Automotive communication systems : from dependability to security

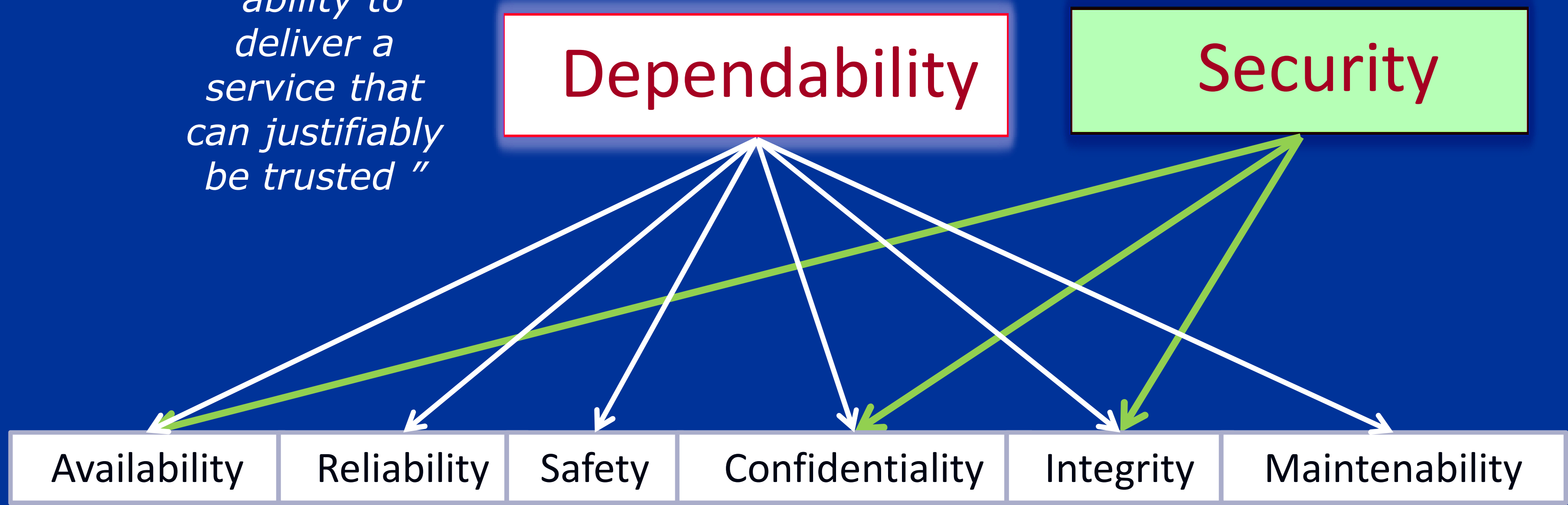
Nicolas NAVET
Real-Time and Interoperability (TRIO) Group at INRIA Nancy

1st Seminar on Vehicular Communications and Applications (VCA 2011)
NetLab / SnT, Luxembourg - 30/05/2011

Dependability vs Security [from Laprie et al, ref.3]

"absence of unauthorized access to, or handling of, system state"

"ability to deliver a service that can justifiably be trusted "



- **Availability**: *Readiness for usage* — *for authorized users only*
- **Reliability**: *Continuity of service*
- **Safety**: *Absence of catastrophic consequences*
- **Confidentiality**: *Absence of unauthorized disclosure of information*
- **Integrity**: *Absence of improper system alterations* — *"unauthorized" system alteration*
- **Maintenability**: *Ability to undergo repairs and evolutions*

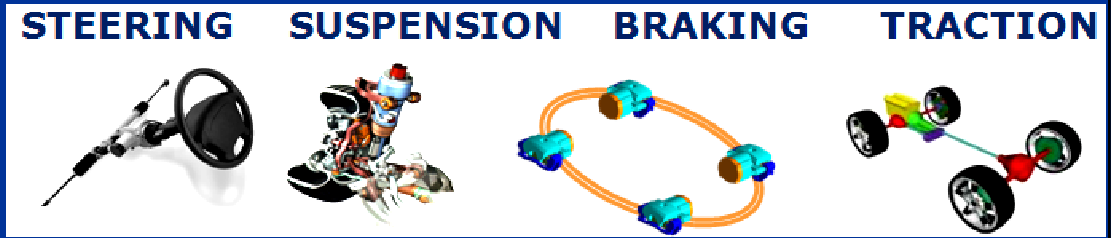
Outline

1. **Trends in automotive embedded systems:** increasing safety requirements and complexity
2. **The (numerous) impediments/threats to dependability:** with a focus on timing constraints verification
3. **Security against malicious attacks :** physical access to the vehicle or wireless access

