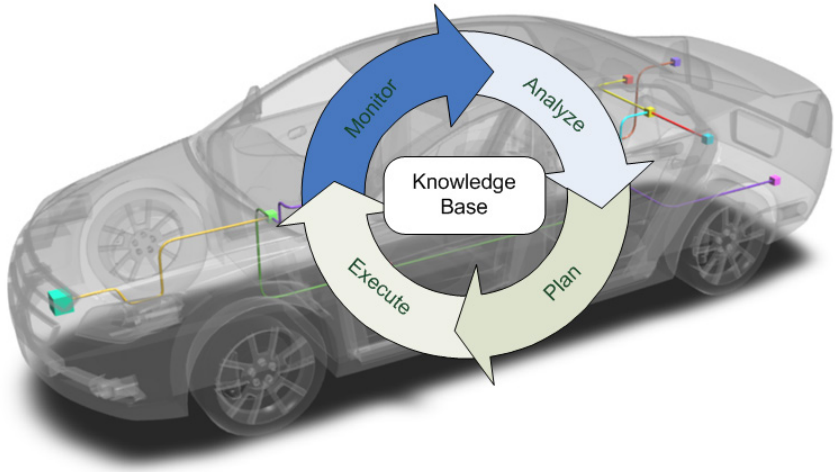
EFFICIENT REDUNDANCY THROUGH A GENERIC AUTOSAR FAILOVER-SERVICE: FROM MODEL TO IMPLEMENTATION

safe.tech (TÜV Süd)
28th & 29th of April 2015, Munich, Germany



Philipp Schleiß

Fraunhofer ESK

Trends in the Automotive Industry

- **Multi-Domain Controllers**
  - AUTOSAR: platform independent design & reuse of software
  - Reduction of dedicated units
  - Automated driving & increase in software

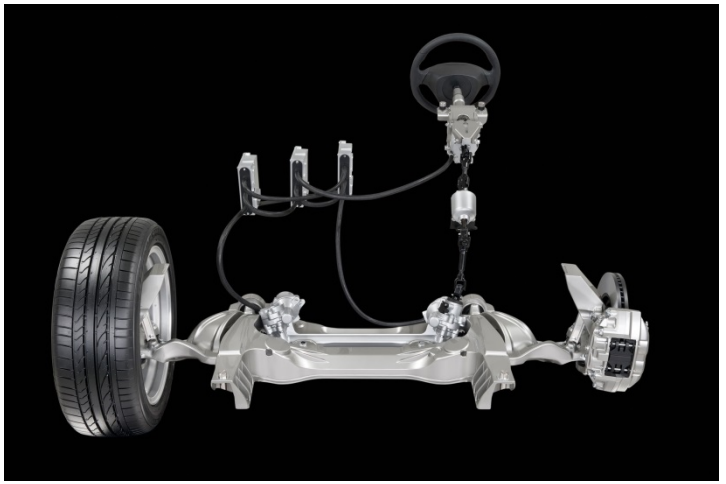
- **E-Vehicles**
  - More reliable electric power & 42V
  - Missing v-belt (e.g. for hydraulic pumps)
  - Potential for X-by-Wire?

➡ **Topic: Example of Demanding Requirements (Steer-by-Wire)**

➡ **Topic: Support for Redundancy Management in AUTOSAR**

History of Steer/Brake-by-Wire

- **Steer-by-Wire (Infinity Q50)**
  - Mechanical fallback with power steering
  - Probably 2oo3(D) design
  - Safety function: activate clutch
  - Return to conventional design in sports edition



Source: Nissan

- **Brake-by-Wire**
  - More common (e.g. Mercedes-Benz, Toyota, …)
  - Safety function: Connect master cylinder
  - Additional functionality (e.g. brake drying)
  - Trend: return to conventional design

➡ **Premium Features – Why not Mass Marketed?**

Requirements & Limitations of Inexpensive X-by-Wire

- **1oo2D Safety Architecture & Graceful Degradation**
- **Efficient Product Development Process**
- **No Mechanical Backup**
  - 70/311/EEC

  2.2.2.1: It must be **possible to steer** the vehicle even in the event of **total** or partial **failure** of the hydraulic, pneumatic or **electrical components** of the steering gear
  - 92/62/EEC

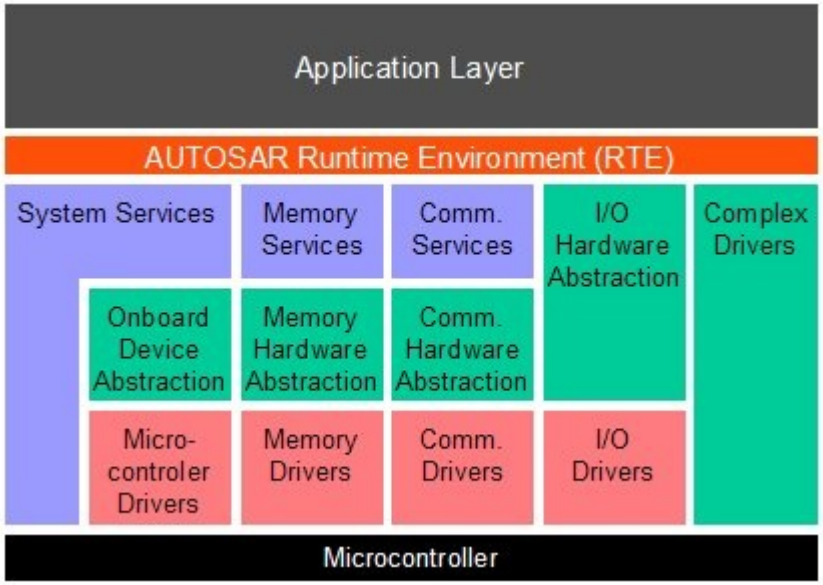
  4.1.6: Steering equipment with a purely pneumatic, **purely electric** or purely hydraulic transmission or with hybrid transmissions other than those described at item 1.6.4.1 are **prohibited** until specific requirements are added to the requirements of this Directive.

