

DAIMLERCHRYSLER

Concept and Integration of an Agreement Protocol in a Dependable Software Platform for Automotive Integrated Safety Systems

Automotive – Safety & Security 2006

Dipl.-Ing. Xi Chen, M. Sc., DaimlerChrysler AG

Dipl.-Inf. Mourad Limam, IAS, Universität Stuttgart

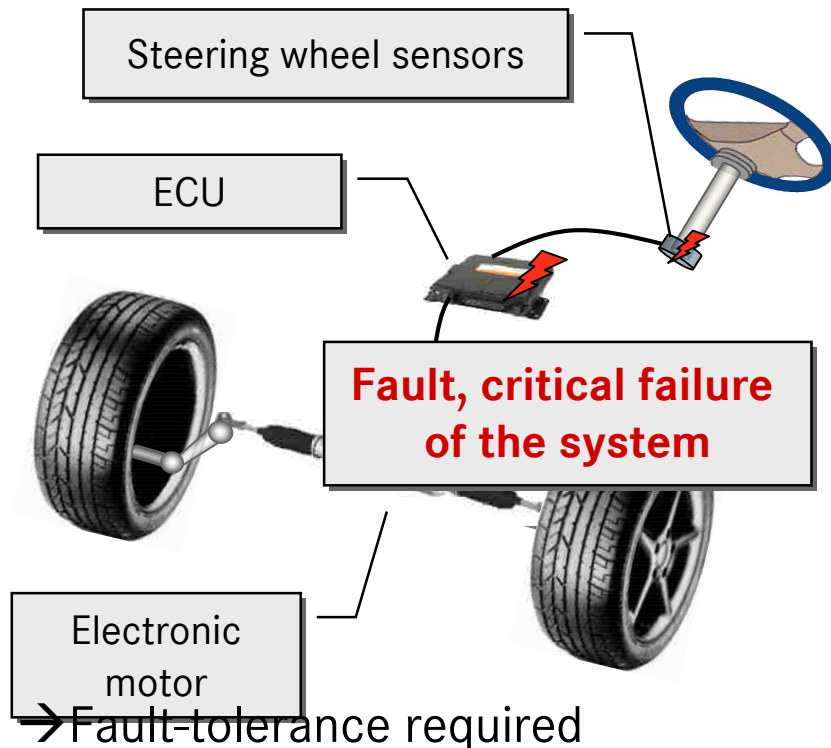
Dipl.-Ing. Michael Wedel, IAS, Universität Stuttgart

Prof. Dr.-Ing. Dr. h. c. Peter Göhner, IAS, Universität Stuttgart

Dr.-Ing. Vera Lauer, DaimlerChrysler AG

Motivation

Increasing number of in-vehicle safety E/E functions with new challenges of dependability

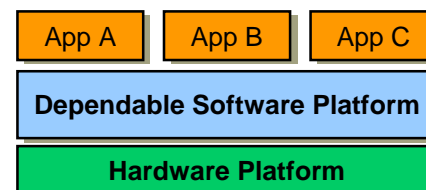


Conception of a modular architecture for fault-tolerance/dependability services

- Increasing variety of models
→ Avoid redevelopment, platform



- Integration of dependability software services in a platform
→ Managing the complexity, improvement of software quality



Contents

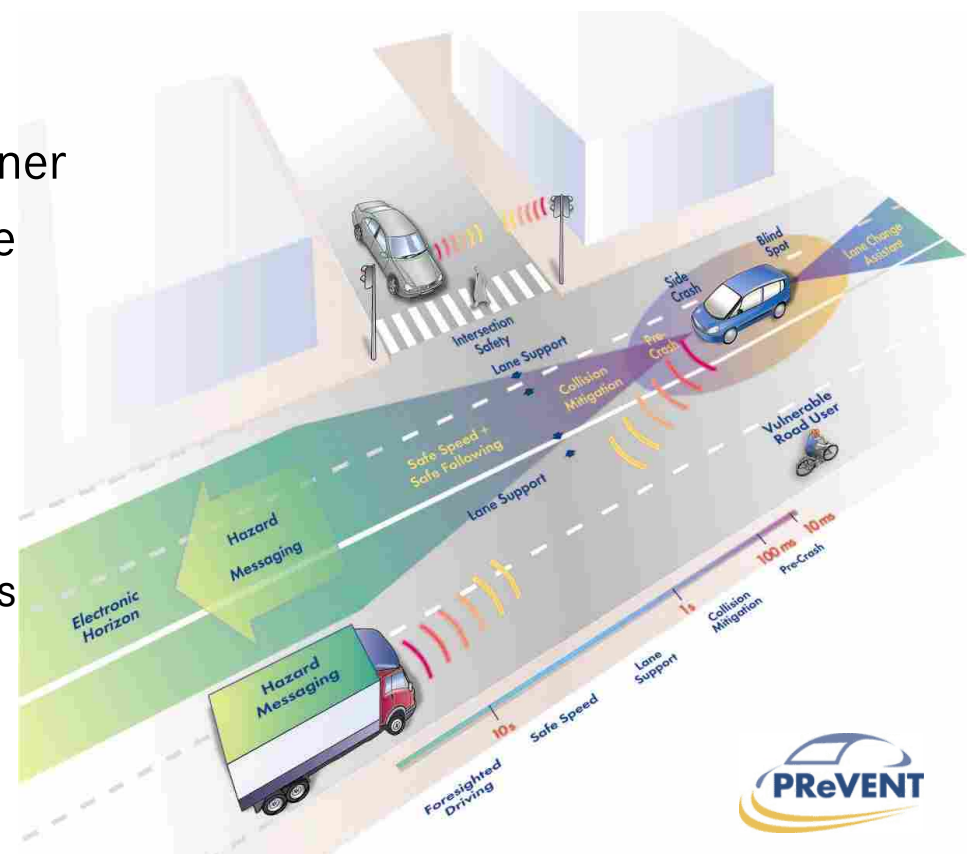
- Motivation
- **Overview of In-vehicle Electronics and Introduction to Integrated Safety Systems**
- Agreement Protocol - Reaching Consensus among Distributed Nodes
- Development of Agreement Protocol Service in EASIS
- Integration and Validation in the EASIS Validator
- Conclusion and Outlook

Overview of in-vehicle electronics

- 90% of the innovations in modern vehicles are driven by electronics/electrics (E/E) and software
- Increasing number of functions implemented with E/E with the requirements for safety and comfort from customer
- Rising Complexity with high number of networked Electronic Control Units (Maybach 77 ECUs)
- Increasing model variants from Cabrio, SUV to VAN

Integrated Safety Systems (ISS)

- Integration of safety applications from active and passive systems and other vehicle domains in a coordinated manner
- Composition of functions that enhance the level of safety for
 - passengers
 - environment, e. g. pedestrians
- ISS applications
 - are distributed over in-vehicle domains and networks borders
 - consist of functions with different safety integrity levels
 - make use of components that are not safety-critical themselves

