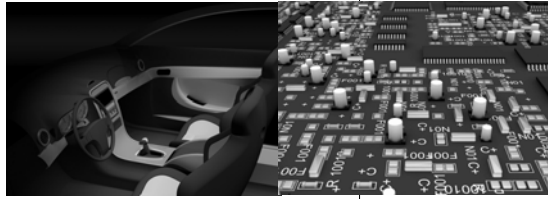


Aperiodic traffic in response time analyses with adjustable safety level

Dawood A. KHAN (INRIA / INPL)
Nicolas NAVET (INRIA / RTaW)
Bernard BAVOUX (PSA)
Jörn MIGGE (RTaW)



ETFA'2009, Palma
24/09/2009

Validation is a key activity in automotive systems design
Personal view on the developments

Mostly ahead
of us!

« correctness by construct » and
optimal synthesis

Probabilistic analysis
system level

« Worst-case » deterministic analysis
system level

Probabilistic analysis (sub-system)

« Worst-case » deterministic analysis (sub-system)

« Smart » monitoring tools

Simulation tools (co-simulation, HIL)

1994

1997

2009



Probabilistic analysis is needed

- Systems are not designed for the worst-case (provided it is rare enough!)
- Reliability/Safety are naturally expressed and assessed in terms of probability (e.g. $< 10^{-9}$ per hour)
- Deterministic assumptions are sometimes unrealistic or too pessimistic, e.g.:
 - Worst-Case Execution Time on modern platforms,
 - Aperiodic activities: ISR, frame reception,
 - ...
- Faults/errors are not deterministic (and better modeled probabilistically)



Accounting for the aperiodic traffic

- Transmission patterns can hardly be characterized: purely aperiodic, mixed periodic/aperiodic, etc
 - Aperiodic frames do jeopardize RT constraints
 - Few approaches in the litterature:
 - deterministic approaches, such as sporadic, generally lead to unusable results (e.g., $\rho > 1$)
 - Average case probabilistic approach not suited to dependability-constrained systems
- Probabilistic approaches with safety adjustable level, see paper ref[6] and ref[7]



Approach advocated here

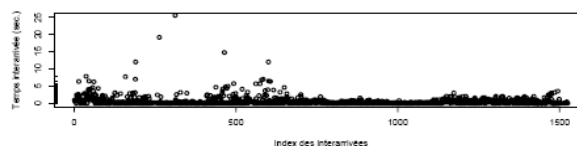
- 1) Measurements / data cleaning
- 2) Modeling aperiodic traffic arrival process
- 3) Deriving aperiodic Work Arrival Process (WAF)
- 4) Integrating aperiodic WAF into schedulability analysis



Data trace analysis

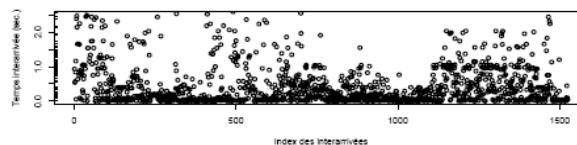
y: aperiodic interarrival times – x: index of interarrivals

ZOOM +

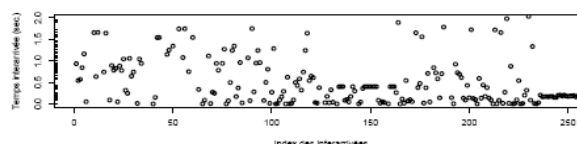


x : [0-1500]
y : [0-25]

Approximate because what is seen on the bus is not the actual arrival process at ECU level! can be handled



