Safety evaluation of in-car real-time applications distributed on TDMA-based networks

Françoise Simonot-Lion

3rd Nancy-Saarbrücken Workshop on Logic, Proofs and Programs

Nancy, 13-14 October 2005

Safety evaluation of in-car real-time applications distributed on TDMA-based networks

PSA PEUGEOT CITROËN

Cédric Wilwert

Loria

Françoise Simonot-Lion, Ye-Qiong Song

Institut ELIE CARTAN

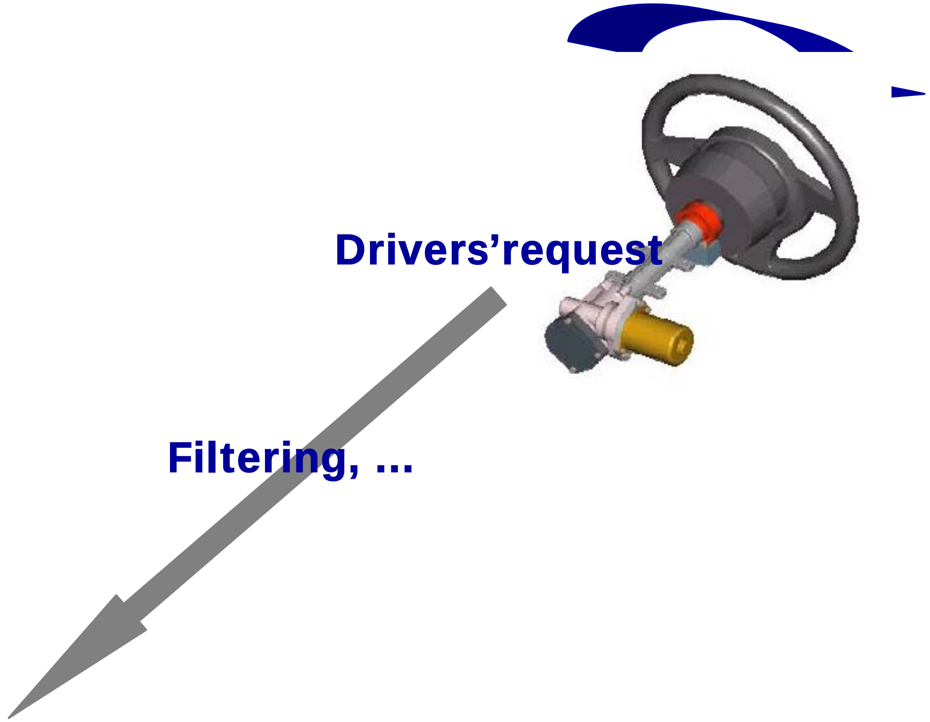
François Simonot

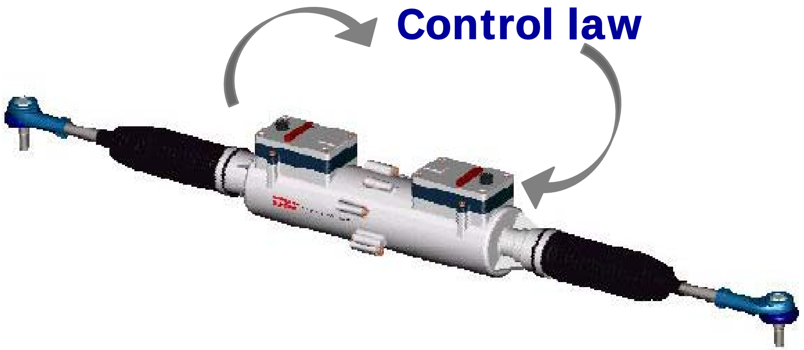
X-by-Wire and Safety assessment: which issue?

Steering system

Critical functions

- **Steering according to the drivers' request**
- ***Force feedback to the steering wheel***