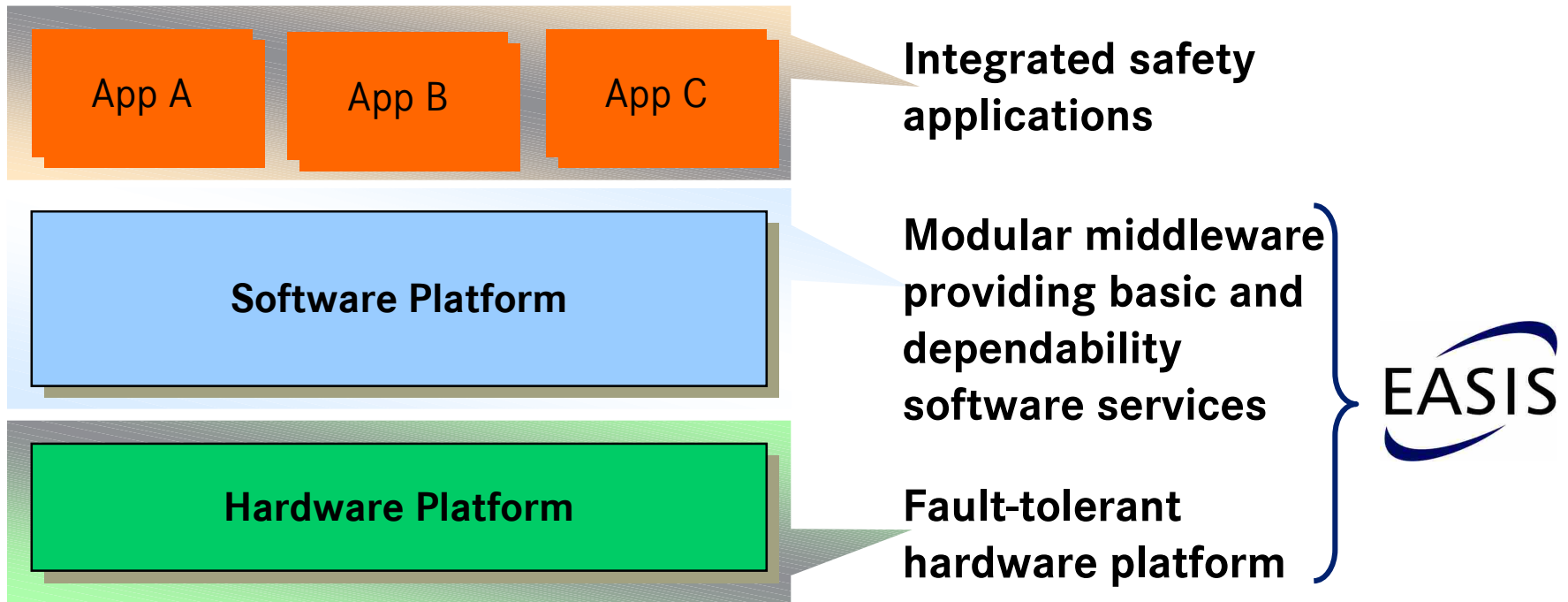


EU-Project EASIS

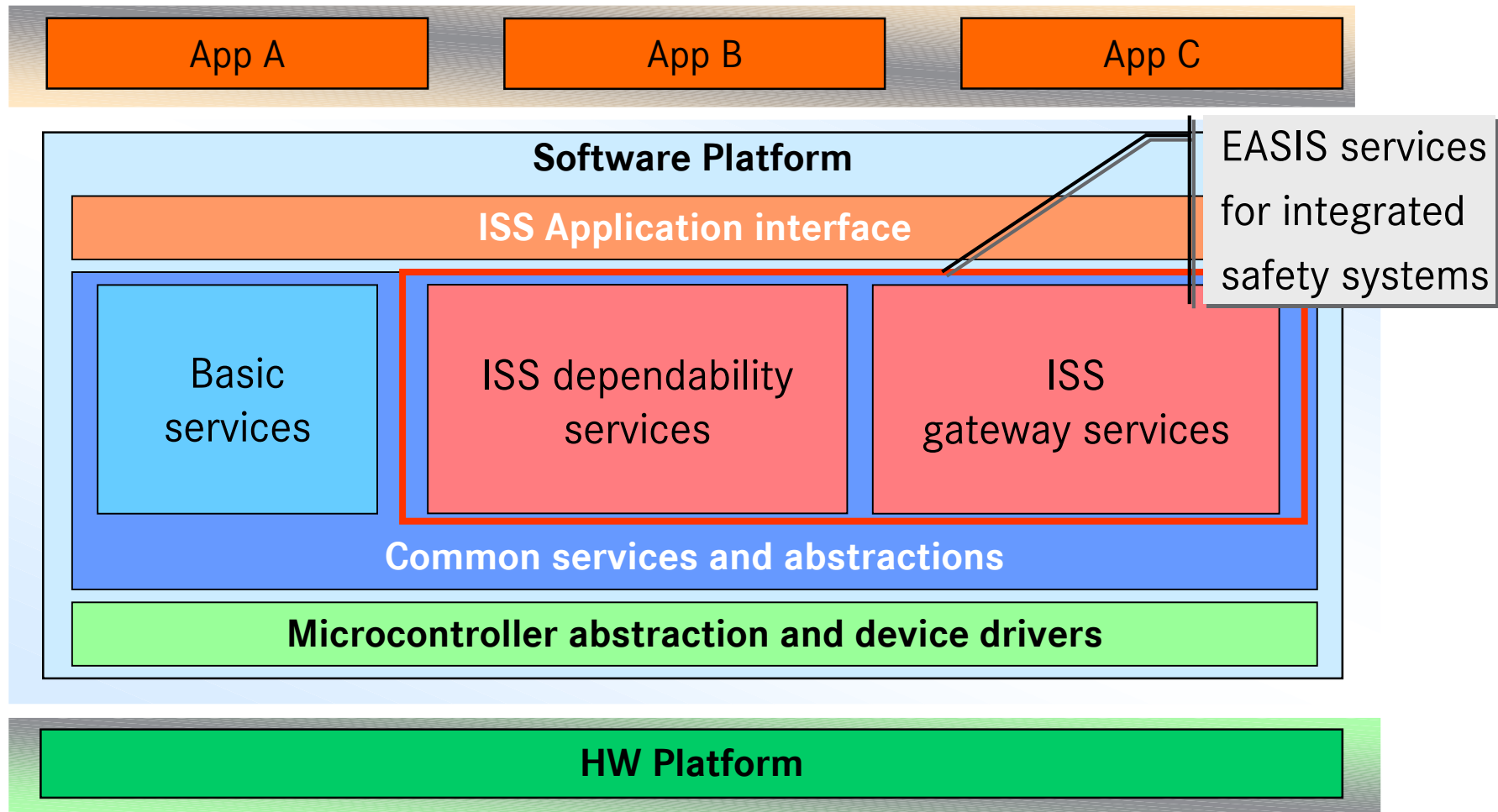


- **Electronic Architecture and System Engineering for Integrated Safety Systems**
 - As an industry consortium launched in 2004
 - cooperation between car manufacturers, suppliers and tool-providers
- **Aim:** Design of a standardized E/E-architecture for ISS
 - independent from OEMs and suppliers
 - defines software, hardware, development process and tool chains