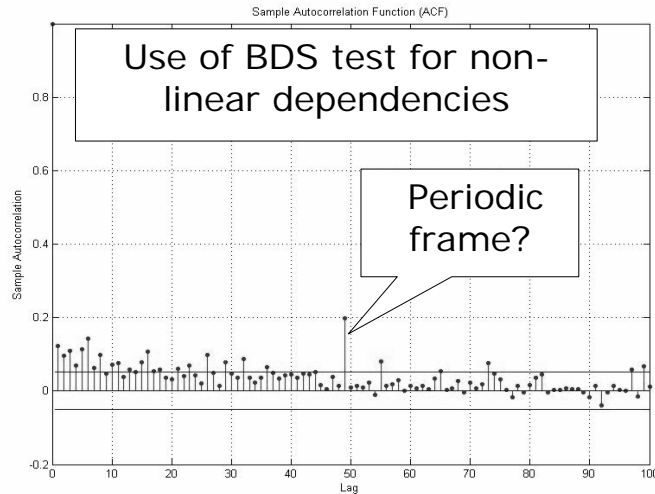
x : [0-1500]
y : [0-2.5]



x : [0-250]
y : [0-2]

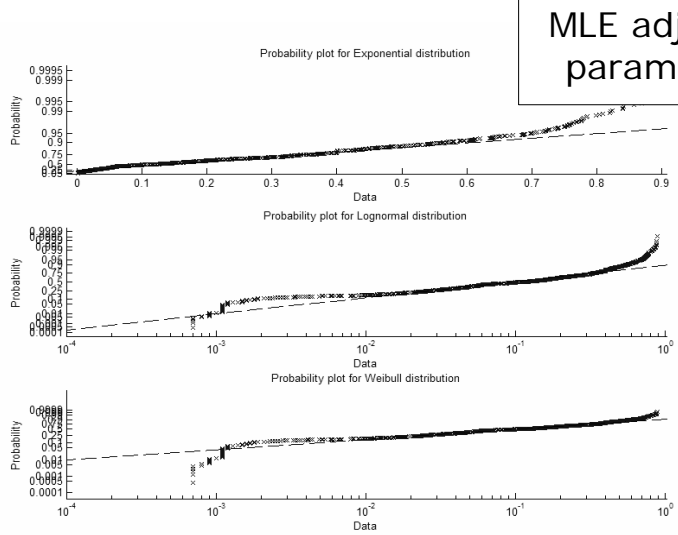


Question: are interarrival times i.i.d. ?

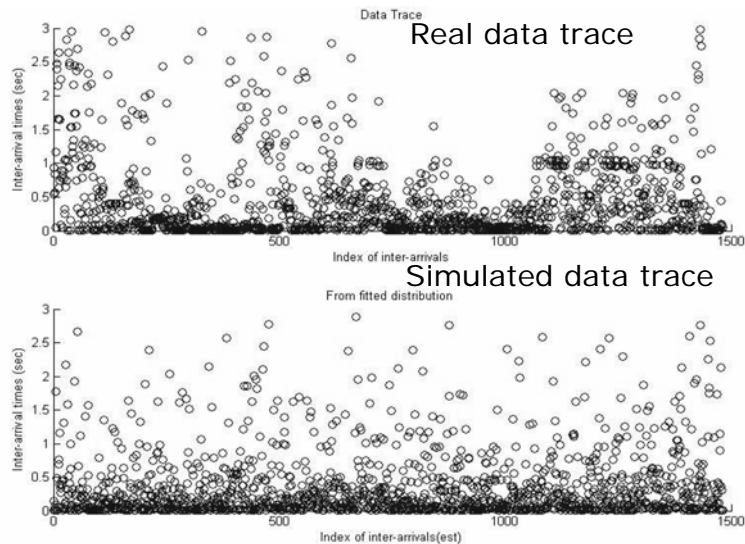


Distribution fitting for aperiodic interarrival : 3 candidates here

Kolmo. Smi. and χ^2 tests to confirm visual impression



Captured data trace VS random trace generated with MLE-fitted Weibull



PSA PEUGEOT CITROËN



INRIA

RTaW
RealTime-at-Work

Deriving the aperiodic WAF

- $S(t)$: aperiodic WAF
- $X(t)$: stochastic process which counts the number of aperiodic frames in time interval t
- “smallest” $S(t)$ such that the probability of $X(t)$ being larger than or equal to $S(t)$ is lower than a threshold α

$$\hat{S}(t) = \min\{S(t) \mid \underline{Pr}[X(t) \geq S(t)] \leq \alpha\}$$

By simulation, numerical approximation or analysis (simplest cases such as exp.)