Focus on the verification issues at the development phase
of the communication systems - highlight issues, not about solutions

Electronics is the driving force of innovation

Many new functions are safety critical: brake assist, cruise control, lane keeping, dynamic lights, etc

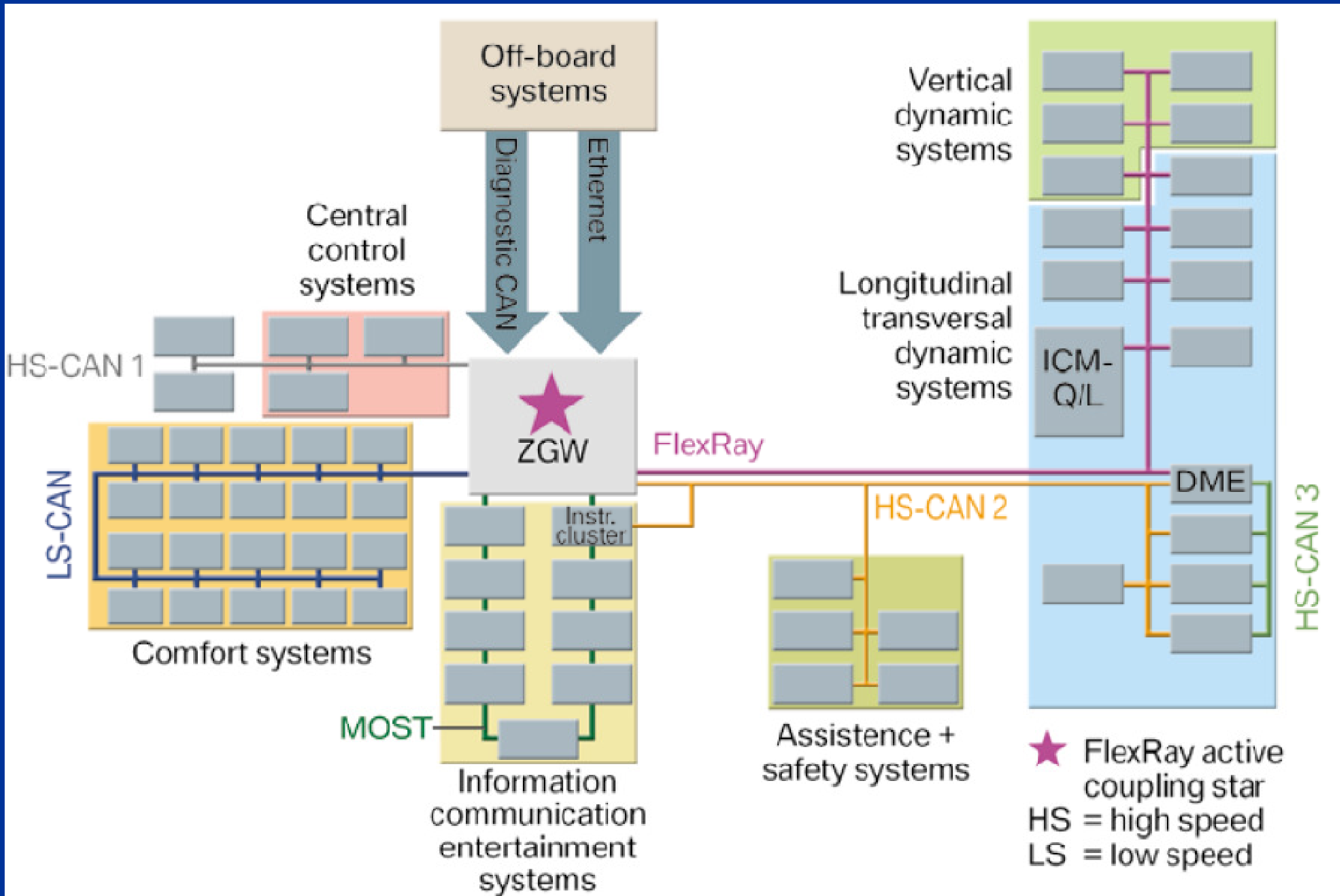


Picture from [10]

