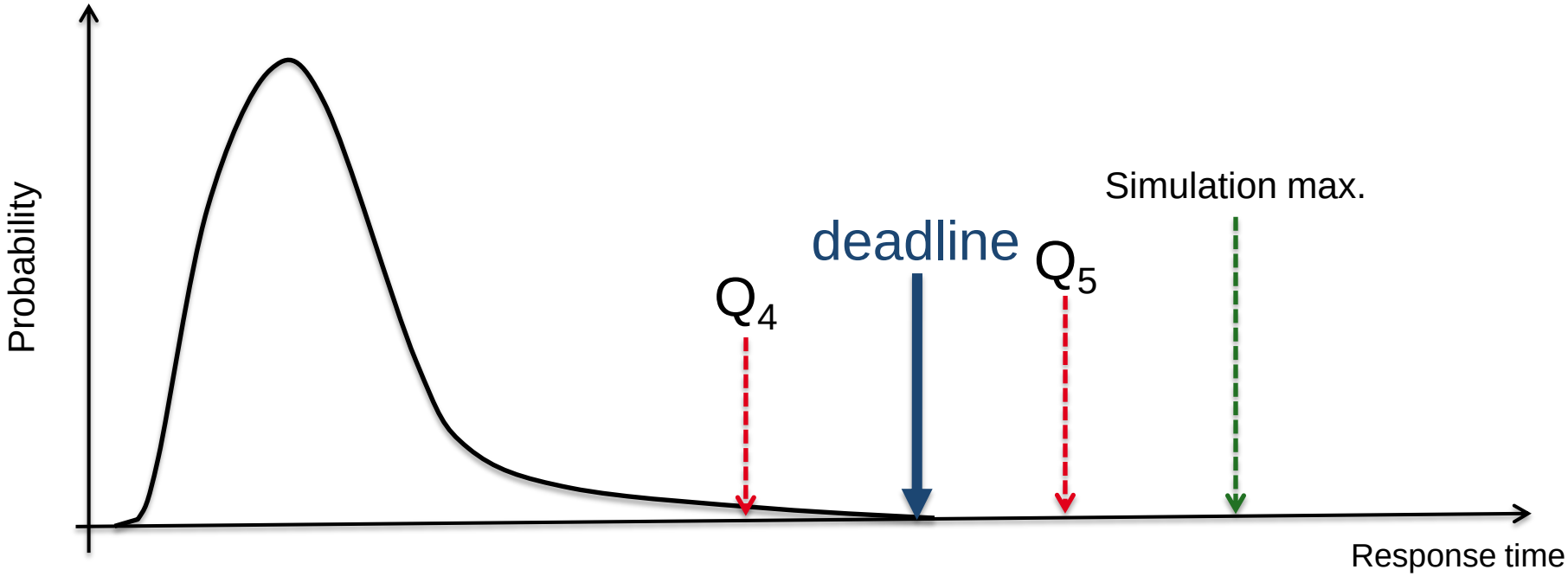
Using quantiles means accepting a ***controlled*** risk

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

Min	Average	Q2	Q3	Q4	Q5	Q6	Max	Bound
0,236 ms	0,272 ms	0,466 ms	0,474 ms	0,477 ms	0,477 ms	0,477 ms	0,477 ms	0,550 ms
					0,719 ms	0,719 ms	0,719 ms	0,830 ms
					0,925 ms	0,925 ms	0,925 ms	1,074 ms
					1,167 ms	1,167 ms	1,167 ms	1,354 ms
					0,943 ms	0,943 ms	0,943 ms	1,092 ms
					1,185 ms	1,185 ms	1,185 ms	1,372 ms
					1,414 ms	1,427 ms	1,427 ms	1,652 ms
					1,669 ms	1,669 ms	1,669 ms	1,932 ms
					1,328 ms	1,339 ms	1,339 ms	1,564 ms
					1,791 ms	1,811 ms	1,822 ms	2,124 ms
0,218 ms	0,313 ms	1,061 ms	1,481 ms	1,750 ms	1,875 ms	2,009 ms	2,035 ms	2,386 ms
0,522 ms	0,686 ms	1,490 ms	1,897 ms	2,116 ms	2,267 ms	2,388 ms	2,509 ms	4,890 ms
0,450 ms	0,615 ms	1,398 ms	1,811 ms	2,104 ms	2,293 ms	2,402 ms	2,672 ms	4,818 ms
0,720 ms	0,929 ms	1,832 ms	2,128 ms	2,280 ms	2,374 ms	2,486 ms	2,515 ms	2,946 ms
					2,573 ms	2,710 ms	2,716 ms	3,470 ms
					2,618 ms	2,710 ms	2,843 ms	3,750 ms
					2,989 ms	3,166 ms	3,264 ms	4,030 ms
					2,773 ms	2,854 ms	2,941 ms	3,750 ms
					2,854 ms	2,989 ms	3,103 ms	4,186 ms
					2,092 ms	2,153 ms	2,238 ms	3,276 ms
					2,854 ms	2,971 ms	3,060 ms	4,396 ms
					3,277 ms	3,373 ms	3,460 ms	4,640 ms
					3,076 ms	3,211 ms	3,239 ms	4,640 ms
					3,698 ms	3,806 ms	3,871 ms	8,946 ms
					3,412 ms	3,483 ms	3,483 ms	4,920 ms
					3,491 ms	3,864 ms	3,864 ms	4,920 ms
					3,129 ms	3,181 ms	3,181 ms	4,744 ms
					3,451 ms	3,548 ms	3,548 ms	4,920 ms
					3,392 ms	3,532 ms	3,532 ms	5,182 ms
					3,315 ms	3,336 ms	3,336 ms	5,094 ms
					3,431 ms	3,817 ms	3,817 ms	6,718 ms
					3,511 ms	3,733 ms	3,733 ms	6,772 ms
					3,471 ms	3,587 ms	3,587 ms	6,754 ms
0,182 ms	0,391 ms	2,068 ms	2,726 ms	3,148 ms	3,412 ms	3,578 ms	3,578 ms	6,718 ms
0,166 ms	0,383 ms	2,080 ms	2,805 ms	3,184 ms	3,416 ms		3,416 ms	6,982 ms