Overview of EASIS Electronic Architecture



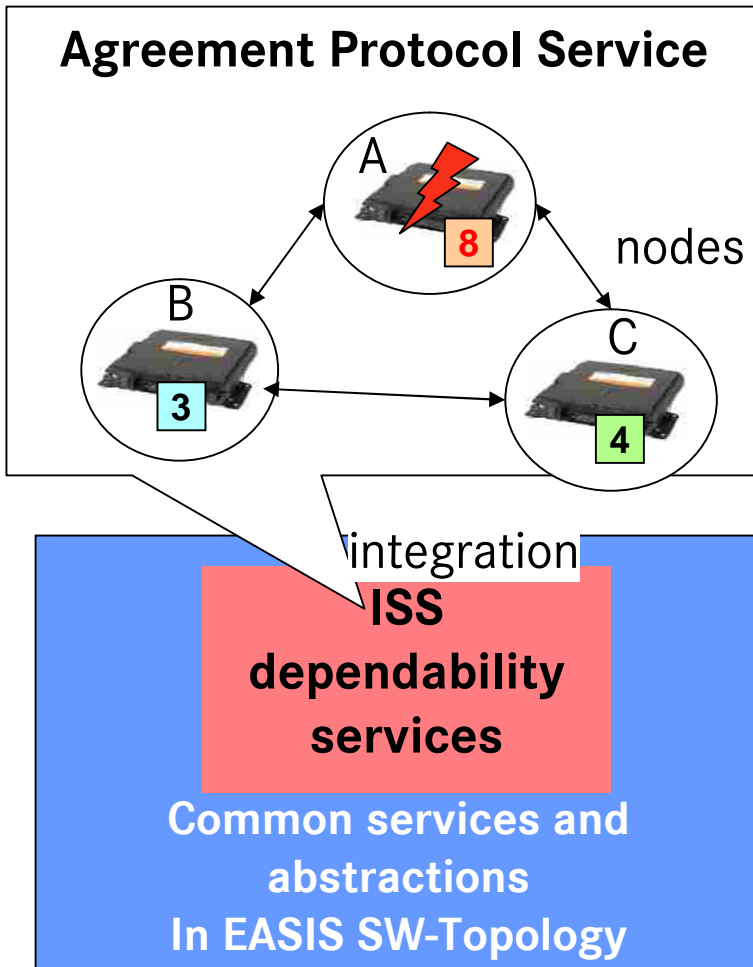
EASIS Dependable software platform



Contents

- Motivation
- Overview of In-vehicle Electronics and Introduction to Integrated Safety Systems
- **Agreement Protocol - Reaching Consensus among Distributed Nodes**
- Development of Agreement Protocol Service in EASIS
- Integration and Validation in the EASIS Validator
- Conclusion and Outlook

Agreement in Distributed Nodes



- Distribution of ISS-applications among different nodes
 - distributed topologies because of historical reasons
 - avoidance of single point of failure by redundancy
 - coordinated behavior of safety actions
 - nodes have to reach a consensus
 - no central node for voting