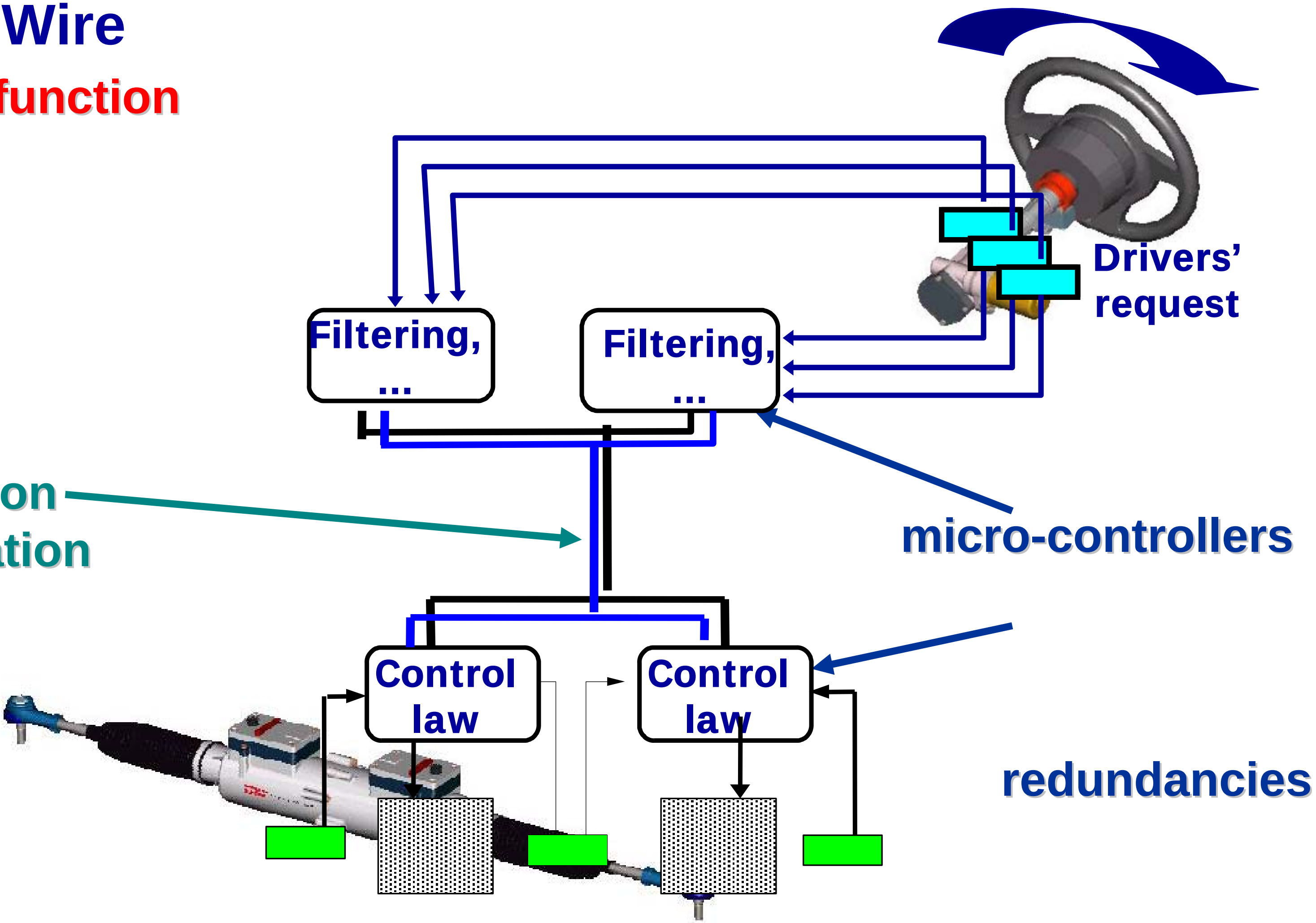




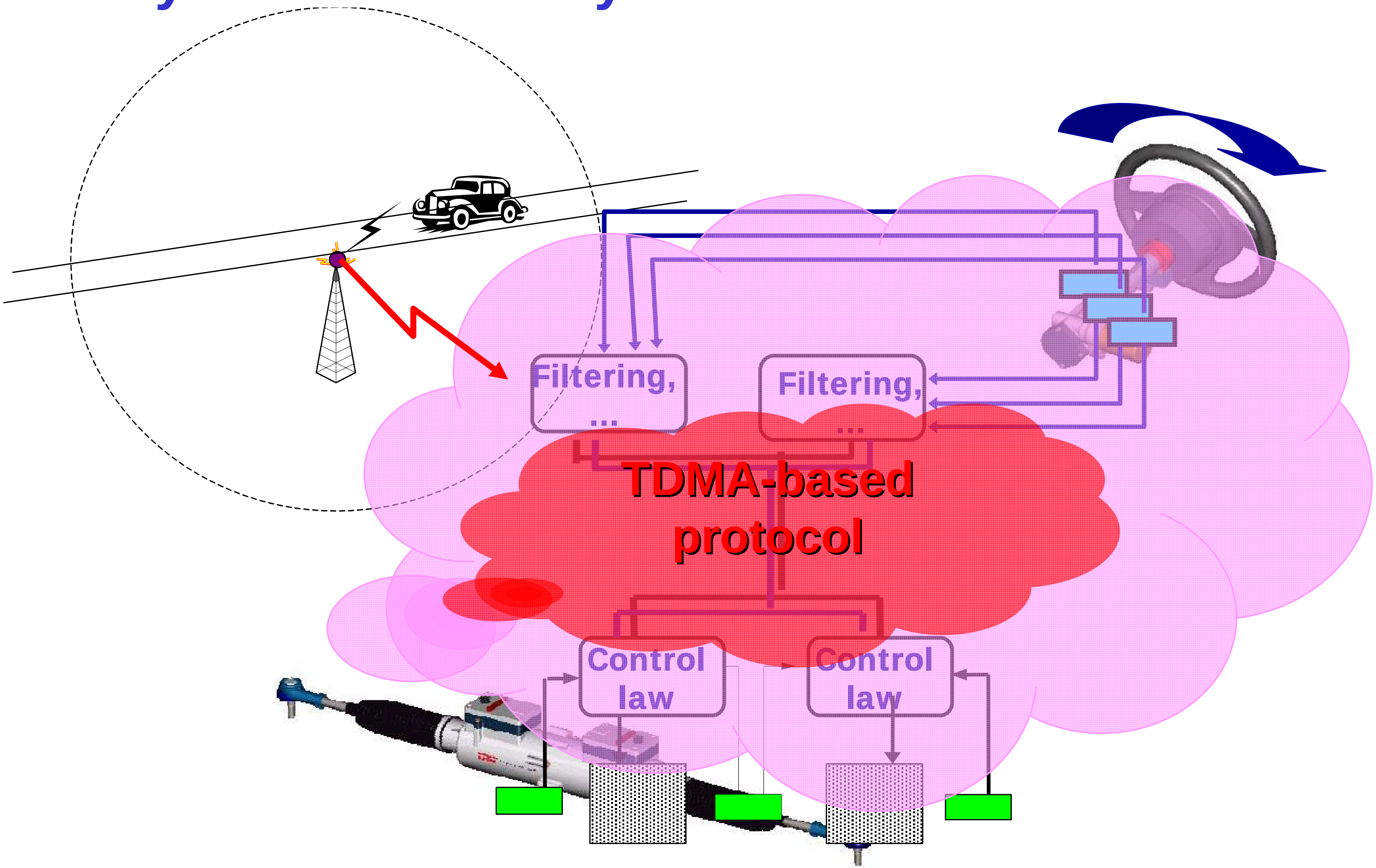
X-by-Wire and Safety assessment: which issue?