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

[RTaW-sim screenshot]

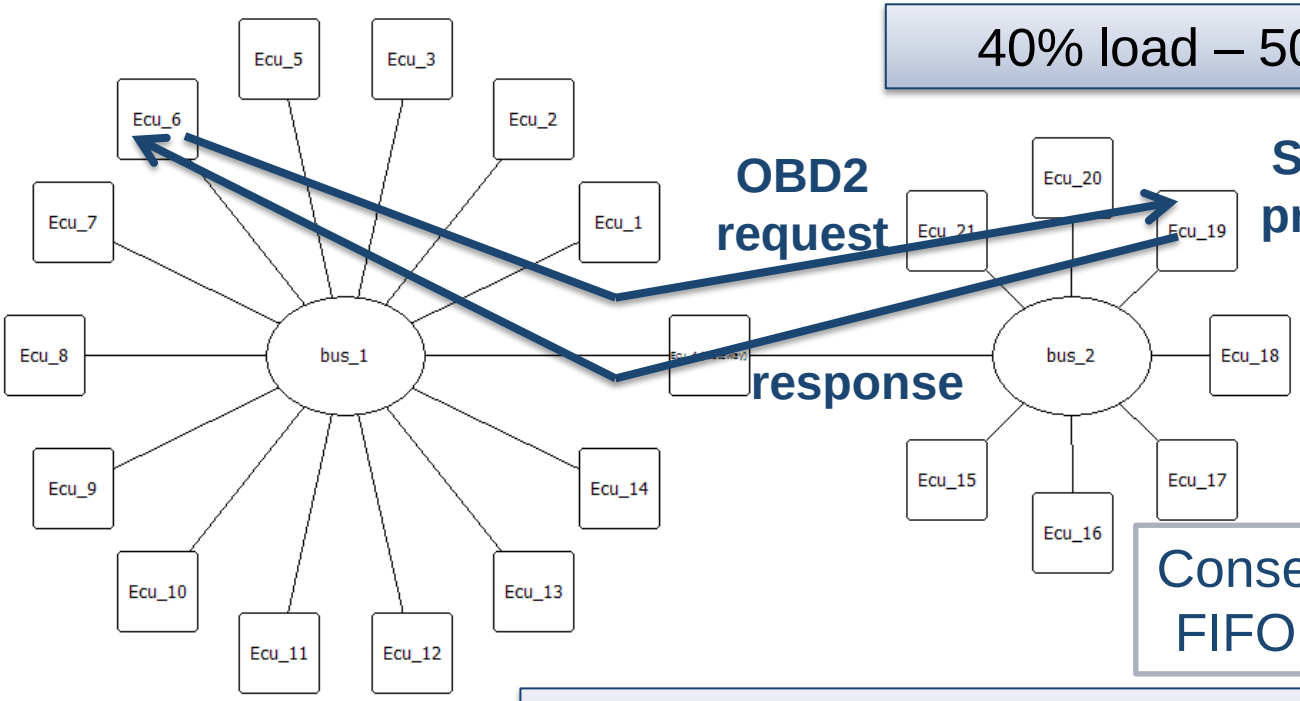
3

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

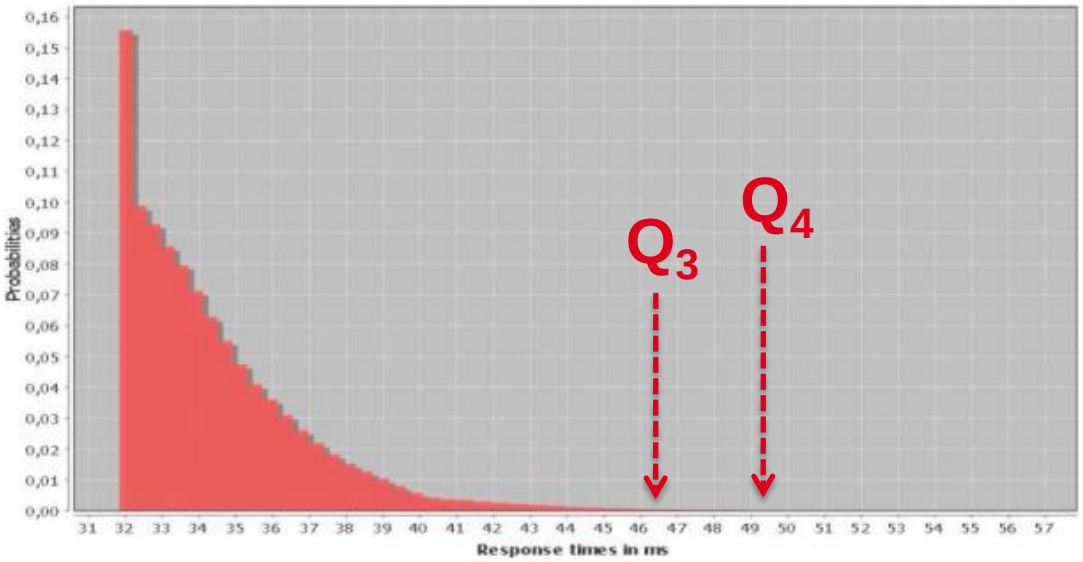
[RTaW-sim screenshot]