- Integration of Agreement Protocol Service in EASIS software topology

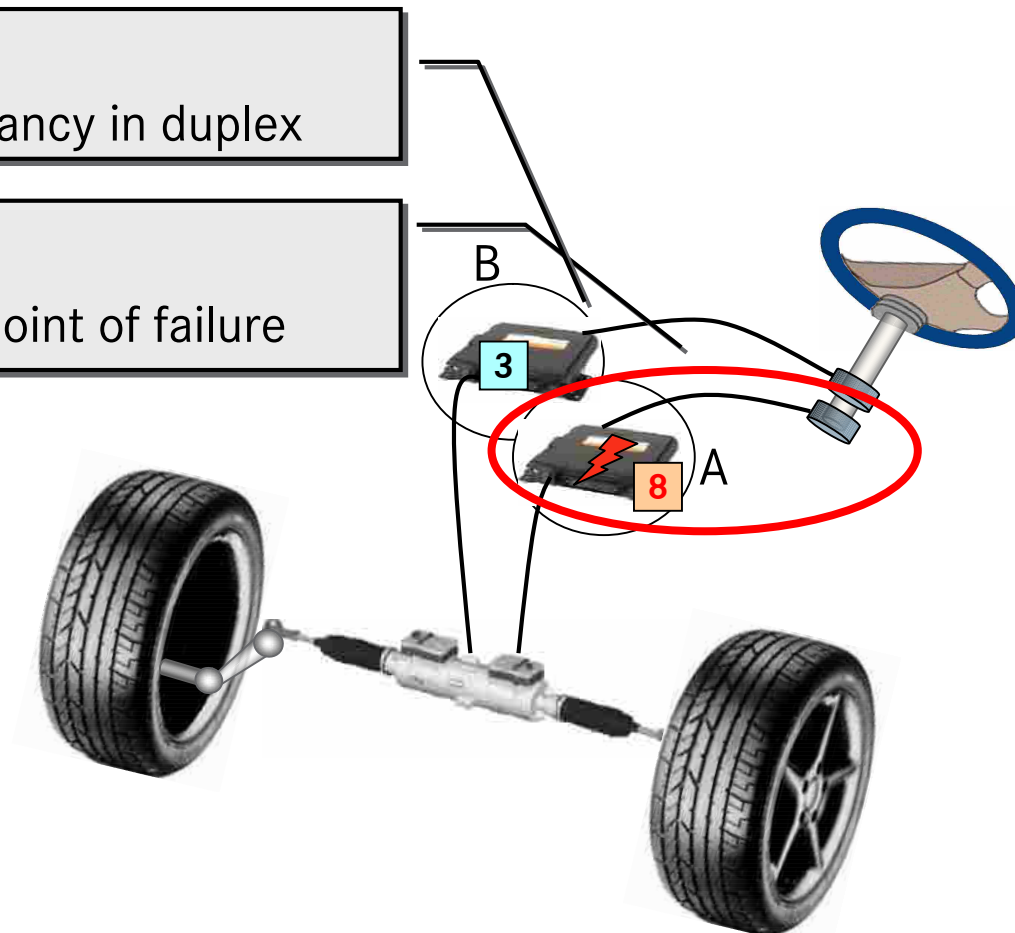
Fault-Detection in Duplex-System

Solution

- Redundancy in duplex

Problem

- Single point of failure



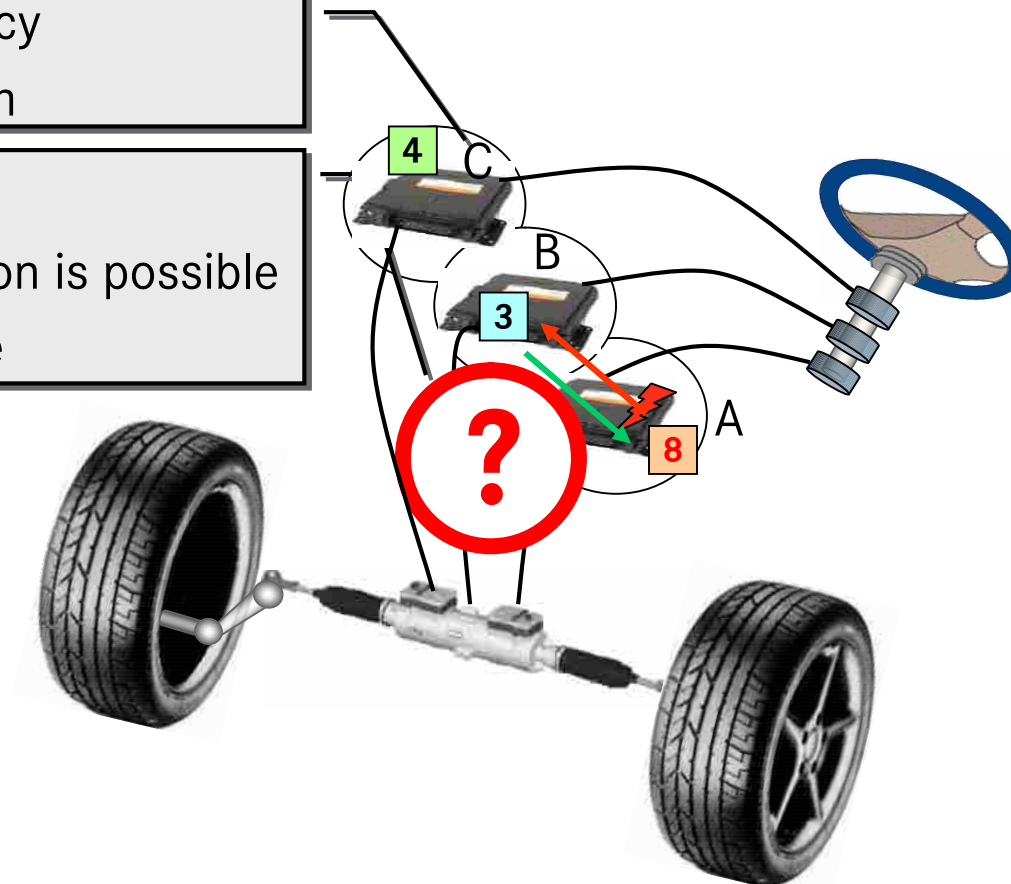
Fault-Tolerance in Triplex-System

Solution

- Further redundancy
- Voting mechanism

Problem

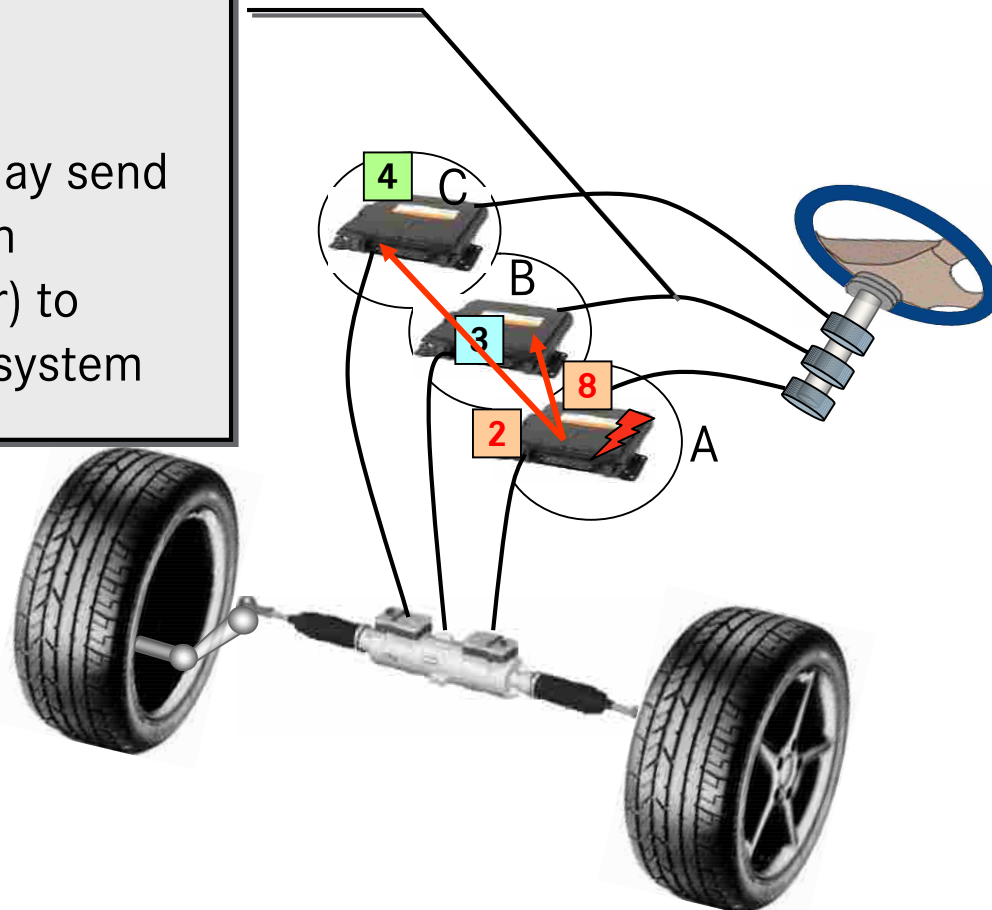
- Only fault detection is possible
- No fault tolerance



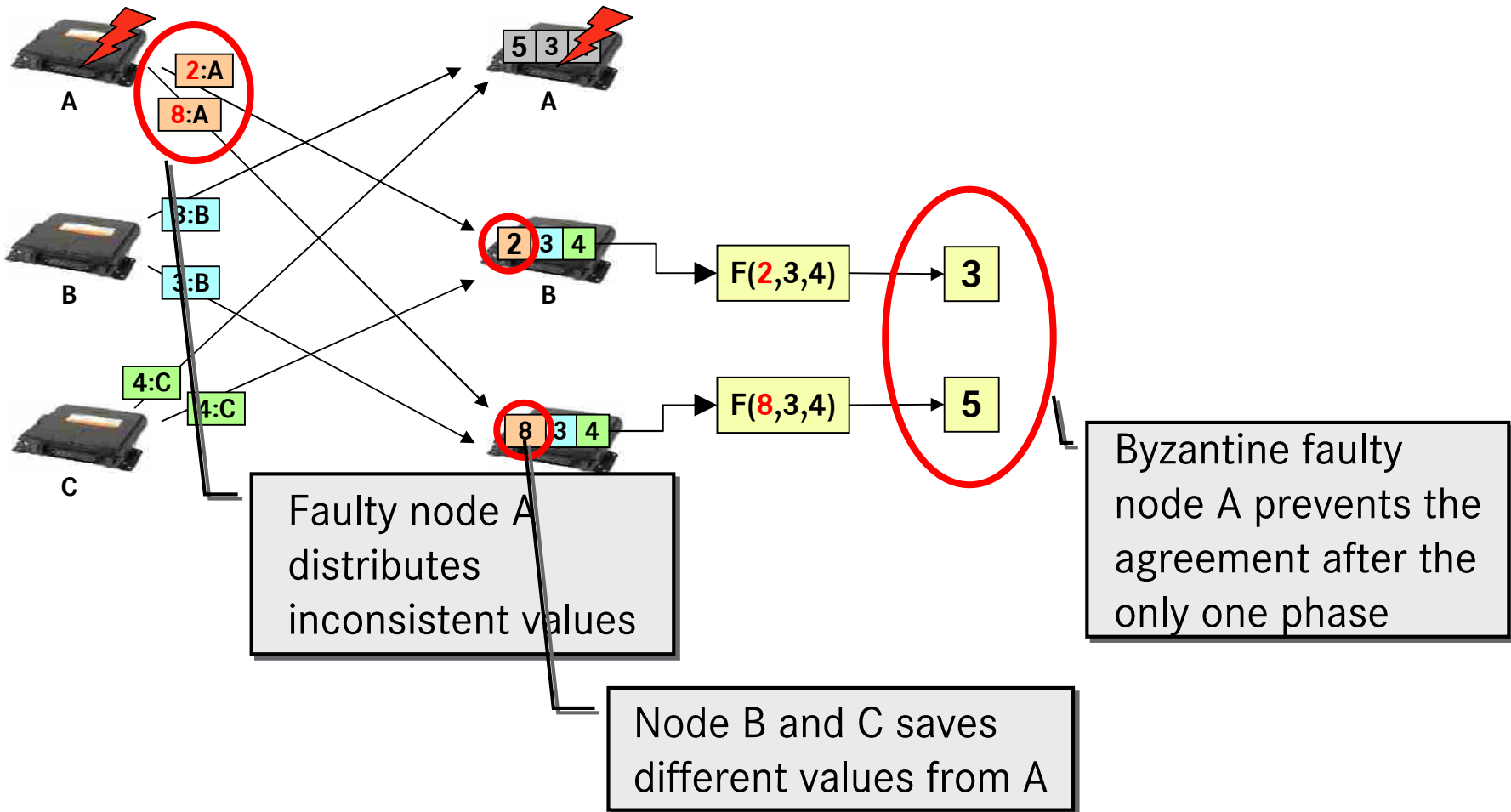
Byzantine Faults (1)