Design choice:
e.g., 10^{-9}

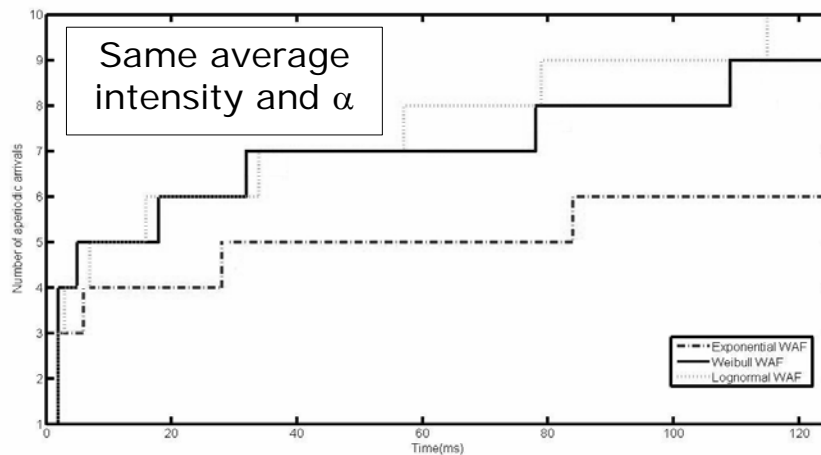
PSA PEUGEOT CITROËN



INRIA

RTaW
RealTime-at-Work

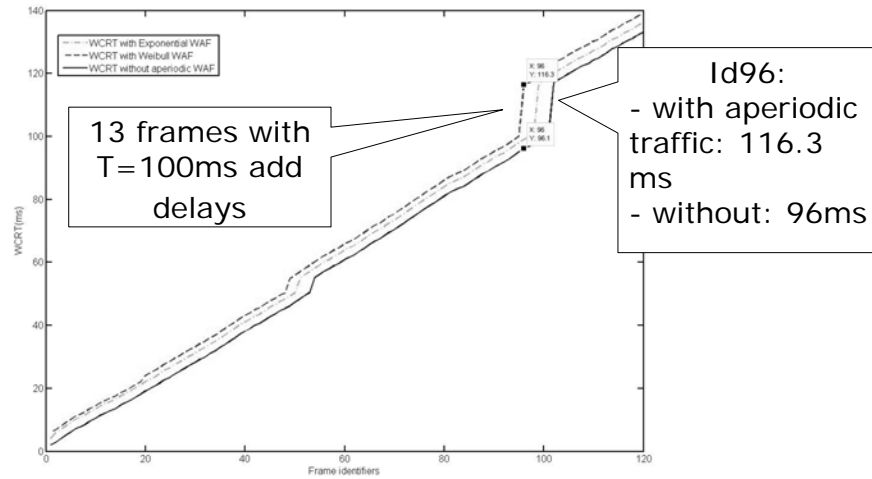
Aperiodic WAF depends on the underlying interarrival distribution



