TIMING VERIFICATION OF REAL-TIME AUTOMOTIVE ETHERNET NETWORKS: WHAT CAN WE EXPECT FROM SIMULATION?

Nicolas NAVET, University of Luxembourg
Jan R. SEYLER, Daimler A.G, Mercedes Cars
Jörn MIGGE, RealTime-at-Work (RTaW)
Use-cases for Ethernet in vehicles

**Infotainment**
- Synchronous traffic
- Mixed audio and video data
- MOST like

**Cameras**
- High data rates
- Continuous streaming
- LVDS like

**Diag. & flashing**
- Interfacing to external tools
- High throughput needed

**Control functions**
- **ADAS**
  - Time-sensitive communication
  - Small and large data payload
  - Cover CAN / Flexray use cases and more
Empirical study

Early stage verification techniques
- Simulation
- Analysis
- Lower bounds
- Performance metrics

Simulation Methodology
- Q1: is a single run enough?
- Q2: can we run simulation in parallel and aggregate results?
- Q3: simulation length?

What to expect from simulation and analysis?
- Q4: is worst-case analysis accurate?
- Q5: simulation to derive worst-case latencies?
- Q6: the case of a synchronous startup
Schedulability analysis
“mathematic model of the worst-case possible situation”

Simulation
“program that reproduces the behavior of a system”

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

max number of instances that can accumulate at critical instants

max number of instances arriving after critical instants

😊 Upper bounds on the perf. metrics → safe if model is correct and assumptions met

😊 Models close to real systems

😊 Fine grained information

🤔 Might be a gap between models and real systems → unpredictably unsafe then

🤔 Worst-case response times are out of reach - occasional deadline misses must be acceptable

$$S_{n+1} = F(S_n)$$
Is schedulability analysis alone sufficient?

1. Pessimism due to conservative and coarse-grained models $\rightarrow$ over-dimensioning of the resources

2. Complexity that makes analytic models error prone and hard to validate: black-box software, unproven and published analyses, small user-base, no qualification process, no public benchmarks, ..., main issue: do system meets analysis’ assumptions?

3. Inability to capture today’s complex software and hardware architectures $\rightarrow$ e.g., Socket Adaptor

- No, except if system conceived with analyzability as a requirement
- Good practice - several techniques & tools for cross-validation
Quantile $Q_n$: smallest value such that $P[\text{latency} > Q_n] < 10^{-n}$

Less than 1 frame every 100 000, 1 every 17mn with 10ms period

Using simulation means accepting a quantified risk system must be robust to that
Working with quantiles in practice – see [5]

1. Identify frame deadline
2. Decide the tolerable risk $\rightarrow$ target quantile
3. Simulate “sufficiently” long
4. If target quantile value is below deadline, performance objective is met
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>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Warning: successive failures in some cases might be temporally correlated, this can be assessed.
Performance metrics: illustration on a Daimler prototype network (ADAS, control functions)

Case-study #1: flows sorted by increasing WCTT

Less than 1 transmission every 100,000 above red curve

Min, Average, Q5, MAX, WCTT

WCTT (upper bound)

Max (sim)

Q5

Avg

Min

Frame Flow Needs

Case-study #1: flows sorted by increasing WCTT
Software Toolset and performance evaluation techniques

✓ **RTaW-Pegase** – modeling and analysis of switched Ethernet (industrial, automotive, avionics) + CAN (FD) and ARINC
✓ Higher-level protocols (e.g. Some IP) and functional behavior can be programmed in CPAL® language [4]

✓ Developed since 2009 in partnership with Onera

✓ Ethernet users include Daimler Cars, Airbus Helicopters and ABB

✓ **Worst-case Traversal Time (WCTT) analysis** - based on state-of-the-art Network-Calculus, all algorithms are published, core proven correct [2]
✓ **Timing-accurate Simulation** – ps resolution, ≈ 4·10⁶ events/sec on a single core (I7 - 3.4Ghz), suited up to (1-10⁶) quantiles
✓ **Lower-bounds on the WCTT** - “unfavorable scenario” [3]
CASE-STUDY #1 - Mercedes prototype Ethernet network

