

# CEDES

Cost Efficient Dependable Electronic Systems



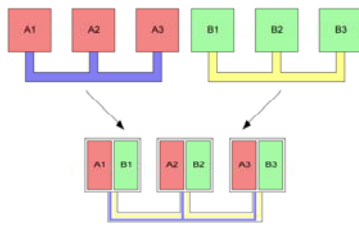
## Technical implementation of a FlexRay system



- From federated to integrated systems
- Byzantine failures - Why we need to tackle this?
- Ongoing research in CEDES - Putting it together
  
- Overview of FlexRay
- Implementation experiences of a FlexRay Cluster

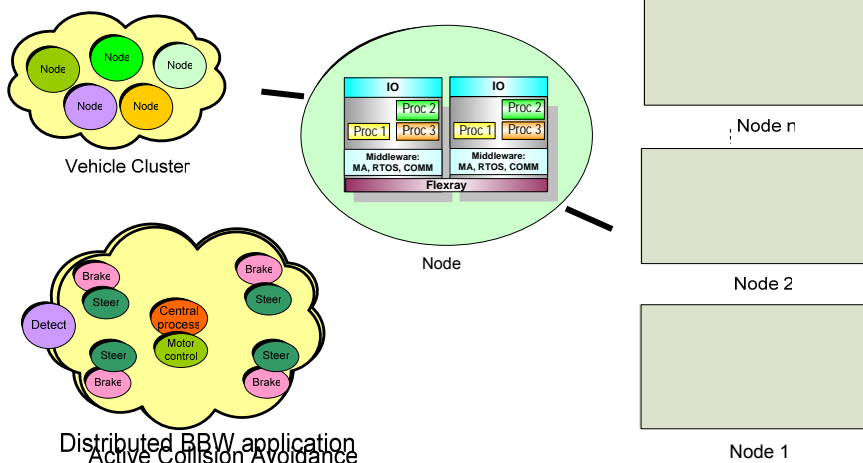
## Federated to Integrated Architecture

- From loosely to tightly coupled
- Federated architecture
  - ▶ + Inherent simplicity, fault containment
  - ▶ - Independent subsystem per function
  - ▶ - Difficult to co-ordinate functions



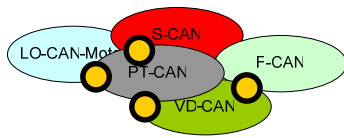
- New approach needed to enable “advanced functions”
  - ▶ Coming innovations will be software based....
- Share resources and maintain high integrity
- Integrated architecture
  - ▶ + Enables higher functionality
  - ▶ - Cost?

## Future Automotive Electrical Architecture

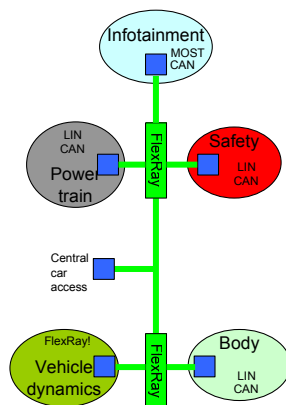


## Current Automotive Architecture?

- Federated design
  - ▶ Loosely coupled
- Four gateways and five CAN
  - ▶ Waste of bandwidth due to overlapping
  - ▶ Unacceptable delays
  - ▶ Cost and complexity
- Busload close to max at SOP
  - ▶ No reserve for future functions
  - ▶ Non deterministic behaviour at high bus load

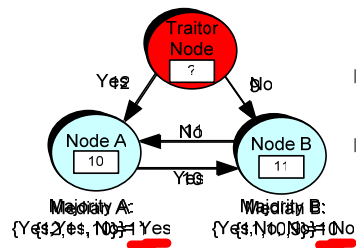


## Bright Outlook (with FlexRay)



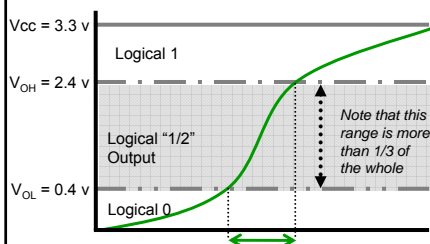
- Roadmap (BMW)
  - ▶ 2006: Pilot application - FlexRay in EDC
  - ▶ 2010: FlexRay as a Backbone
- Architectural flexibility through scalability and functional alternatives
  - ▶ Concerns network architecture only....

## Byzantine Faults I



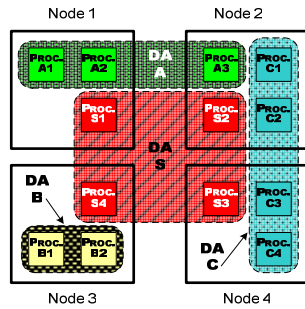
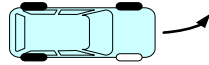
- Well established in theories, now in reality!
  - ▶ Byzantine Generals Problem
  - ▶ Traitor with arbitrary behaviour
- Must have consensus among correct nodes
- Must be aware of this in safety-critical systems
  - ▶ Fault avoidance - design
  - ▶ Fault tolerance - redundancy

## Byzantine Faults II



- Root: different receivers have different interpretations of:
  - ▶ logic level
  - ▶ arrival time of message
- BGP in “space” and time
- No such thing as “digital circuitry”
- Only analogue circuitry driven to extremes
  - ▶ Possibility of a “1/2”
  - ▶ E.g. floating CMOS logic

## Research within CEDES



- Membership for distributed applications
  - ▶ Which proc. is live and which is not?
- Partitioned systems
  - ▶ Applications share platform (ECU)
  - ▶ What hardware support is required?
- Assume that transient errors are common
  - ▶ Fault model
- Thanks to Time-Triggered communication!

## Agenda

- From federated to integrated systems
- Byzantine failures - Why we need to tackle this?
- Putting it together - Ongoing research in CEDES
- ➔ ■ Overview of FlexRay
- Implementation experiences of a FlexRay Cluster