- 90% of new functions use software
- Electronics: 40% of total costs
- Huge complexity: 70 ECUs, 2500 signals, >6 comm. protocols, multi-layered run-time environment (AUTOSAR), multi-source software, multi-core CPUs, number of variants, etc

Strong costs and time-to-market constraints !

BMW 7 Series networking architecture [10]



Picture from [4]

- ZGW = central gateway
- 4 CAN buses
- 1 FlexRay Bus
- 1 MOST bus
- Several LIN Buses (not shown here)
- 1 Ethernet bus
- Wireless

Impediments to safety: complexity!

Technologies: numerous, complex and not explicit. conceived for critical systems

– e.g.: more than 150 specification documents (textual) for Autosar, no two implementations can behave identically!

Size of the system!

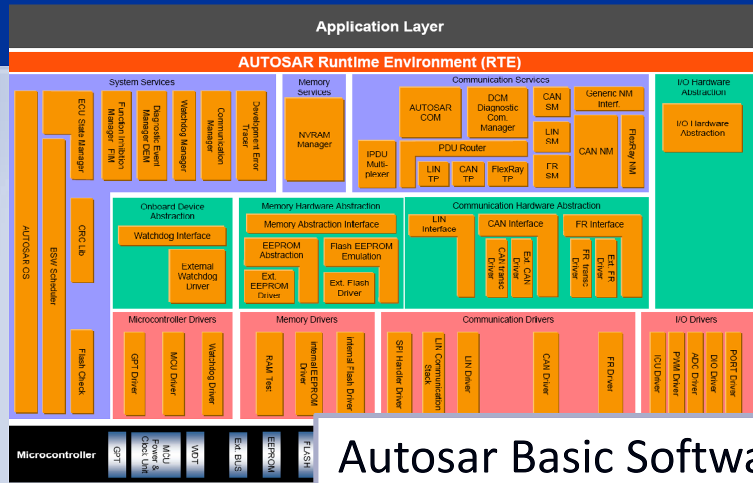
– Number of functional domains, buses, gateways, ECUs, size of code, tasks, wiring, number of variants, etc

Design process

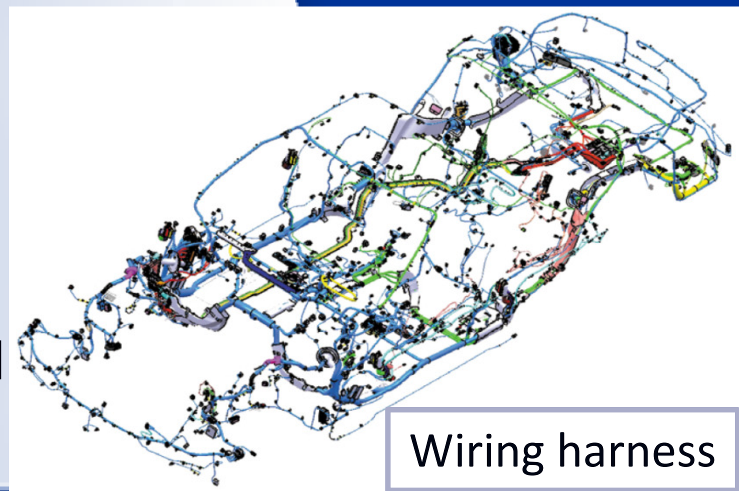
– Most developments are not done in-house : less control on externalized developments

– Carry-over / Vehicle Family Management : need to share/re-use architecture and sub-systems between several brands/models with different requirements [2]

– Optimized solutions for each component / function does not lead to a global optimal! [2]



Autosar Basic Software



Wiring harness

Picture from [4]