Problem

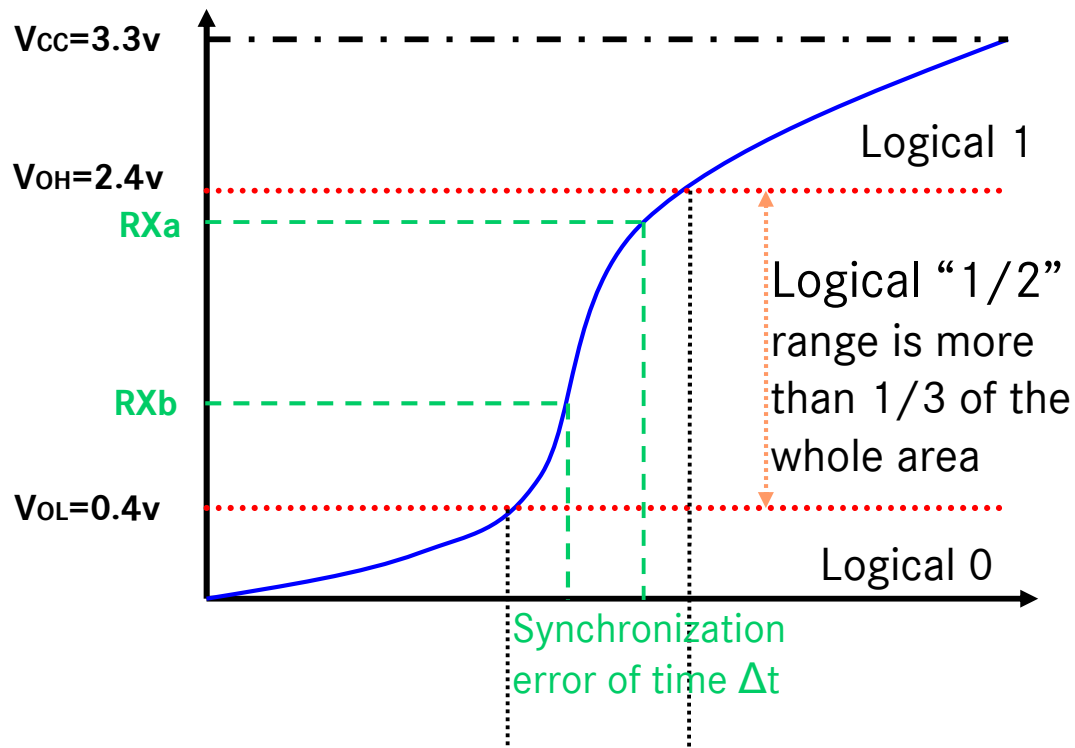
- Byzantine faults:
A failed component may send conflicting information (inconsistent behavior) to different parts of the system



Byzantine Faults (2)



