Membership Agreement in Time-triggered Systems

Johan Karlsson

Department of Computer Science and Engineering
Chalmers University of Technology
Göteborg, Sweden

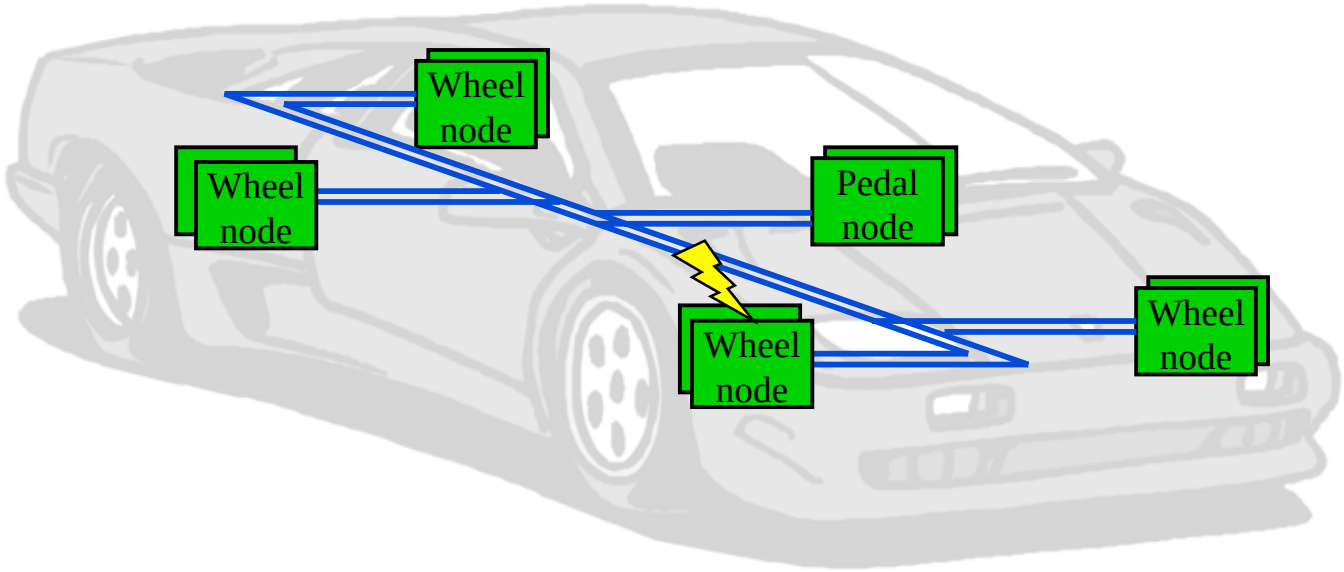
www.ce.chalmers.se/~johan

CHALMERS

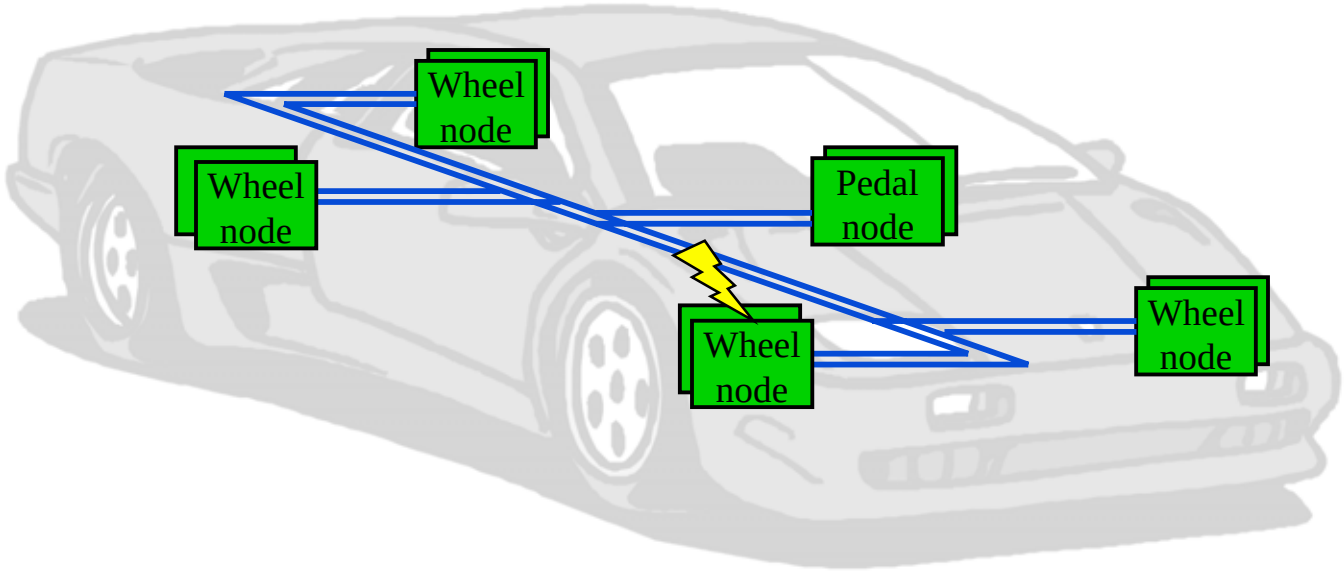
Outline

- Brake-by-wire example
- System design principles
- Design alternatives for membership protocols