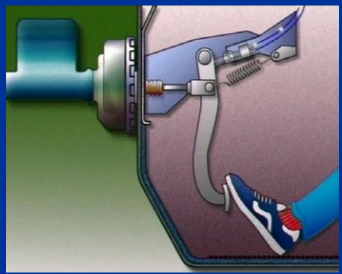
impediments to safety: cultural/regulatory

- Eg: Automotive embedded systems have not been designed with the same standards as airplanes - different tradeoff costs / safety :
  - little (no?) fault-tolerance using hardware redundancy
  - Technical parameters are regarded as less important than cost for supplier / components selection [2]
  - ISO2626-2 upcoming standard: no safety quantification, in-house certification accepted
  - Lack well-accepted design process, decision on experience, “gut-feeling”, poor tool support [2]
  - **Verification / validation does not ensure 100% coverage**

Formal verification is gaining acceptance:
code analysis, timing analysis, etc

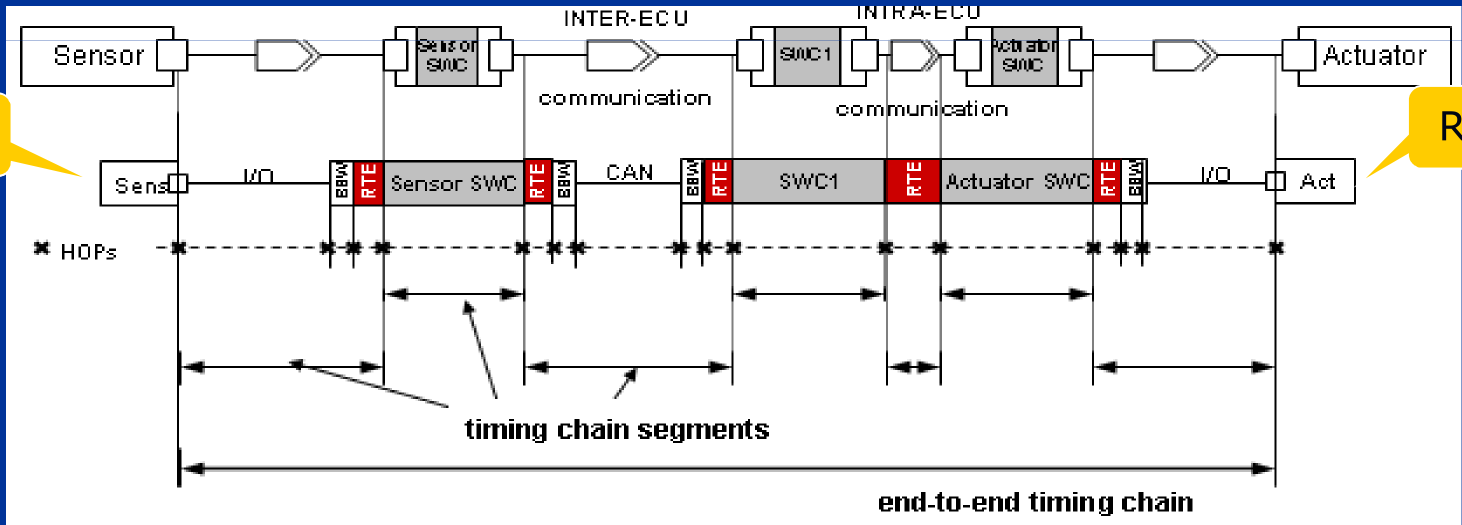
Threats to safety :
the case of timing constraints

Several hundreds of timing constraints: responsiveness, data refresh rate



Constraint : brake light on < 50ms

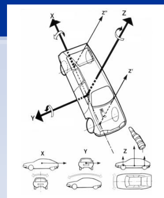
Stimulus



Response

Figure from [12]

Why timing constraints may not be respected occasionally?