Steer-by-Wire

- **Steering function**

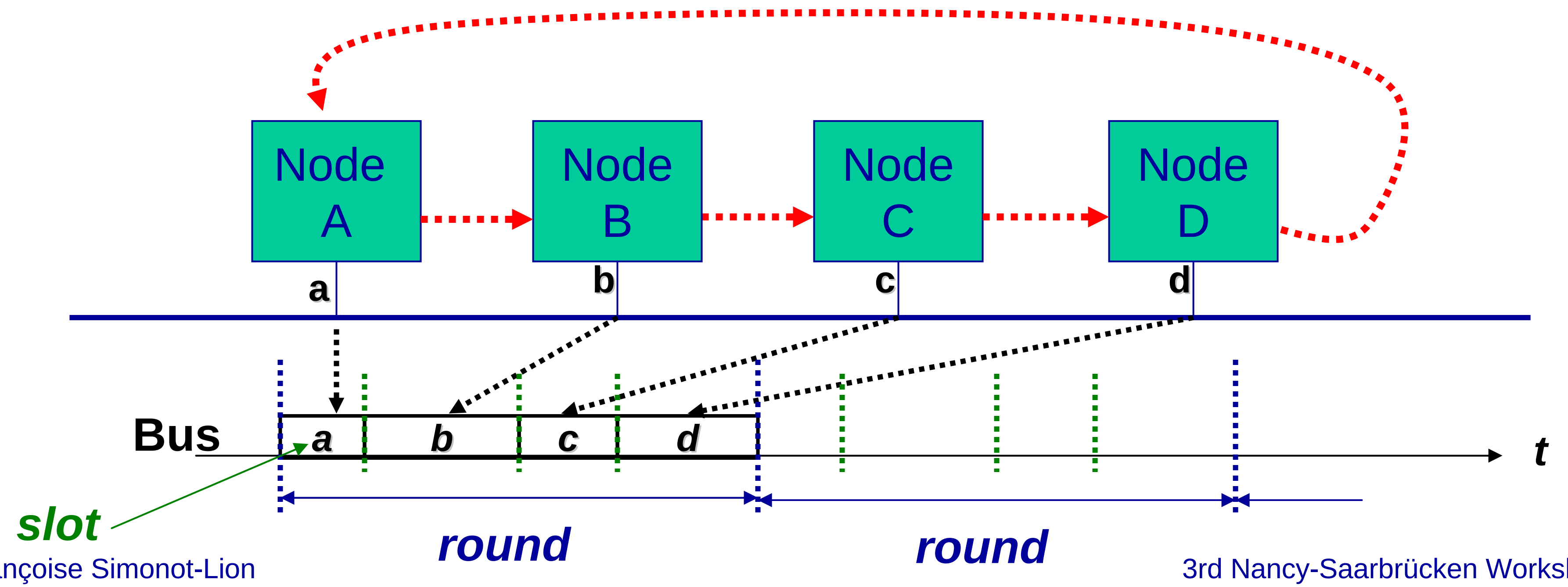


X-by-Wire and Safety assessment: which issue?



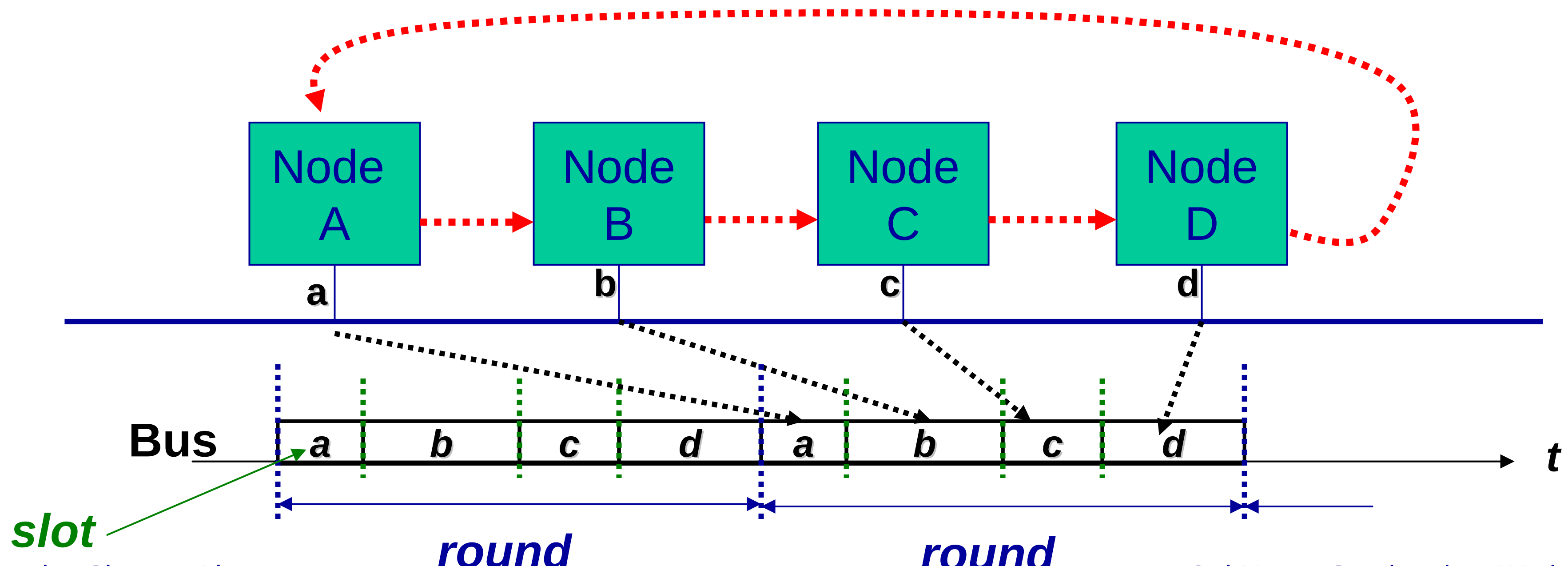
TDMA protocol (*Time Division Multiplexed Access*) TTP/C

