FlexRay™

www.flexray-group.com

The communication system for advanced automotive control applications

FlexRay International Workshop

16th and 17th April, 2002

Munich

FAN analysis

Dipl. Inf. Jens Lisner - University of Essen

Project FAN - Goals

- Verify the design of FlexRay
  - in particular: countermeasures against faults
- Assess properties of FlexRay
  - in particular: effectiveness of countermeasures
- Study of the parameters
- Identify potential weak points
- Discuss improvements and extensions

Project FAN - Topics

- General
  - Fault modeling
  - Modeling of time consumption
  - Agreement protocols
- Operation of the communication controller
- Behaviour of the Channel
- Clock synchronization
- Operation of the bus guardian
- Start-up phase

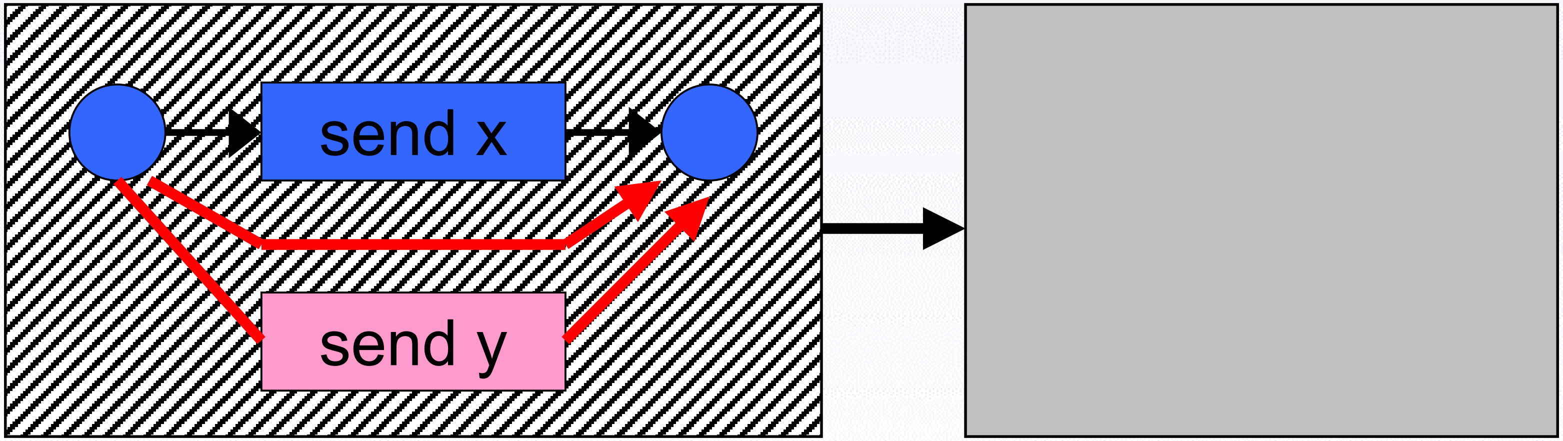
Project FAN - Methods

- Paper studies
  - including calculations and formal proofs
- Fault modeling in a formal framework
- SDL models
  - of components and protocol parts
- Simulation
- Reachability analysis
- Interpretation of results

Fault Modeling

- Definition of fault regions - typically components
  - internal behaviour not of interest
- Potential fault propagation
  - at the interfaces between fault regions
- Potential malfunctions:
  - fail silence, fail omission, timing failure,non-code value failure, arbitrary failure, ...

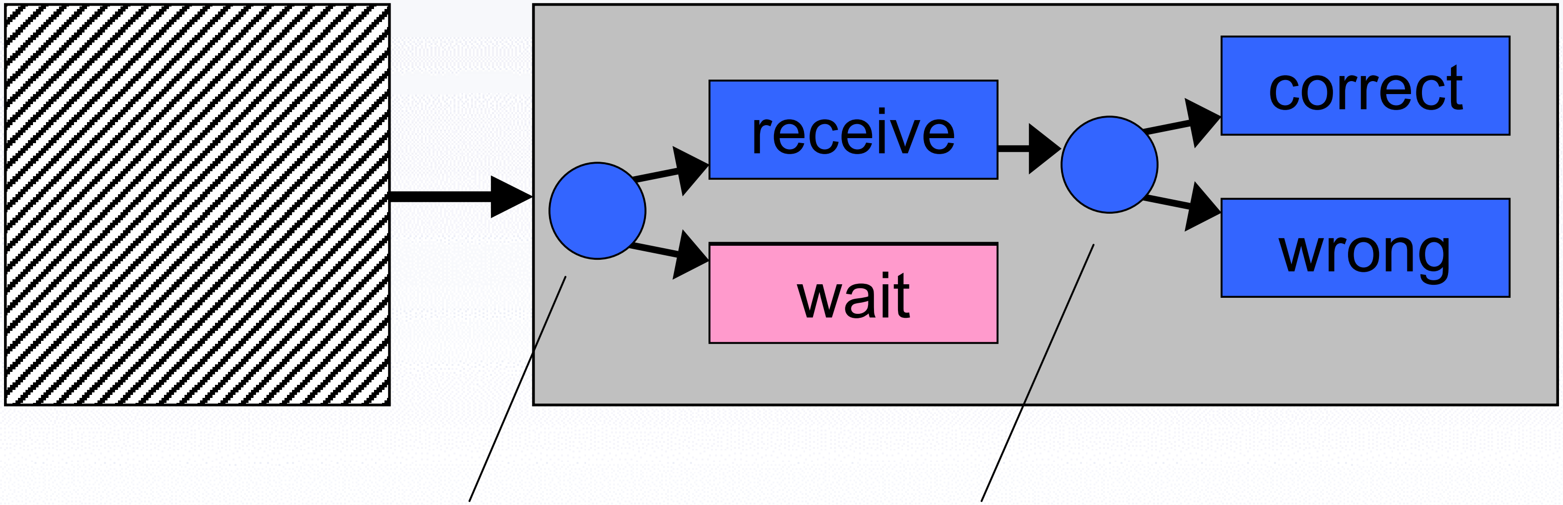
Explicit Fault Modeling in SDL



- Sometimes problem:
  - many different faults, all leading to the same error processing