Topology of case-study #1 with a broadcast stream sent by ECU4

<table>
<thead>
<tr>
<th>#Nodes</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>#Switches</td>
<td>2</td>
</tr>
<tr>
<td>#Maximum</td>
<td>6us</td>
</tr>
<tr>
<td>switching</td>
<td></td>
</tr>
<tr>
<td>delay</td>
<td></td>
</tr>
<tr>
<td>#streams</td>
<td>58</td>
</tr>
<tr>
<td>#priority</td>
<td>2</td>
</tr>
<tr>
<td>levels</td>
<td></td>
</tr>
<tr>
<td>Cumulated</td>
<td>0.33Gbit/s</td>
</tr>
<tr>
<td>workload</td>
<td></td>
</tr>
<tr>
<td>Link data</td>
<td>100Mbit/s and</td>
</tr>
<tr>
<td>rates</td>
<td>1Gbit/s (2 links)</td>
</tr>
<tr>
<td>Latency</td>
<td>confidential</td>
</tr>
<tr>
<td>constraints</td>
<td></td>
</tr>
<tr>
<td>Number of</td>
<td>1 to 7</td>
</tr>
<tr>
<td>receivers</td>
<td>(avg: 2.1)</td>
</tr>
<tr>
<td>Packet period</td>
<td>0.1 to 320ms</td>
</tr>
<tr>
<td>Frame size</td>
<td>51 to</td>
</tr>
<tr>
<td></td>
<td>1450 bytes</td>
</tr>
</tbody>
</table>
CASE-STUDY #2 – medium AFDX network

Topography of case-study #2 with a multi-cast stream sent by node E1

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>#Nodes</td>
<td>52</td>
</tr>
<tr>
<td>#Switches</td>
<td>4</td>
</tr>
<tr>
<td>#Maximum switching delay</td>
<td>7us</td>
</tr>
<tr>
<td>#Streams</td>
<td>3214</td>
</tr>
<tr>
<td>#Priority levels</td>
<td>none</td>
</tr>
<tr>
<td>Cumulated workload</td>
<td>0.49Gbit/s</td>
</tr>
<tr>
<td>Link data rates</td>
<td>100Mbit/s</td>
</tr>
<tr>
<td>Latency constraints</td>
<td>2 to 30ms</td>
</tr>
<tr>
<td>Number of receivers</td>
<td>1 to 42 (avg: 7.1)</td>
</tr>
<tr>
<td>Packet period</td>
<td>2 to 128ms</td>
</tr>
<tr>
<td>Frame size</td>
<td>100 to 1500bytes</td>
</tr>
</tbody>
</table>
CASE-STUDY #3 – large AFDX network, as used in civil airplanes

Topology of case-study #3 with a multi-cast stream sent by node E1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>#Nodes</td>
<td>104</td>
</tr>
<tr>
<td>#Switches</td>
<td>8</td>
</tr>
<tr>
<td>#Maximum switching delay</td>
<td>7us</td>
</tr>
<tr>
<td>#streams</td>
<td>5701</td>
</tr>
<tr>
<td>#priority levels</td>
<td>5</td>
</tr>
<tr>
<td>Cumulated workload</td>
<td>0.97Gbit/s</td>
</tr>
<tr>
<td>Link data rates</td>
<td>100Mbit/s</td>
</tr>
<tr>
<td>Latency constraints</td>
<td>1 to 30ms</td>
</tr>
<tr>
<td>Number of receivers</td>
<td>1 to 83 (avg: 6.2)</td>
</tr>
<tr>
<td>Packet period</td>
<td>2 to 128ms</td>
</tr>
<tr>
<td>Frame size</td>
<td>100 to 1500bytes</td>
</tr>
</tbody>
</table>
Simulation and analysis models are in line in terms of what they model

Assumptions:
- Streams are strictly periodic and successive packets of a stream are all of the same size
- Nodes are not synchronized on startup, they start to send within 100ms (same results with larger values)
- Communication stack reduced to a queue: FIFO or priority queue
- Store-and-forward communication switches with a sub-10us max. switching delays
- No transmission errors, no packet losses in the switches

Simulation’s specific setup:
- Nodes’ clock drifts: 200ppm (same results with 400ppm)
- Each experiment repeated 10 times (with random offsets and clock drifts)
- Long simulation means at least 2 days of functioning time (samples large enough for Q5 for sub-100ms flows)
Simulation methodology
Intuitively, “a dynamic system is said to be ergodic if, after a certain time, every trajectory of the system leads the same distribution of the state of the system, called the equilibrium state”

Consequences:
- Q1: a single simulation run enough, initial conditions do not matter
- Q2: results from simulation run in parallel can be aggregated – how long is the transient state that occurs at the start?