- **Slot: time interval for a node to send a message (frame)**
- **Round (cycle): a sequence of slots such as each node sends one and only one time (TTP/C)**



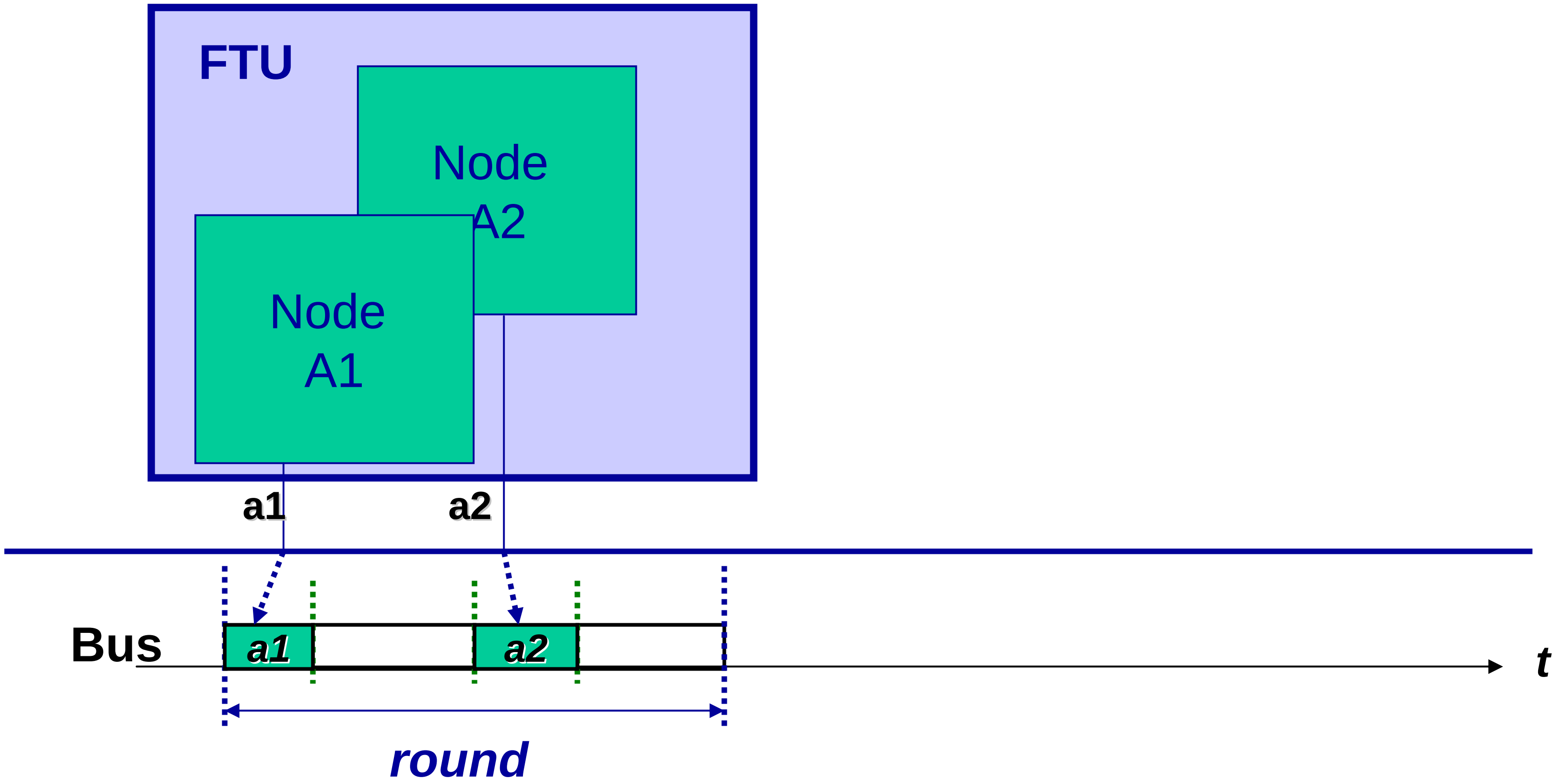
TDMA protocol (*Time Division Multiplexed Access*) TTP/C

- **Slot: time interval for a node to emit a message (frame)**
- **Round: a sequence of slots such as each node emit one and only one time (TTP/C)**