Lack of precise specification : hard to identify the right timing requirements for each function

Lack of traceability : from the architects to the suppliers

Flaws in the verification:

– Knowledge of the system and its environment is incomplete:
  - What is done by the suppliers?
  - Implementation choices really matter and standards do not say everything
  - Environmental issues: EMI, α-particles, heat, etc
  - Traffic is not always well characterized and/or well modeled e.g. aperiodic traffic ?! see [5]

– Testing /simulation alone is not enough

– Analysis is not enough too:
  - Analytic models, especially complex ones, can be wrong (remember " CAN analysis refuted, revisited, etc" [6] ?!)
  - They are often much simplified abstraction of reality and might become optimistic: neglect FIFOs, hardware limitations

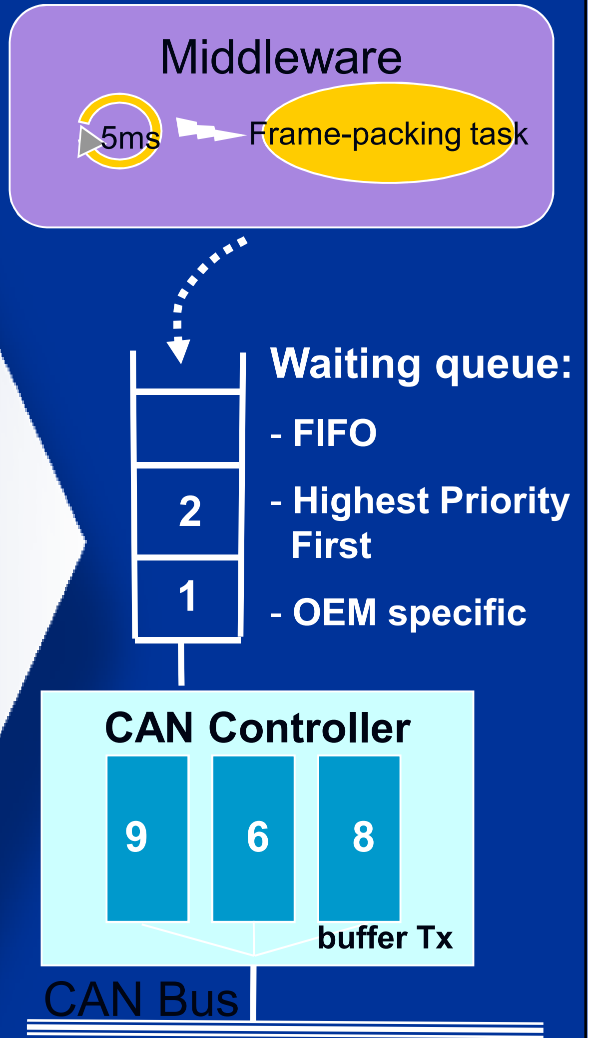
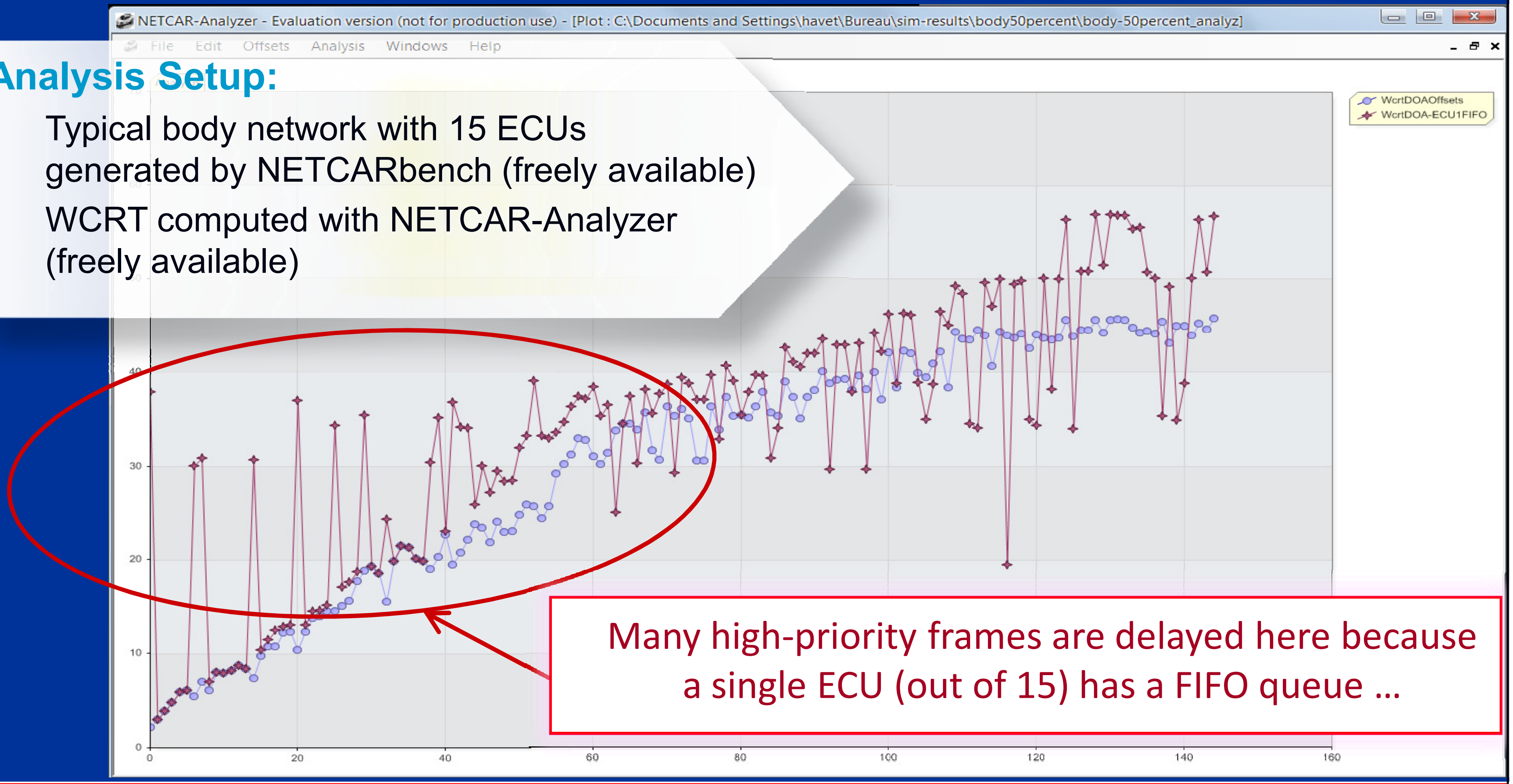