Empirical approach: test if the distributions converge though the Q5 quantiles:
- Random offsets and random clock drifts
- Random offsets and fixed clock drifts
- Fixed offsets and random clock drifts
Case-study #1: flows sorted by increasing WCTT
Case-study #1: flows sorted by increasing WCTT

Comparing Q5 values of different simulations

Average difference between max and min value is 1.9%

1 second period packet simulation too short

3 experiments with random clock-drifts and random offsets
Case-study #2: flows sorted by increasing WCTT

1 second period packet simulation too short

3 experiments with random clock-drifts and random offsets

Average difference between max and min value is 2.3%
Q5: Case-study #3 – convergence of the Q5 quantiles

Comparing Q5 values of different simulations

Average difference between max and min value is 2.2%

3 experiments with random clock-drifts and random offsets

Case-study #1: flows sorted by increasing WCTT
Determine the minimum simulation length

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

Tool support can help here:
Right : numbers in gray should not be trusted
Left : derive simulation time wrt quantile

Reasonable values for Q5 (for periods up to 100ms) can be obtained in a few hours of simulation
What to expect from simulation and analysis?

Analysis (Network-Calculus) VS
Lower-bound (unfavorable scenario) VS
Timing-Accurate Simulation
Q4: Are Worst-Case Traversal Times (WCTT) computed with Network Calculus accurate?

WCTT are accurate in the non-prioritized case: average difference is 4.7% (up to 35%)

The actual true worst-case is between the two curves

Unfavorable scenario (lower bound)

WCTT (upper bound)

Case-study #2: flows sorted by increasing WCTT
Q5: Case-study #1 – difference between analysis upper bounds and simulation maxima

**Simulation max vs schedulability analysis**

- **Average difference is 21% - up to 48%**
- **5 frames above 35%**

Simulation max in the synchronous case and with random startup offsets

Case-study #1: flows sorted by increasing WCTT
Q5 : Case-study #2 – difference between analysis upper bounds and simulation maxima

average difference is 51% (up to 84%)

Case-study #2 : flows sorted by increasing WCTT
Q5: Case-study #3 – difference between analysis upper bounds and simulation maxima

Average difference is 56% (up to 88%)

Simulation max. vs schedulability analysis

WCTT (upper bound)

Sim. max synchronous startup

Sim. max random offsets

Case-study #3: flows sorted by increasing WCTT
Q5 : Memory usage in the switches: difference between analysis upper bounds and simulation maxima

Case-study #1: max. difference 31%

Ongoing work to reduce the pessimism of the memory usage analysis

Case-study #2: max. difference 74%

Case-study #3: max. difference 76%
State-of-the-start Network-Calculus is an accurate and fast technique for switched Ethernet - can be coupled with other types schedulability analysis for CAN (FD), gateways, ECUs.

Deriving lower-bounds with unfavorable scenarios approaches is key to validate correctness and accuracy → more research still needed here

Simulation suited to assess – with high confidence - the performances in a typical functioning mode → worst-case latencies/buffer usage are out of reach - except in small systems

Worst-case latencies are extremely rare events (less than once every $10^6$ transmissions) - if network can be made robust to these cases, then designing with simulation is more effective in terms of resource usage
Q6: synchronous startup of the node leads to very unfavorable trajectories
Synchronous startup of the system: many large latencies observed shortly after startup - statistics are biased wrt typical functioning mode

Two explanations:
- no offsets between streams on nodes
- symmetry of the network

Case-study #3 - maximum latencies observed in simulation in last switch for flow FF3 (top) occurring immediately after a synchronous startup
Synchronous startup of the system – short simulation are enough for maxima

The simulation maximum latencies is usually seen during the first few seconds.

Case-study #3: flows sorted by increasing simulation maximum (2 days)

Tails of the latency distributions are identical

Black curve: Simulation max after 2 days

Blue curve: Simulation max after 1mn
Synchronous startup of the system – all other statistics eventually converge, but transient state takes time to be amortized.

**Q5 : random vs synchronous offsets**

**Green curve:** Simulation Q5 after 2 days - synchronous startup

**Black curve:** Simulation Q5 after 2 days – random offsets

**Red curve:** Simulation Q5 after 8 days – synchronous startup

Case-study #3: flows sorted by increasing simulation maximum
Concluding remarks

- Timing verification techniques & tools should not be trusted blindly → body of good practices should be developed
- AUTOSAR communication stacks support the numerous automotive communication requirements at the expense of complexity → schedulability analyses cannot capture everything
- Simulation is well suited to automotive systems that can tolerate deadline misses with a controlled risk
- Today: timing accurate simulation of complete heterogeneous automotive communication architectures
- Tomorrow: system-level simulation with models of the functional behavior
- Ergodicity, evidenced here empirically for Ethernet, must be studied theoretically at a the scope of the system
Thank you

Interested in this talk?
You can consult the associated paper published at ERTSS’2016
References
Interested in this talk? Please consult the technical report available from www.realtimeatwork.com