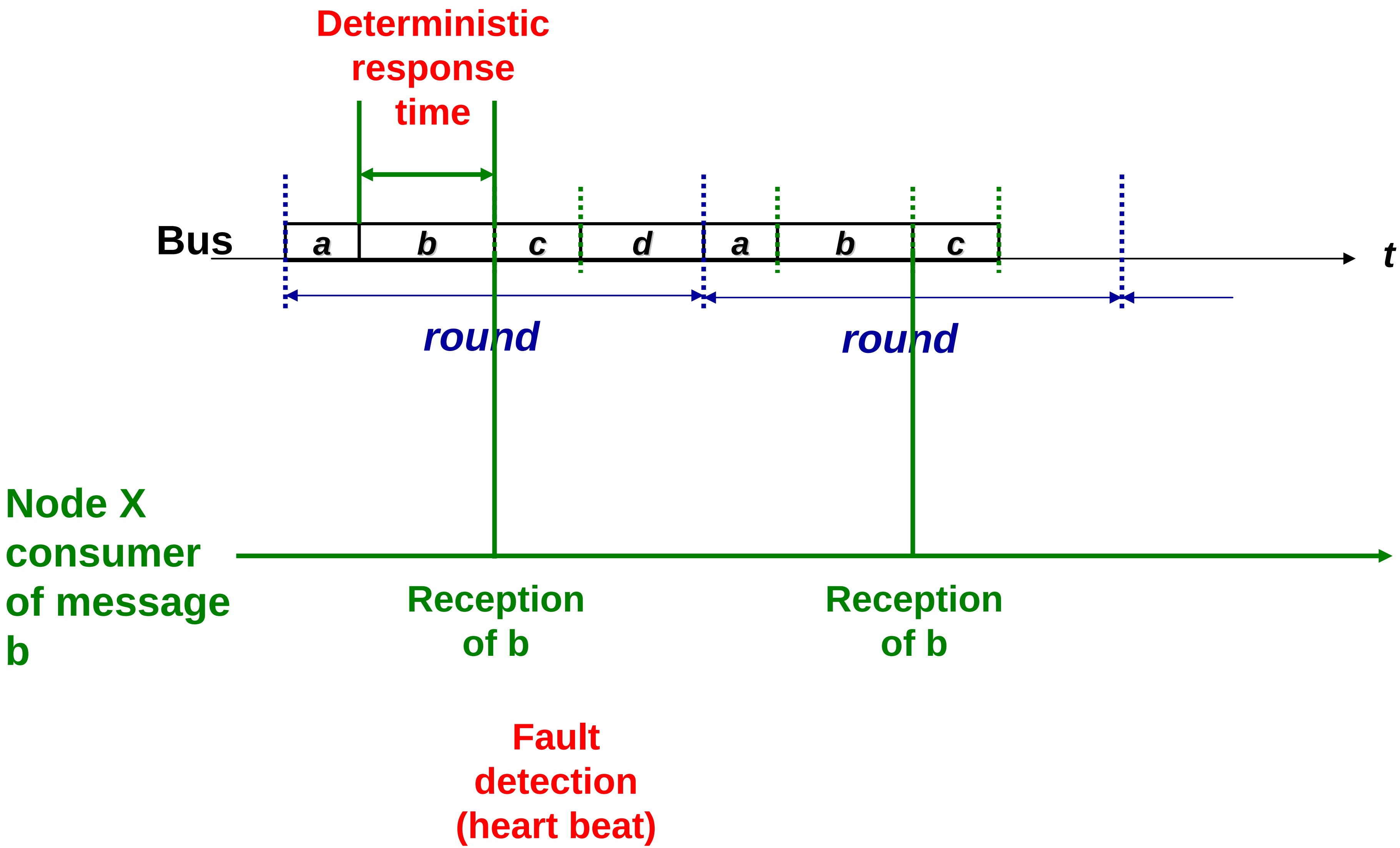


TDMA protocol - Fault Tolerant Unit (FTU)

- **FTU: redundant nodes**
  - **perform identical computations**
  - **message redundancy in each TDMA round**