Illustration: Worst-Case Response Times on a CAN bus

Frame waiting queues are HPF, except ECU1 where queue is FIFO
the OEM does not know or verification software cannot handle it …



Analysis Setup:

- Typical body network with 15 ECUs generated by NETCARbench (freely available)
- WCRT computed with NETCAR-Analyzer (freely available)

Many high-priority frames are delayed here because a single ECU (out of 15) has a FIFO queue …

Threats to dependability: Faults → errors → service failures [3]

When faults are introduced in the development phase ?

– Requirements capture + Specification + SW development: 99% (infineon [10])
– HW development : ε

Why ? The factors :

– Technologies: not conceived with dependability as a priority
– Complexity / size of the system
– Developments are mainly externalized
– Strong cost / time-to-market pressure
– Limited regulatory constraints
– Limited used of formal methods for verification
– Human factors
– etc

INRIA

RTaW RealTime-at-Work

Security : some identified risks and scenarios

Security : two scenarios

Case 1 : **attackers have physical access to the vehicle**

- Easy to get access to internal networks through the On-Board Diagnostic (OBDII) port
- AFAIK, automotive systems are not protected at all
- Open question: should we go beyond basic protection measures? Can we afford it?

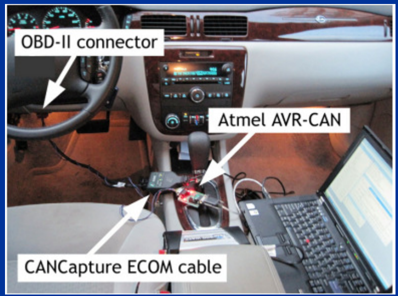
Case 2 : **remote access through wireless networks**

- Strong protection needed against remote attacks because of Internet access, manufacturer telematics services, Car-to-Car & Car-to-infrastructure communication, , etc
- Open question: is it the case today ?