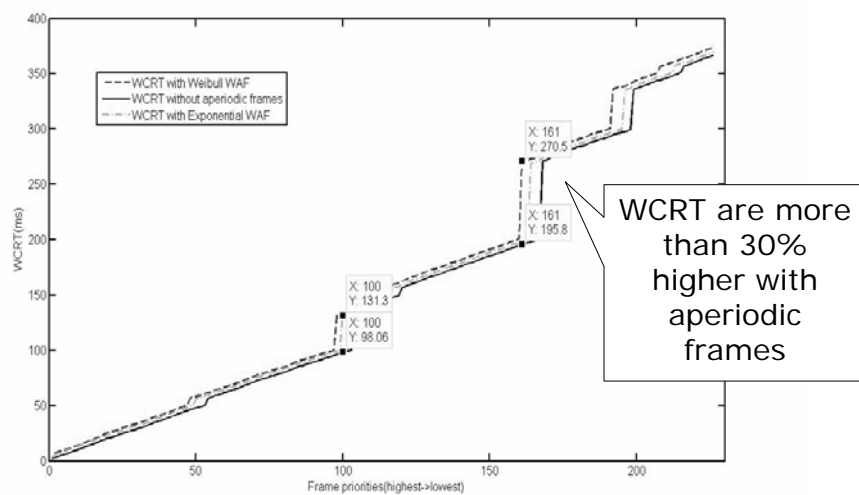
Case-study on a typical body network

- Body network benchmark generated using GPL-licensed Netcarch
- Characteristics:
 - 125kbps, 16 ECUs, 105 CAN frames with deadlines equal to periods and 1 to 8 bytes of data.
 - Total periodic load is equal to 41%
- NETCAR-Analyzer for WCRT computation
- 3% aperiodic traffic
- 7 byte aperiodic frames
- $\alpha = 10^{-4}$

Worst-case response times with/out aperiodic traffic (3%)



On a more loaded network...



Observations

- In this context where the periodic load is relatively small and the aperiodic traffic is limited (3%) one observes:
 - aperiodic traffic significantly impacts the worst-case response times of the periodic frames (more than +30% sometimes).
 - the exact model of the aperiodic traffic plays some role
 - depends on the priority of the aperiodic frames (working on this)
 - Measured arrival time on bus at which the frames started to be transmitted can be different than time at which the transmission requests were issued



Conclusion

- Chosen dependability requirements are met while pessimism kept to minimum:
 - Practical approach
 - Real data are required
 - Can be extended to the non i.i.d. case (not needed here)
- What is needed now is a system level approach that
 - Can handle arbitrary activation processes
 - goes beyond the i.i.d. case (for dependability assessment)



References



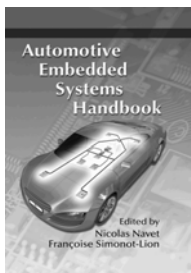
References (1/2)

Automotive Embedded Systems - General

- [1] N. Navet, F. Simonot-Lion, editors, The Automotive Embedded Systems Handbook, Industrial Information Technology series, CRC Press / Taylor and Francis, ISBN 978-0849380266, December 2008.
- [2] P. Wallin, Axelsson, A Case Study of Issues Related to Automotive E/E System Architecture Development, IEEE International Conference and Workshop on the Engineering of Computer Based Systems, 2008.
- [3] H. Hansson, M. Nolin, T. Nolte, Beating the Automotive Code Complexity Challenge: Components, Models and Tools, National Workshop on High-Confidence Automotive Cyber-Physical Systems, 2008.

Dependability / probabilistic framework

- [4] N. Navet, H. Perrault, "Mécanismes de protection dans AUTOSAR OS", RTS Embedded Systems 2009 (RTS'09), Paris, April 2009.
- [5] D. Khan, N. Navet, B. Bavoux, J. Migge, "Aperiodic Traffic in Response Time Analyses with Adjustable Safety Level", IEEE ETFA2009, Mallorca, Spain, September 2009.
- [6] N. Navet, Y-Q. Song, F. Simonot, "Worst-Case Deadline Failure Probability in Real-Time Applications Distributed over CAN (Controller Area Network)", Journal of Systems Architecture, Elsevier Science, vol. 46, n°7, 2000.
- [7] A. Burns, G. Bernat, I. Broster, A probabilistic framework for schedulability analysis, Third International Conference on Embedded Software (EMSOFT 2003), 2003.



Questions / feedback ?



Please get in touch at:
nicolas.navet@realtimedatwork.com
<http://www.realtimedatwork.com>

PSA PEUGEOT CITROËN



INRIA

RTaW
RealTime-at-Work