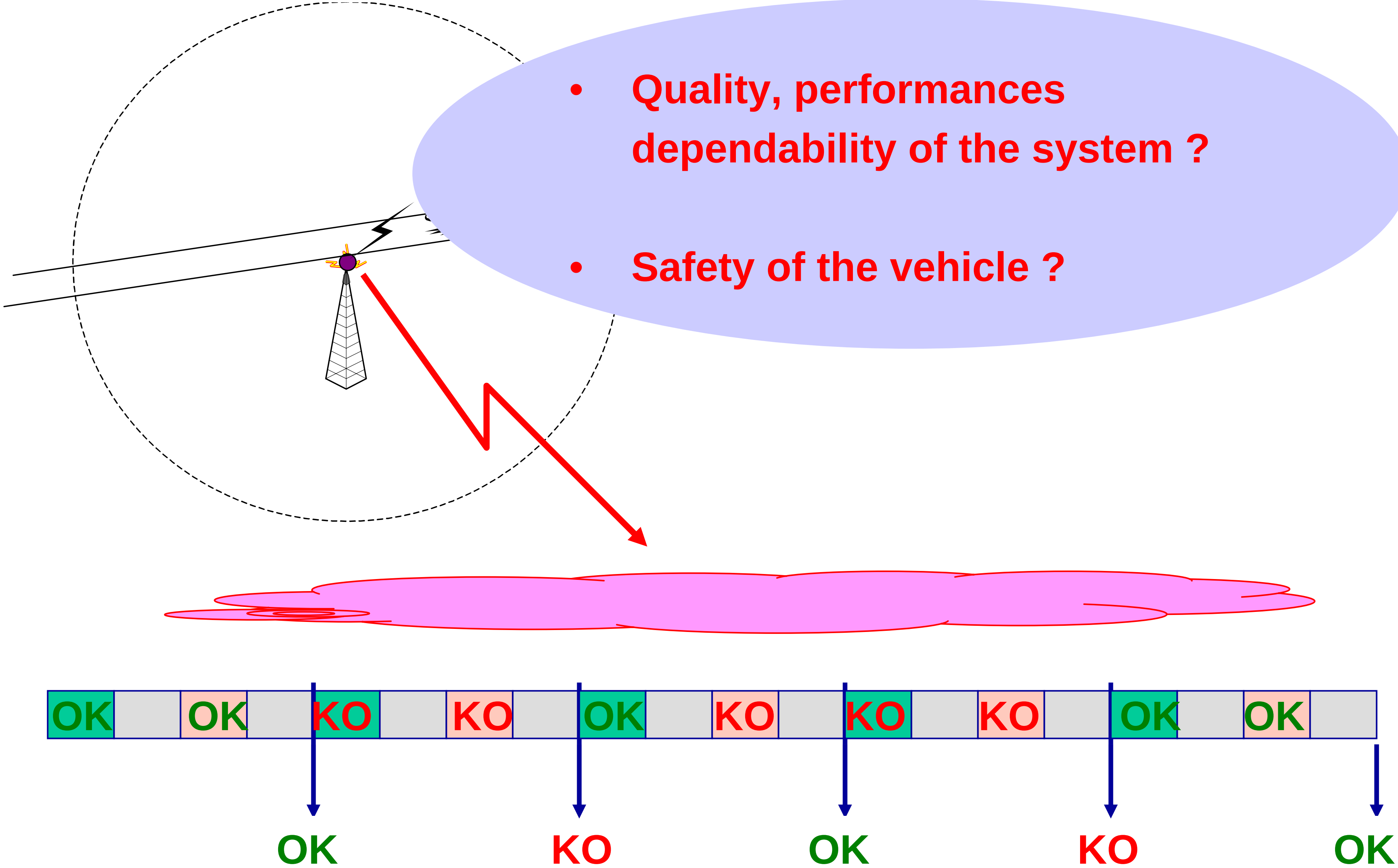


TDMA protocol for X-by-Wire systems



Impact of EMI perturbation on a TDMA-based communication system

- Quality, performances dependability of the system ?
- Safety of the vehicle ?



Standard and Certification

A Steer-by-Wire system is a Safety Critical System

Regulatory laws → Certification and standard

Quantitative evaluation of the safety

Probability to have a *critical* failure in one hour $< 10^{-10}$
(IEC 61508 / SIL4)
Industrial requirement

Verification on an Operational Architecture?

-Mechanical / hydraulical components - architectures

-Electronic devices

- ???? Behavior of software architecture (tasks, messages)

A contribution to the safety assement of X-by-Wire systems

- **Quantitative evaluation of a failure probability**
  - **extreme situation for the vehicle (worst case)**
  - **focus on the communication and EMI perturbations**
    - **TDMA-based protocol**
    - **Granularity: one TDMA cycle**
  - **transient faults (EMI perturbations): from transient faults to vehicle failure**
  - **metric and means for safety evaluation**

Outline

Introduction

☞ **Key points for the safety assessment of X-by-Wire system**

Technical solutions

Case study

Conclusions

Leading angles of the method

- **Robustness of the control law**
- **System *possibly* perturbated**
  - **How?**
  - **How long?**

Robustness of the control law

- **Control law used as a black box**

- **Matlab / Simulink model**
  - **of the vehicle (SimulinkCar – PSA Peugeot-Citroën)**
  - **of the control law**

  for an « extreme » situation of the vehicle (worst case)

Fault injection + Simulations → 2 results

- **Acceptable length of the TDMA cycle**
- **Maximal number of consecutive lost TDMA cycles - η_{max}**

How is a TDMA cycle affected by a perturbation?

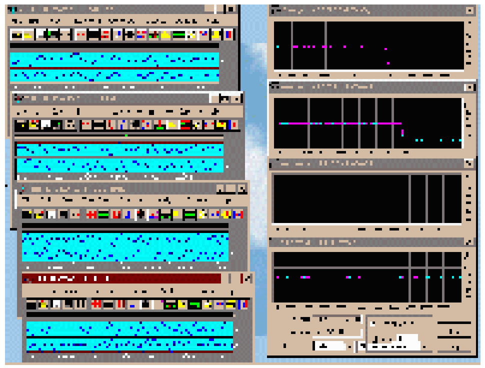
- **Error model**
  - **Obtained by measurement**
  - **Know-how of PSA Peugeot-Citroën**