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

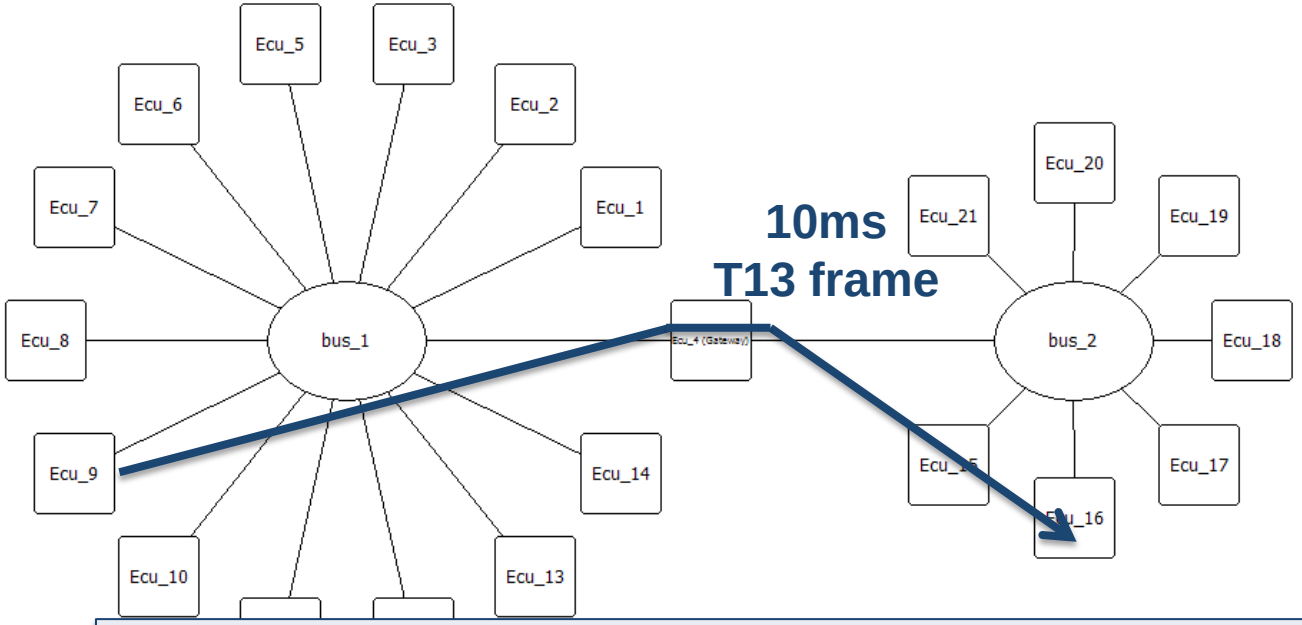
Time between the OBD2 request frame and reception of the first answer frame must not be greater than 50ms once every 1000 requests

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