Implicit Fault Modeling in SDL

Model processing of information originating from a faulty node



Non-deterministic selection

Non-deterministic selection - without expressing the (correct or wrong) information itself

Modeling of Faults in FlexRay

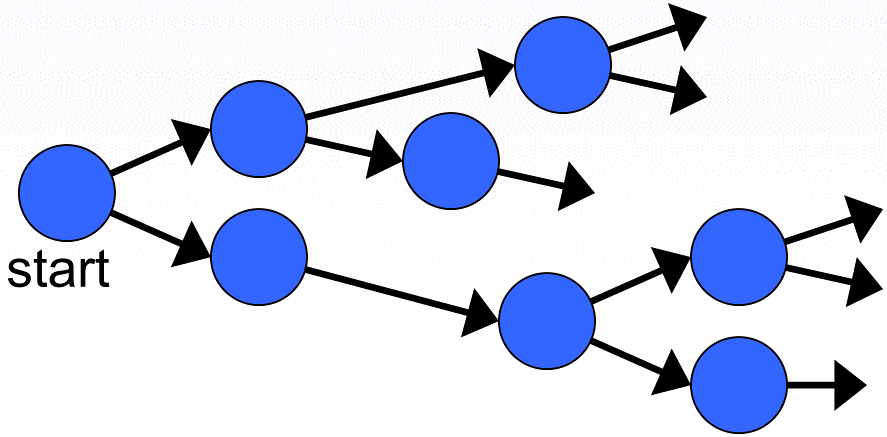
- Faults of FlexRay components have been identified
  - controller, guardian, bus driver, star coupler,...
- Explicit fault model in special cases
- Implicit fault model in most cases

- Sometimes extensive fault models because
  - Fault can be propagated through several components
  - Error processing can be distributed over several components

Reachability Analysis

- Language SDL (specification and design language)
- Components = extended finite state machines.
- Interactions = exchange of signals.
- Typical: non-determinism, caused by concurrency and non-predictable durations

Generate all potential sequences of events:



All potential behaviours of the system.

Tools for Reachability Analysis

SDT:

- Simulation and reachability graph
- Message sequence charts (incl. sequence of events, timeouts, ...)
- Exceptional situations: deadlocks, unreachable states, ...
- Observation of user-specified rules

Quest, additional features:

- Accurate model of time and shared resources
- Observation of user-specified rules expressed in temporal logic

Partial and Exhaustive Analysis

Potential problems:

- State space explosion
- Extremely high number of paths to reachable states.

Solution: partial state space exploration

- Random walk
- Bit-state algorithm
- Exploration from a user-defined point in the reachability graph
- User-defined cuts in the reachability graph
- Step-by-step

Conclusion

Project FAN:

Deep Investigation of Countermeasures against Faults in FlexRay

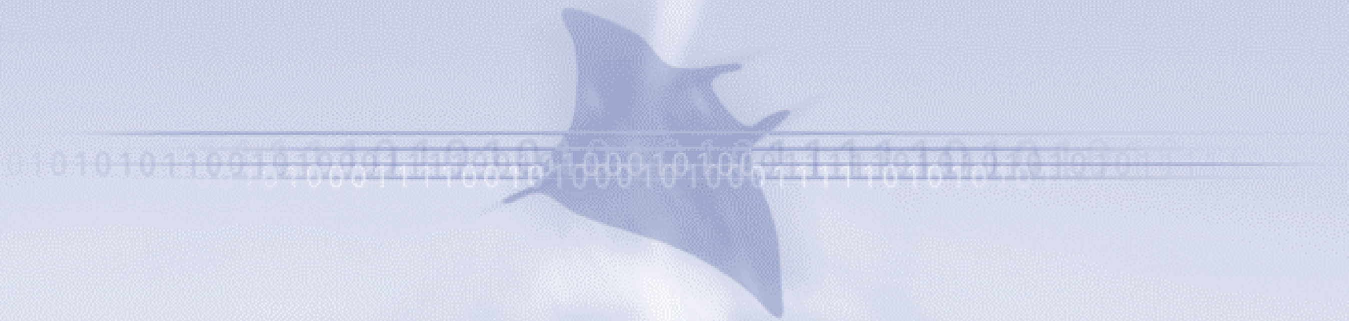
Verification of the Countermeasures

Fields of Research

Klaus Echtle, Patrik Kessler, Jens Lisner, Bruno Müller-Clostermann
Research Group: Dependability of Computing Systems
Institute for Computer Science
University of Essen

- Design of efficient fault-tolerant protocols
- Efficient combination of redundancy techniques
- Modeling and analysis of fault tolerance
- Software-implemented fault injection
- Virtual duplex systems, based on time diversity
- Systematic diversity

FlexRay International Workshop



www.flexray-group.com