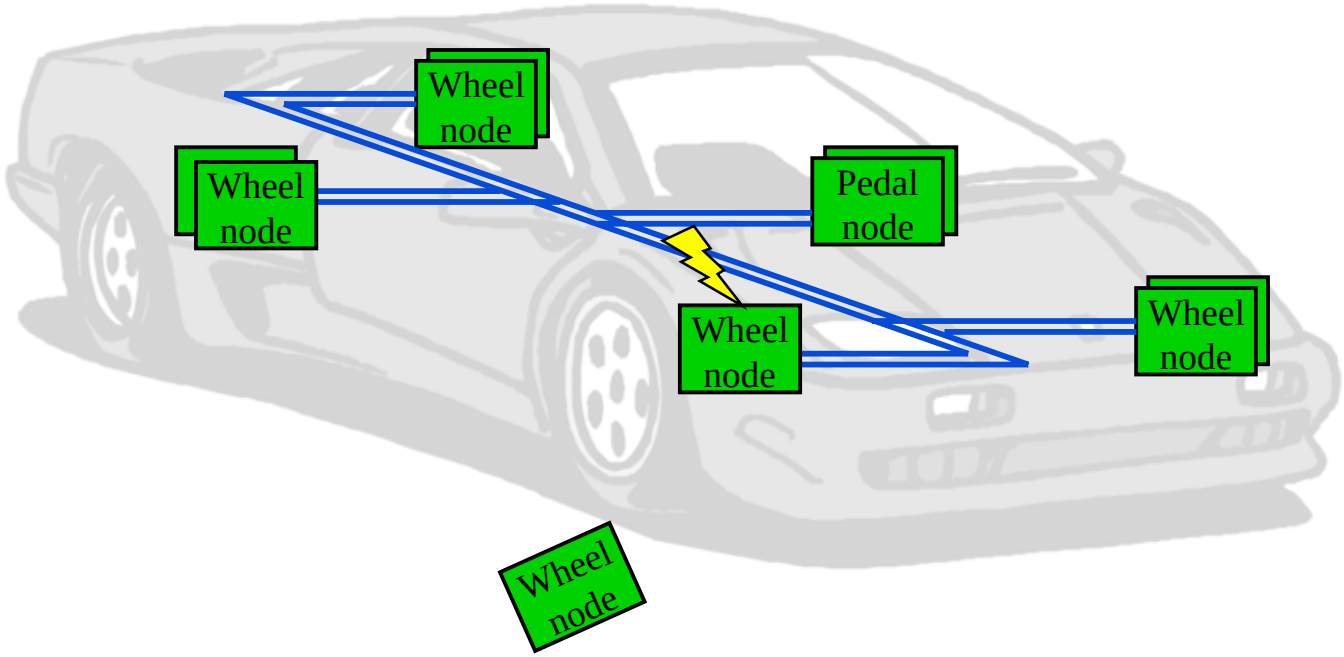
Brake-by-wire system



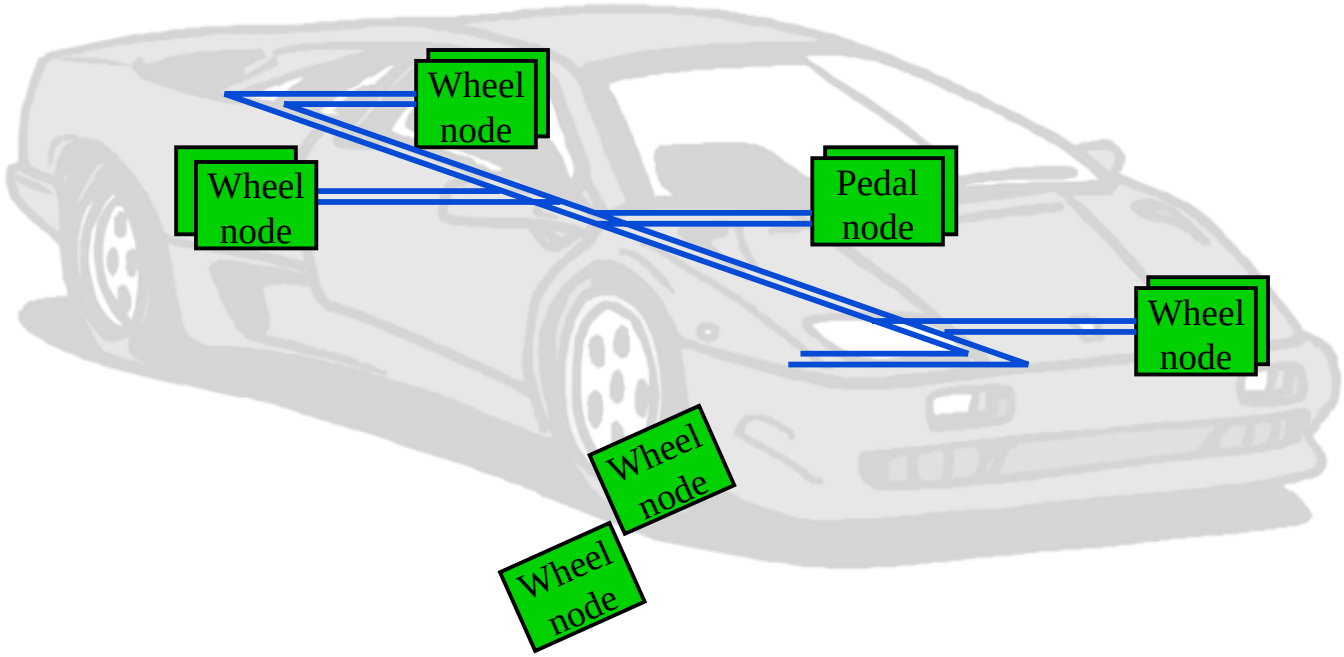
Brake-by-wire system



Brake-by-wire system



Brake-by-wire system



Core Design Principles

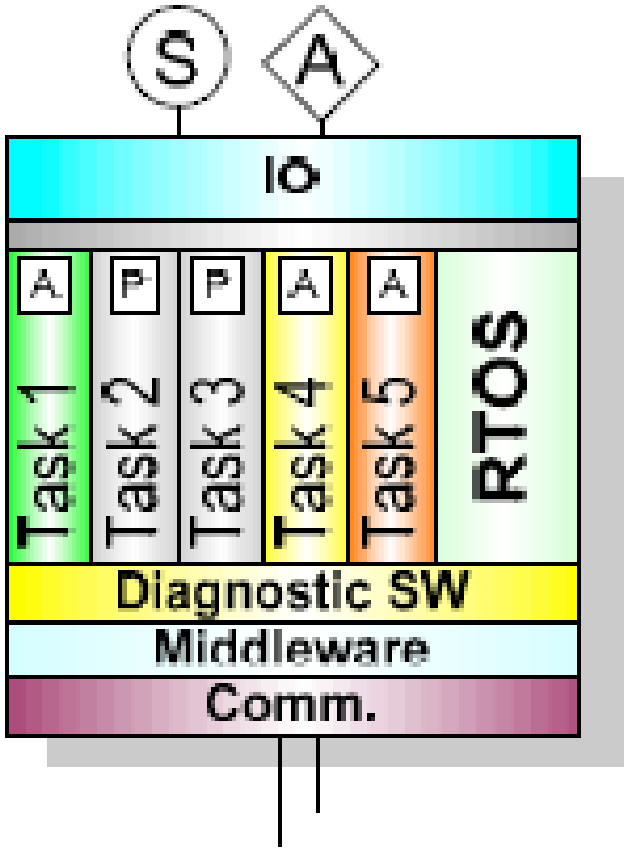
- Time-triggered communication
  - FlexRay (10 Mbit/s) – For automotive
  - Time-triggered Ethernet (100 Mbit/s) – For avionics
- Multi-level fault-tolerance
  - System-level
    - Duplication of nodes and communication channels
  - Node-level
    - exceptions, assertions, temporal error masking, application specific recovery, …

Architectural Issues

- Component-based software architecture
  - Based on AUTOSAR, ARINC 653
  - Support for composability, incremental validation/certification, …
    => time-triggered scheduling of tasks and data communication

- System partitioning
  - Application software layer
  - Core software layer
  - Isolation between application tasks and between core/applications
    - Microcontrollers with memory management unit (MPC 5554)
    - OS with support for MMU (Extension of MicroC OS)

Node structure



Problem

- How do we design a reliable membership service with low latency for the core software layer?

Failure Assumptions

- Smallest unit of failure = task (application component)
- Node failure modes
  - Fail-reporting (application failure)
  - Fail-silent (core failure)
- Communication failures
  - Incoming/Outgoing link failures
  - Symmetrical failure
    - All nodes receive an incorrect message and detect that the message is incorrect.
  - Asymmetrical failure
    - Some nodes receive a message correctly while other nodes receive the same message incorrectly.

Design alternatives

- Consensus-based protocol
  - All non-faulty nodes communicate their view of previously sent messages.
  - Based on the views communicated, each node execute an decision algorithm.
- Sponsor-based protocol
  - A sponsor is node that acknowledge a message send by another node (positively or negatively)
  - There are only a few (say two or three) nodes that acknowledge each message.

Questions/Comments?

Ideal place for a *Real* Winter Meeting?

The Ice Hotel, Jukkasjärvi, Sweden

Change of state suit 300 - 2006

Suit 300 M.C. Escher - 2006

CHALMERS

Ice church

The Northern Lights – Aurora Borealis

- Very beautiful,
- But also a Sinister Source of Computer Failures!

More pictures at www.icehotel.com/Winter

Thank You!