➔result

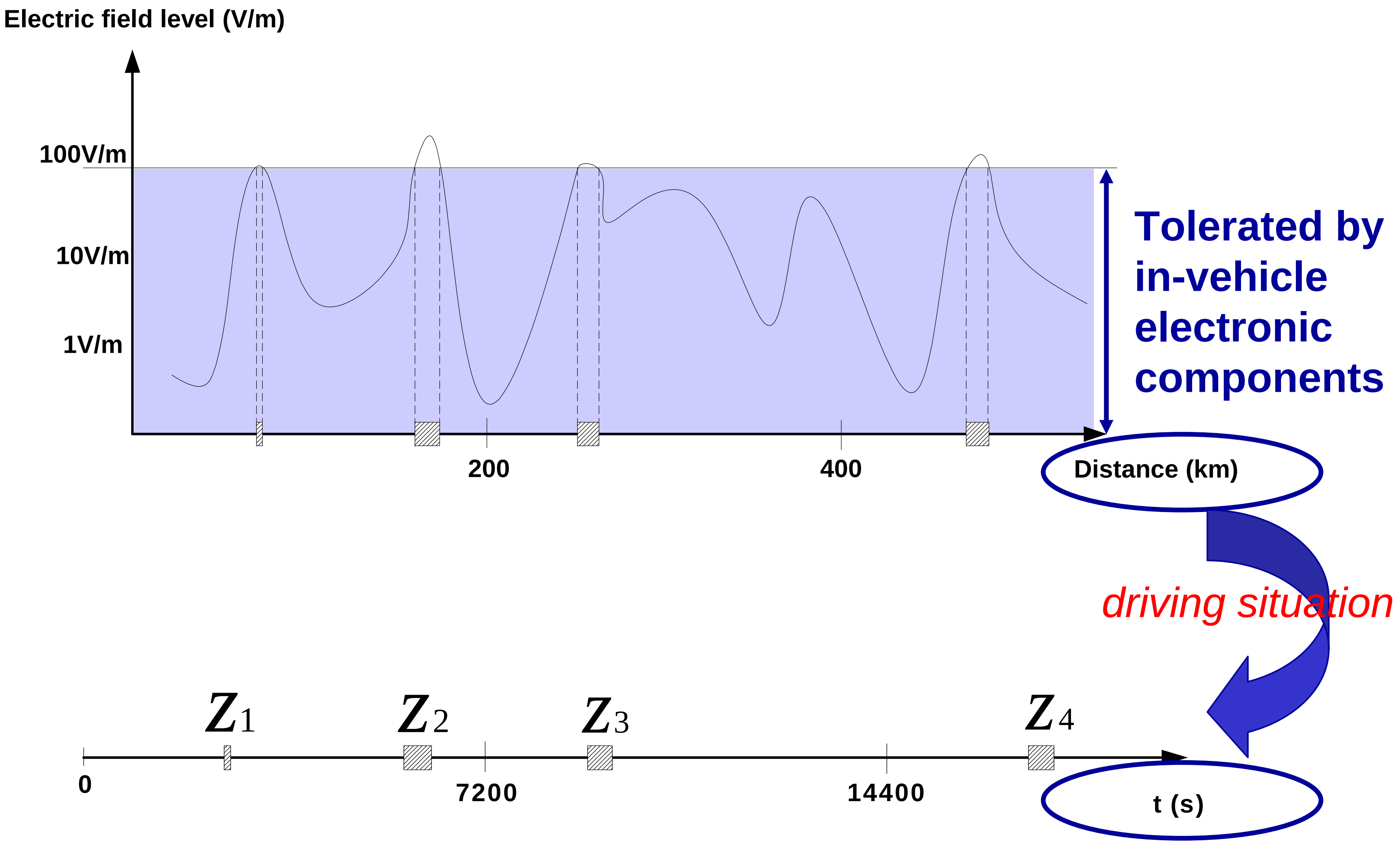
P_{err}, probability for a TDMA cycle to be *fully corrupted* when the network is submitted to a perturbation

How long is a perturbation?

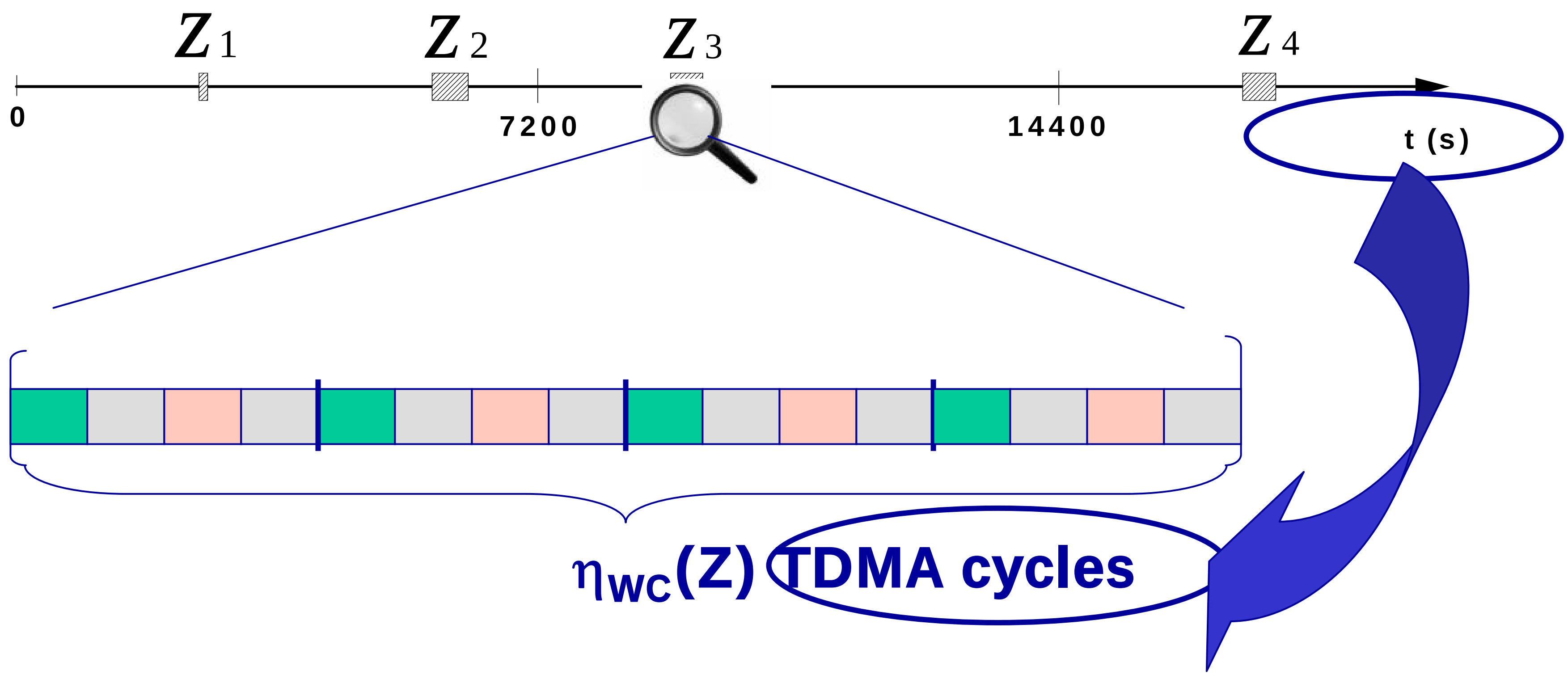
- **Electric field level of a reference road**
  - **Based on the results of a French project**
  - **Measured on board**
  - *Assuming a tolerance level of embedded electronic components*



How long is a perturbation?