Byzantine Faults in Automotive Electronics



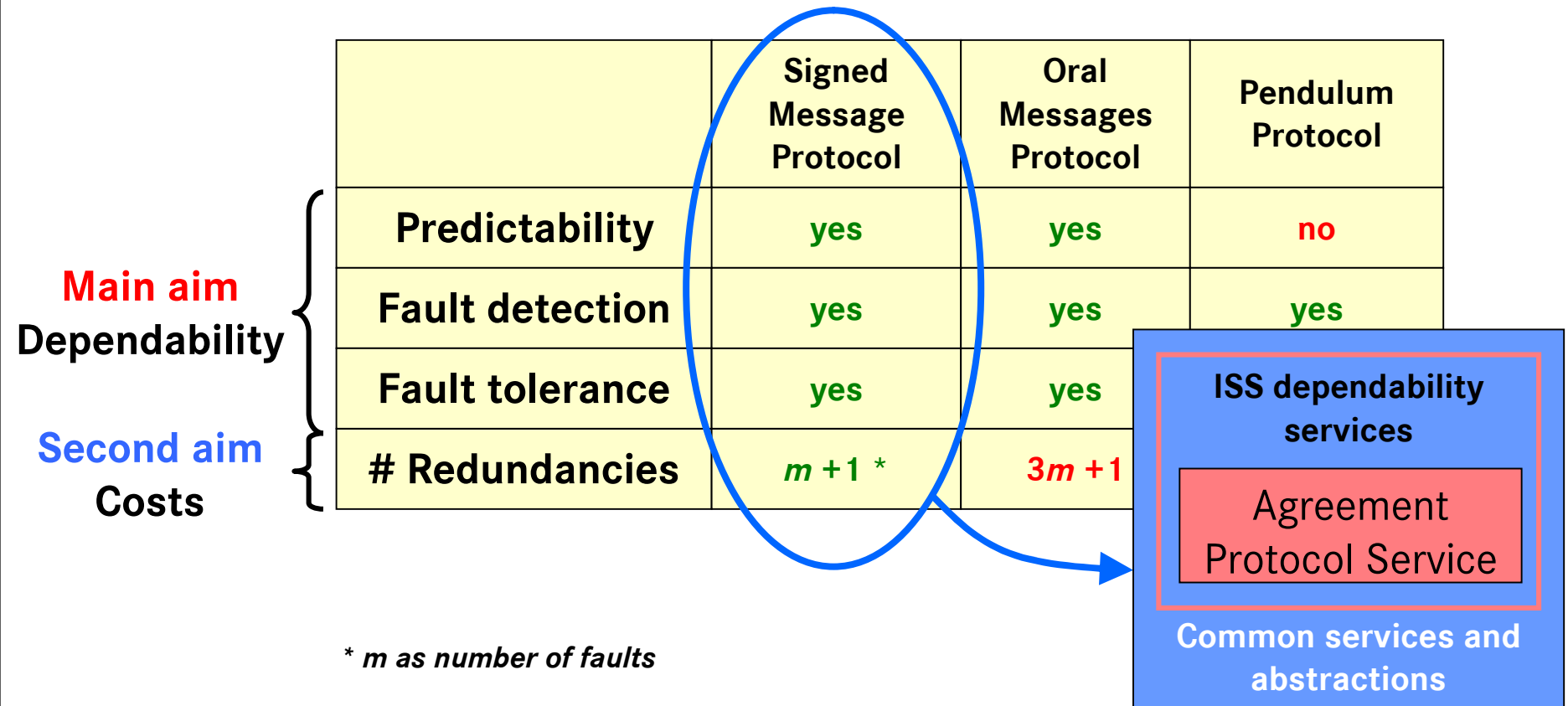
Problem

- Byzantine fault resulted from "1/2" threshold in signals and CRC
- Byzantine fault resulted from variation in signal amplitude and time synchronization

Contents

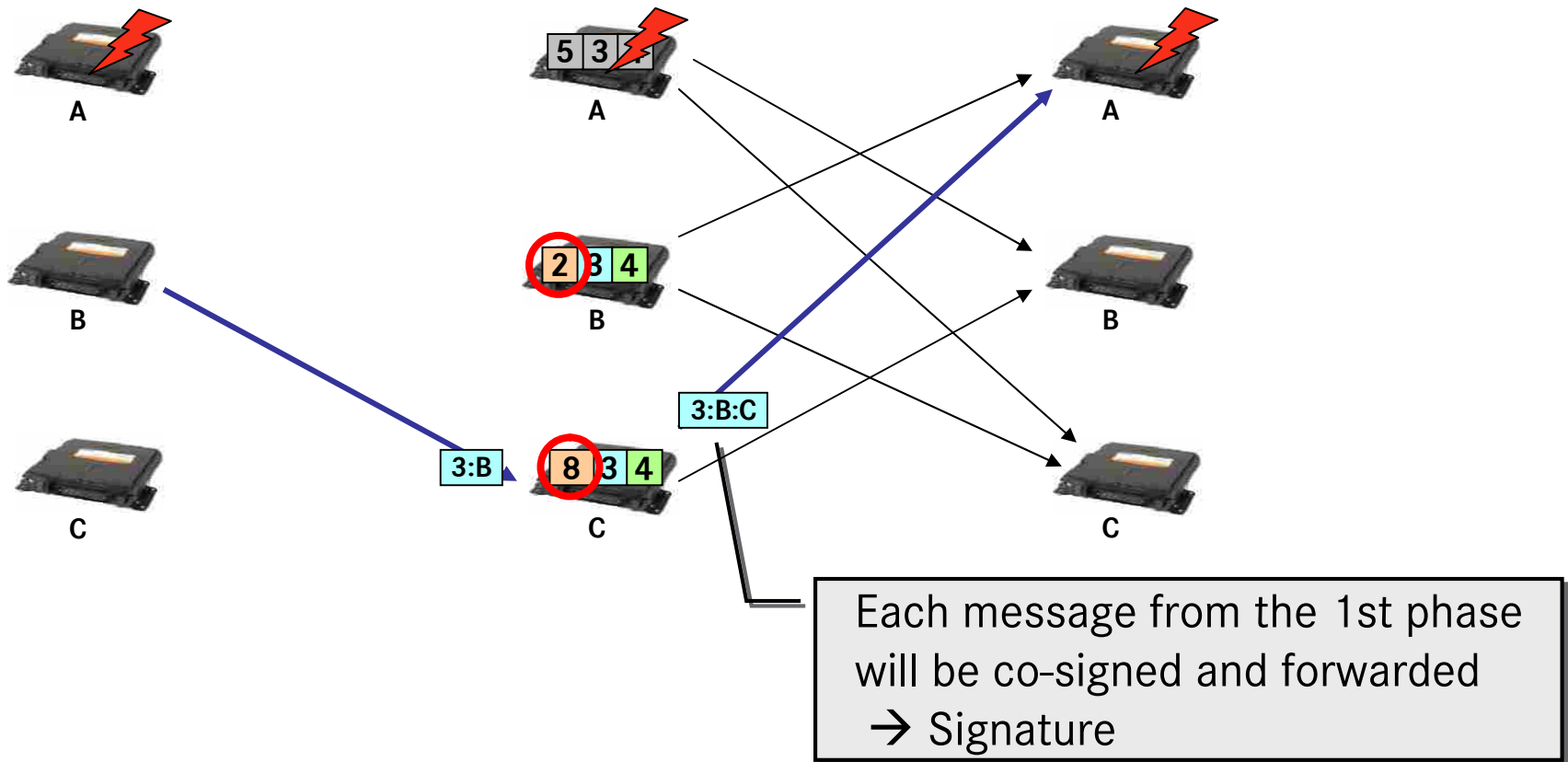
- Motivation
- Overview of In-vehicle Electronics and Introduction to Integrated Safety Systems
- Agreement Protocol - Reaching Consensus among Distributed Nodes
- **Development of Agreement Protocol Service in EASIS**
- Integration and Validation in the EASIS Validator
- Conclusion and Outlook