INRIA

RTaW
RealTime-at-Work

Physical access to the vehicle: experiments in [11]



Picture from [11]

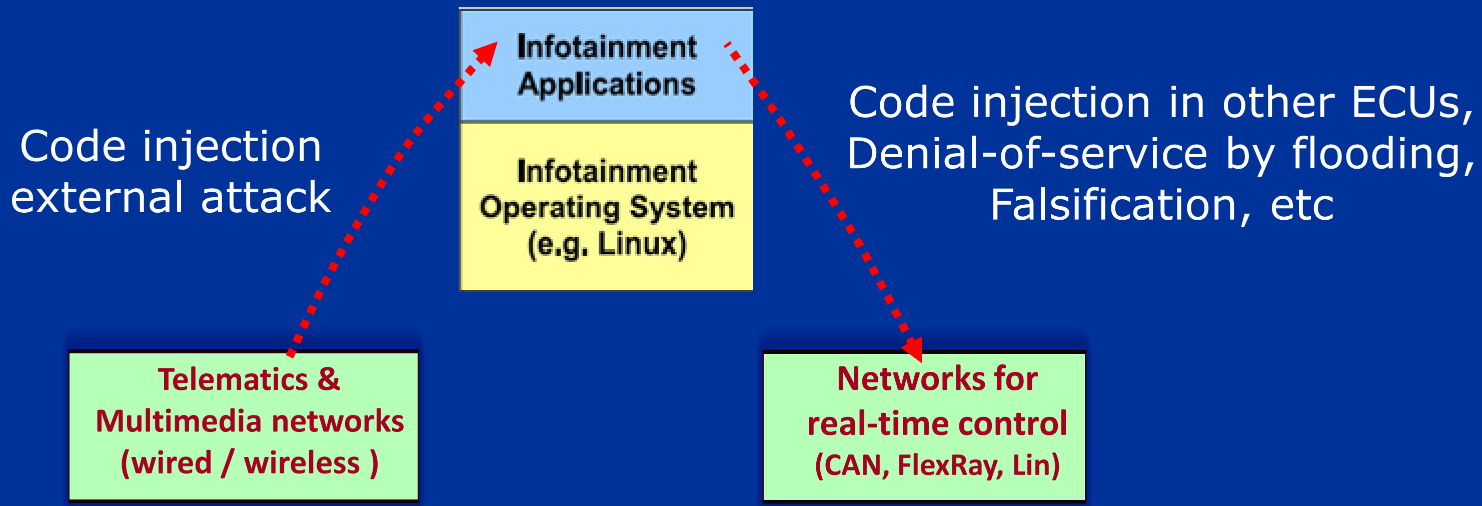
Connection to the OBD-II port

Attacks performed :

- Manipulate speedometer
- Injection of malicious code by re-flashing ECUs (while driving!)
- Disable communications on the CAN buses
- Disable all lights
- Stop the engine
- Disable / lock (specific) brakes
- Were able to manipulate all ECUs!

Attacks through the wireless interfaces

Issue: there are a number of ECUs that have access to both the internal networks and wireless networks, e.g. radio player, bluetooth transmitters, wireless tire pressure sensors, etc