How long is a perturbation?



$$\eta_{wc} = \left\lceil \frac{\text{zone duration}}{\text{TDMA cycle}} \right\rceil + 2 \text{ , (worst case)}$$

Outline

Problem

Key points for the safety assessment of X-by-Wire system

☞ **Technical solutions**

Case study

Conclusions

Technical solutions

- **Given:**
  - η_{max} **: tolerance (consecutive corrupted TDMA cycles)**
  - η_{wc} **: length of the perturbation (TDMA cycles) - extreme situation for the vehicle, worst case of perturbation cover**
  - P_{err}**: probability for one TDMA cycle to be corrupted**

- **Problem:**

  determine the probability to have more than η_{max} consecutive corrupted cycles in η_{wc} cycles (under P_{err}):

$$P_{fail}(\eta_{max}, \eta_{WC}, P_{err})$$

Technical solutions

- **Similar to « consecutive-k-out-of-n:F » systems - C(k,n:F)**
  - **System = ordered sequence of n components**
  - **The system fails if and only if more than k consecutive components fail**
  - ***L_n: number of consecutive failed components***

$$P(L_n < k) = R(k,n;p)$$

[Burr,1961], [Lambridis,1985], [Hwang,1986]

$$R(n,k;p) = \sum_{m=0}^{\lfloor (n+1)/(k+1) \rfloor} (-1)^m p^{mk} q^{m-1} \left(\binom{m-k}{m-1} + q \binom{n-mk}{m} \right)$$

$$\text{with } q = 1 - p$$

Technical solution

- **Recurrent relation:**

$$u_k(x+1) = u_k(x) - qp^k u_k(n-k) \text{ for } x \geq k$$

$$u_k(x) = 1 \text{ for } 0 \leq x \leq k-1$$

$$u_k(k) = 1 - p^k$$

$n \geq 3$ and $p \in]0,1[$

$$u_k(n) = R(k,n;p)$$

$$P_{fail}(\eta_{max}, \eta_{WC}, P_{err}) = 1 - R(\eta_{max}, \eta_{WC}; P_{err}) = 1 - u_{\eta_{max}}(\eta_{WC})$$

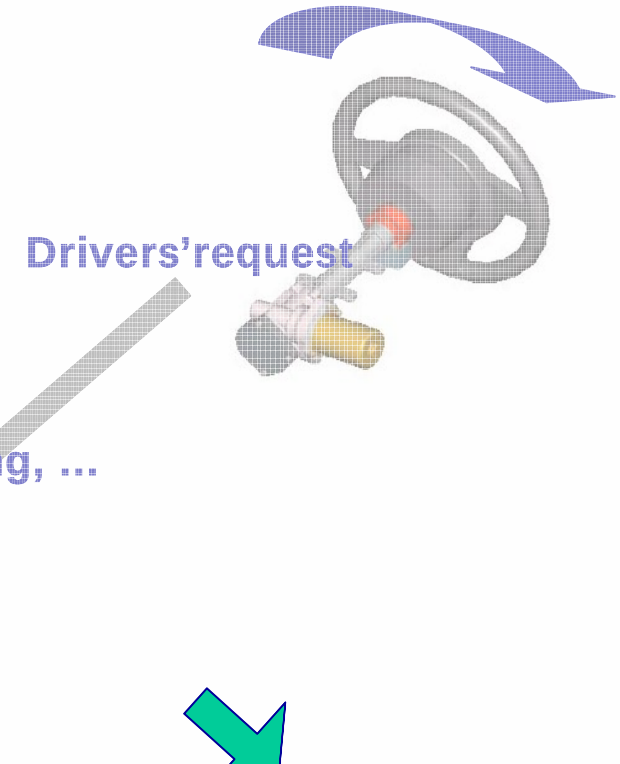
Outline

- Problem
- Key points for the safety assessment of X-by-Wire system
- Technical solutions
- ☞ **Case study**
- Conclusions

Case study: a Steer-by-Wire system

-extreme situation

vehicle speed (90 km/h)
sharp turning
perturbated area = 2s



-robustness

η_{max} **= 7 TDMA cycles**

-impact of the EMI perturbation

$P_{err} = 5\ 10^{-3}$

-duration of the possibly perturbated area

η_{WC} **= 336 TDMA cycles**

$$P_{fail}(\eta_{max}, \eta_{WC}, P_{err}) = 2.87\ 10^{-8}$$

Case study: configuration of a system

$P_{fail}(\eta_{WC}, \eta_{WC}, P_{err}) < 10^{-10}$

$\ldots\eta_{WC}, \eta_{WC}, P_{err}) < 10^{-7}$

TDMA cycle (ms) ➔ (η_{WC}, …max)

P_{err}

	1	2	3	4	5			8	9	10
0,5										
0,4										
0,3										
0,2										
0,1										
0,09										
0,08										
0,07										
0,06										
0,05										
0,04										
0,03										
0,02										
0,01										
0,009										
0,008										
0,007										
0,006										
0,005										
0,004										
0,003										
0,002										
0,001										

Outline

Problem

Key points for the safety assessment of X-by-Wire system

Technical solutions

Case study

☞ **Conclusions**

Conclusions

- **A contribution to the dependability evaluation of an embedded system**
  - Transient fault at communication level to safety property at vehicle level
  - Mathematical evaluation / simulation

- **Generalisation**
  - P_{err} variable (error pattern, Markov process)
  - Other systems (e.g., dependability for application based on wireless networks)