Assessment of variant Agreement Protocols

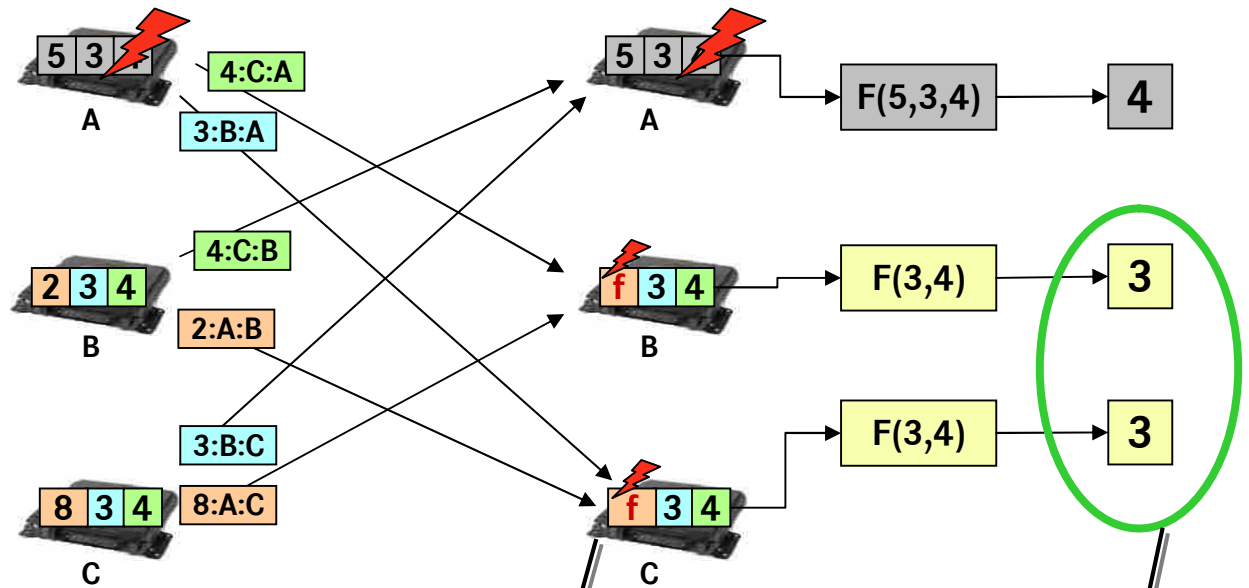


* m as number of faults

Signed Message Protocol



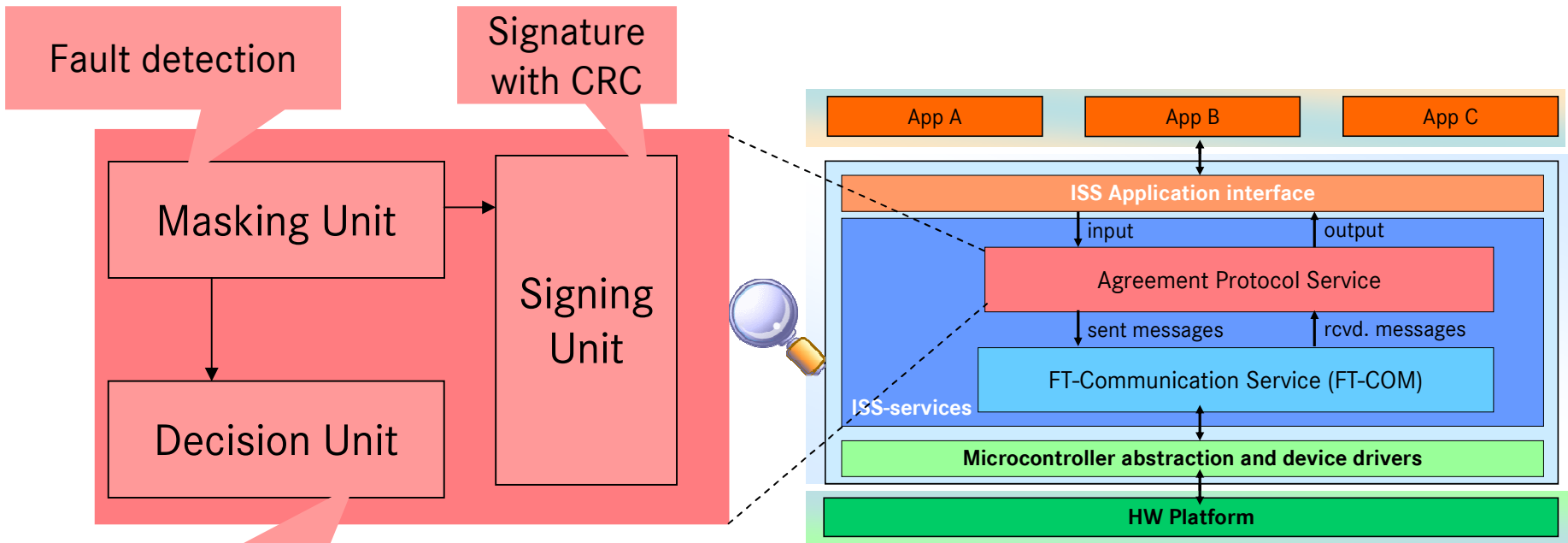
Signed Message Protocol



Inconsistence in the values from A
 → Fault detection

Agreement on the fault-free nodes despite of Byzantine faults
 → Voting mechanism

Integration of Agreement Protocol Service in EASIS SW-Topology

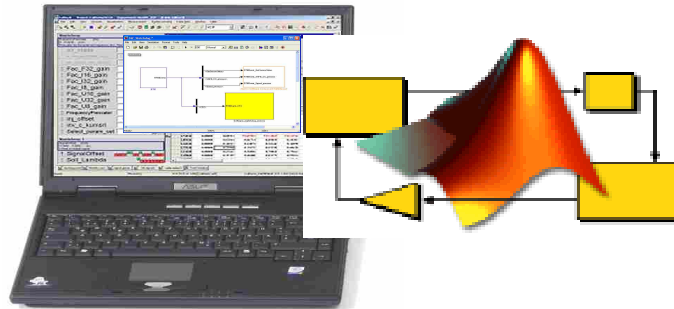


- Adaptation of Agreement Protocol in signing, masking and decision unit
- Integration of Agreement Protocol in EASIS SW-Topology as an extension of FT-COM

Contents

- Motivation
- Overview of In-vehicle Electronics and Introduction to Integrated Safety Systems
- Agreement Protocol - Reaching Agreement among Distributed Nodes
- Development of Agreement Protocol Service in EASIS
- **Integration and Validation in the EASIS Validator**
- Conclusion and Outlook

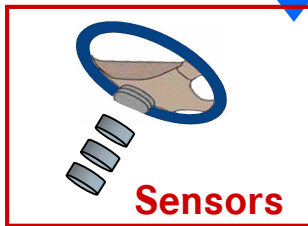
Development and Integration with Rapid Prototyping



Model-based software development of dependability software services with Matlab/Simulink/Stateflow