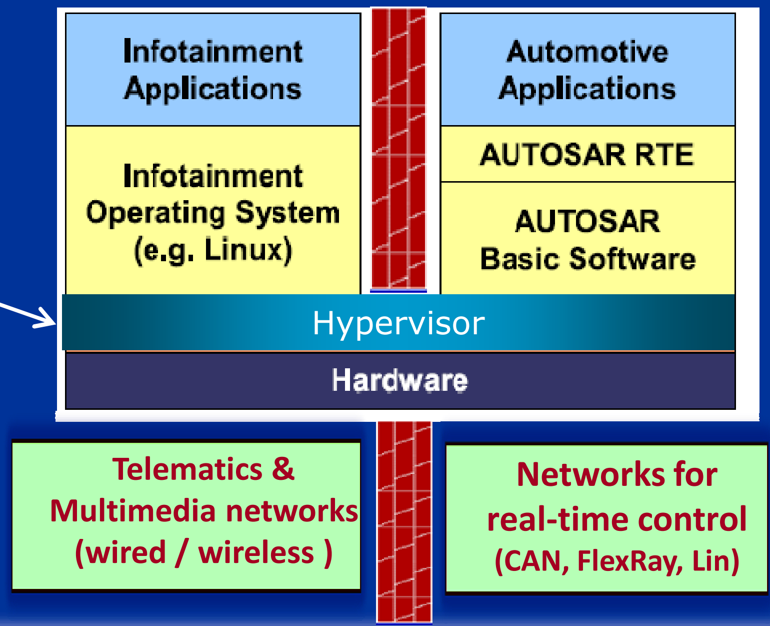


An “infected” vehicle may contaminate others.

Virtualization as a means to enforce security

- Example: Radio-player or Body Control Module with both an infotainment (eg., Linux, Android) and an Autosar Virtual Machine (VM)

Communication between VMs through the hypervisor "secure" mechanisms



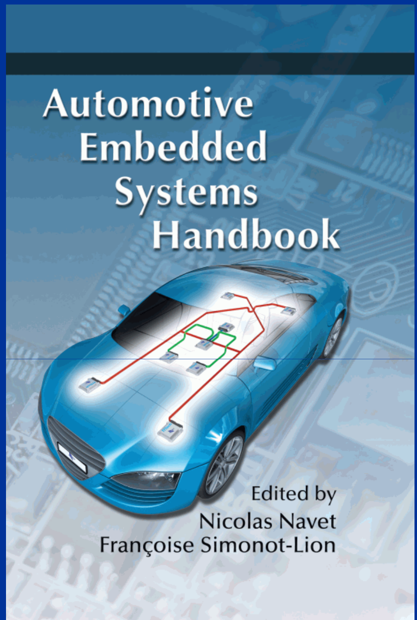
Benefits

- **Security despite open systems**
- Preserve segregation in "vehicle domains"
- Best of both worlds in terms of know-how, time-to-market
- etc

A likely use-case of virtualization – open questions: which technical solutions? role/business model among actors? change wrt aftermarket? etc

References

References



[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] RealTime-at-Work (RTaW), RTaW-Sim: a Fine-Grained Simulator of Controller Area Network with Fault-Injection Capabilities, freely available on RTaW web site: http://www.realtimeatwork.com, 2010.

[3] A. Avizienis, J.C. Laprie, B. Randell, "Dependability and its threat: a taxonomy", IFIP Congress Topical Sessions 2004.

[4] D. Khan, R. Bril, N. Navet, "Integrating Hardware Limitations in CAN Schedulability Analysis", WiP at the 8th IEEE International Workshop on Factory Communication Systems (WFCS 2010), Nancy, France, May 2010.

[5] D. Khan, N. Navet, B. Bavoux, J. Migge, "Aperiodic Traffic in Response Time Analyses with Adjustable Safety Level", IEEE ETFA2009, Mallorca, Spain, September 22-26, 2009.

[6] R. Davis, A. Burn, R. Bril, and J. Lukkien, "Controller Area Network (CAN) schedulability analysis: Refuted, revisited and revised", Real-Time Systems, vol. 35, pp. 239–272, 2007.

[7] M. D. Natale, "Evaluating message transmission times in Controller Area Networks without buffer preemption", in 8th Brazilian Workshop on Real-Time Systems, 2006.

[8] C. Braun, L. Havet, N. Navet, "NETCARBENCH: a benchmark for techniques and tools used in the design of automotive communication systems", Proc IFAC FeT 2007, Toulouse, France, November 7-9, 2007.

[9] R. Kaiser, D. Zöbel, "Quantitative Analysis and Systematic Parametrization of a Two-Level Real-Time Scheduler", paper and slides at IEEE ETFA'2009.

[10] P. Leteinturier, "Next Generation Powertrain Microcontrollers", International Automotive Electronics Congress, November 2007.

[11] K. Koscher et al, "Experimental Security Analysis of a Modern Automobile", IEEE Symposium on Security and Privacy, 2010.

[12] AUTOSAR, "Specification of Timing Extensions", Release 4.0 Rev 2, 2010.

Questions / feedback ?

Please get in touch at :
nicolas.navet@inria.fr