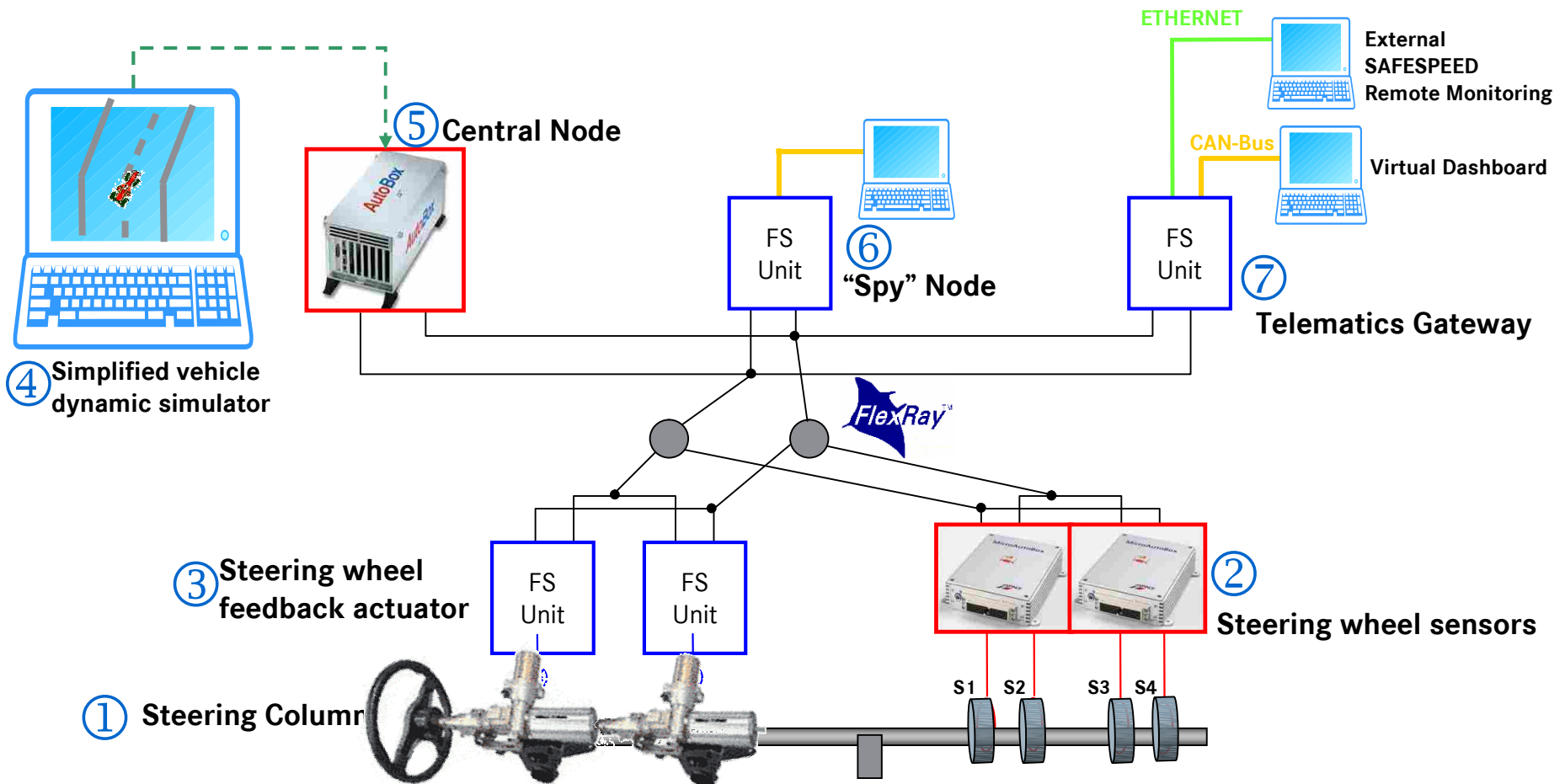


Virtual integration and code generation with e.g. real-time workshop

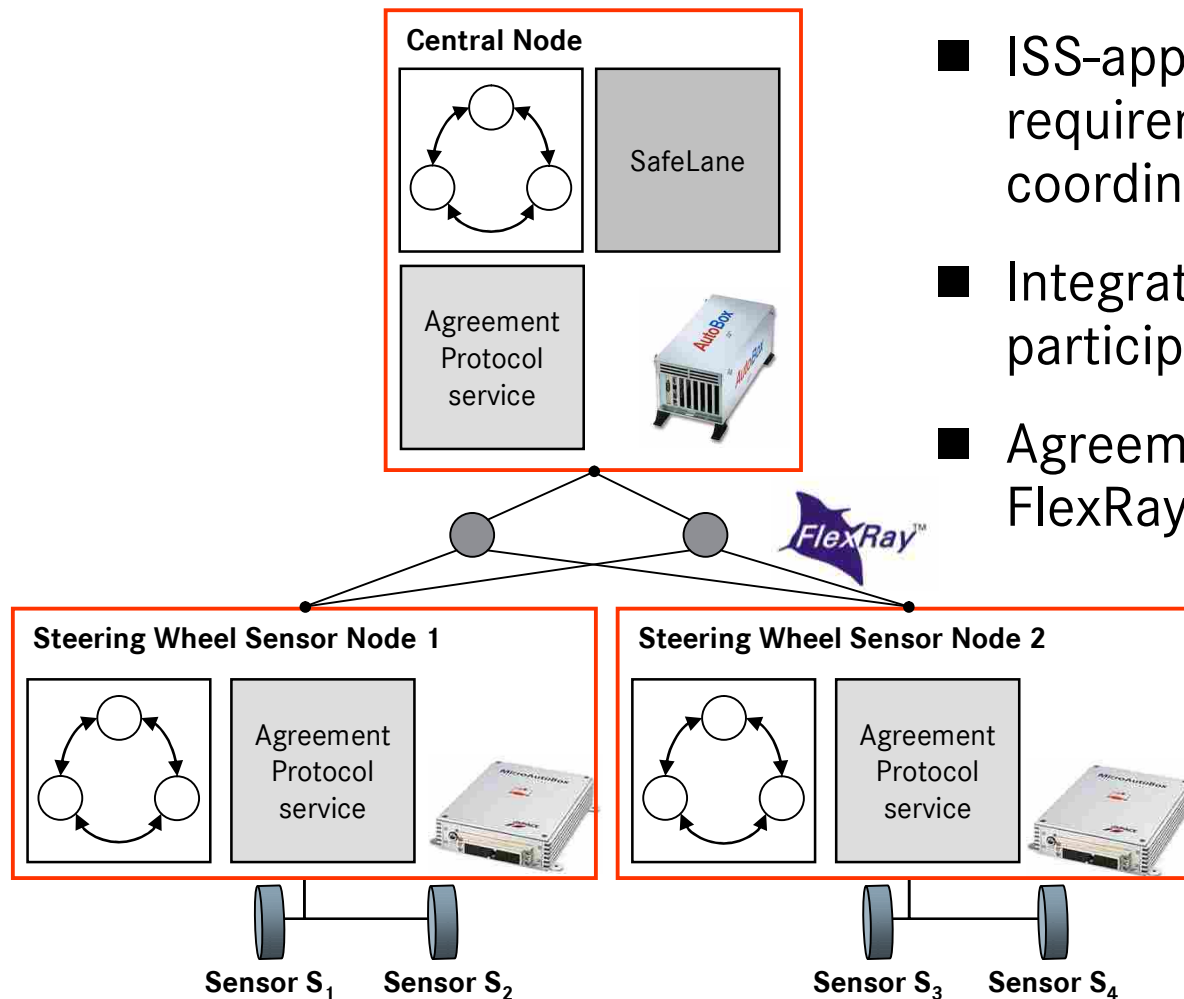


Rapid prototyping platform MicroAutoBox with FlexRay interfaces

EASIS Validator



Validation Scenario of Agreement Protocol Service in EASIS



- ISS-application with dep. requirements of distributed and coordinated state transition
- Integration of AP in each participated node
- Agreement Protocol on basis of FlexRay-communication

Contents

- Motivation
- Overview of In-vehicle Electronics and Introduction to Integrated Safety Systems
- Agreement Protocol - Reaching Consensus among Distributed Nodes
- Development of Agreement Protocol Service in EASIS
- Integration and Validation in the EASIS Validator
- **Conclusion and Outlook**


Conclusion and Outlook

■ Conclusion:

- Integrated Safety Systems bring new requirements to the in-vehicle E/E-architectures and dependability software services
- Concept and design of Agreement Protocol Service was validated with model-based rapid-prototyping approach

■ Outlook:

- Further evaluation of Agreement Protocol Service on an in-vehicle platform
- Agreement Protocol Service with configurable features in a standard library of dependability software services according to the safety requirements



EASIS Thanks for your attention!
Any questions?

For more info see: www.easis.org

E-mail: xi.chen@daimlerchrysler.com