Implications of Steer-by-Wire w/o Mechanical Fallback

- **Reliable Power Supply for Steering**
  - E.g. starter battery is insufficient
- **What is the Safety Function?**
  - Inform the driver?
  - Halt immediately?
  - Prevent continuation of mission?
  - Reconfigure E/E architecture?
- **Effects of False Trips**
  - Stop and restart vehicle?

Generalised Software Requirements

- **Short Failover Times**
- **Reconfiguration (Graceful Degradation)**
  - No dedicated backup units
  - Deterministic behaviour
- **Status Quo**
  - Manual failure management
  - No native support for redundancy in AUTOSAR



Source: AUTOSAR Consortium, www.autosar.org/

Support Redundancy from Model to Implementation in AUTOSAR

SafeAdapt

Research

- Redundancy management in AUTOSAR
- Modelling system architecture
- Tools & development environment
- Evaluation of applying ISO26262

Prototype E-Vehicle

- Two steering engines
- Time-triggered network

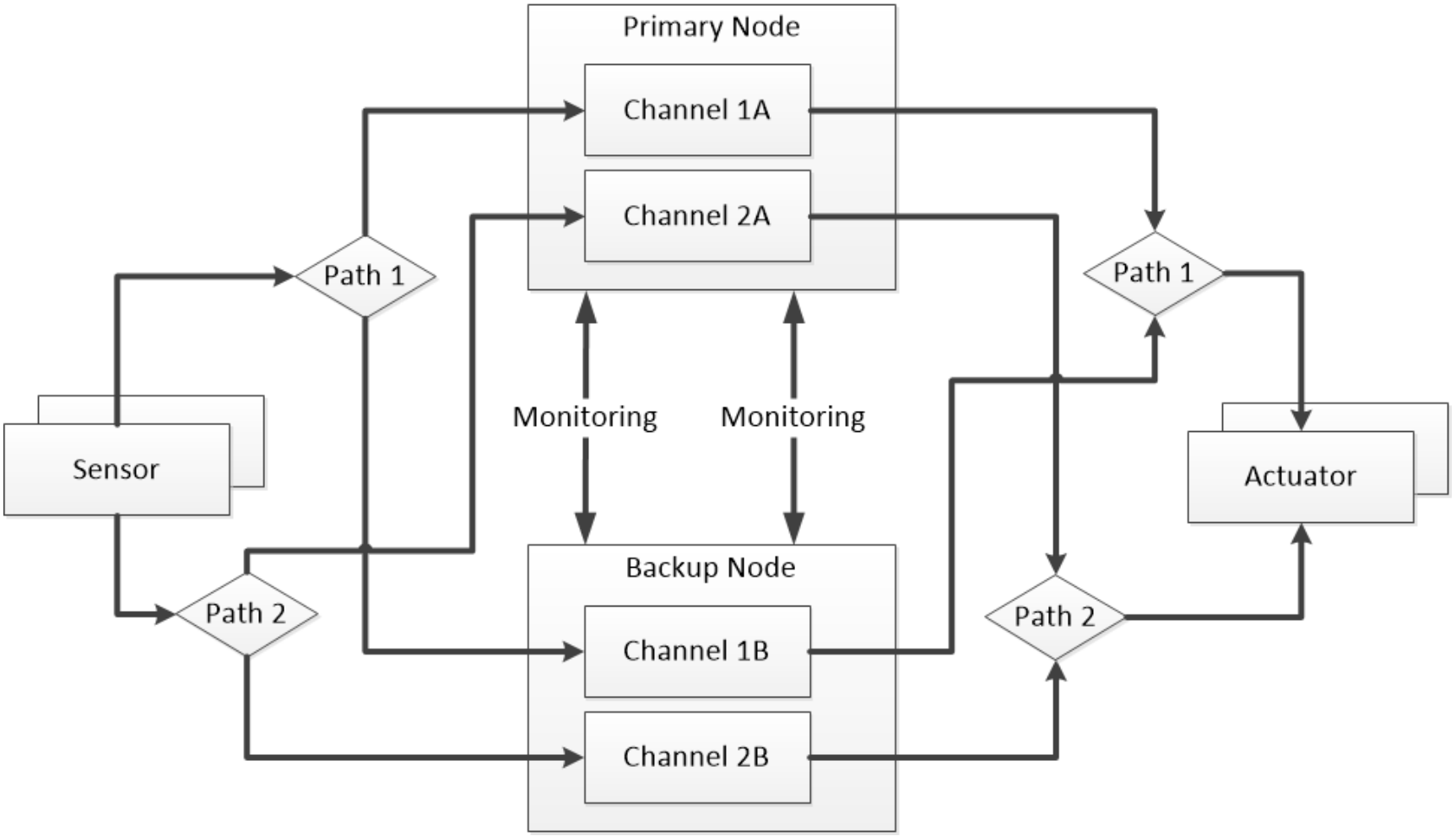
Source: Siemens

Duration: July 2013 - June 2016

SafeAdapt is a European research project under the Seventh Framework Programme – Grant agreement No 608945.

Fraunhofer ESK

Generalised Safety Architecture



Fraunhofer ESK

Properties of Safety Architecture

Distributed Safety Function

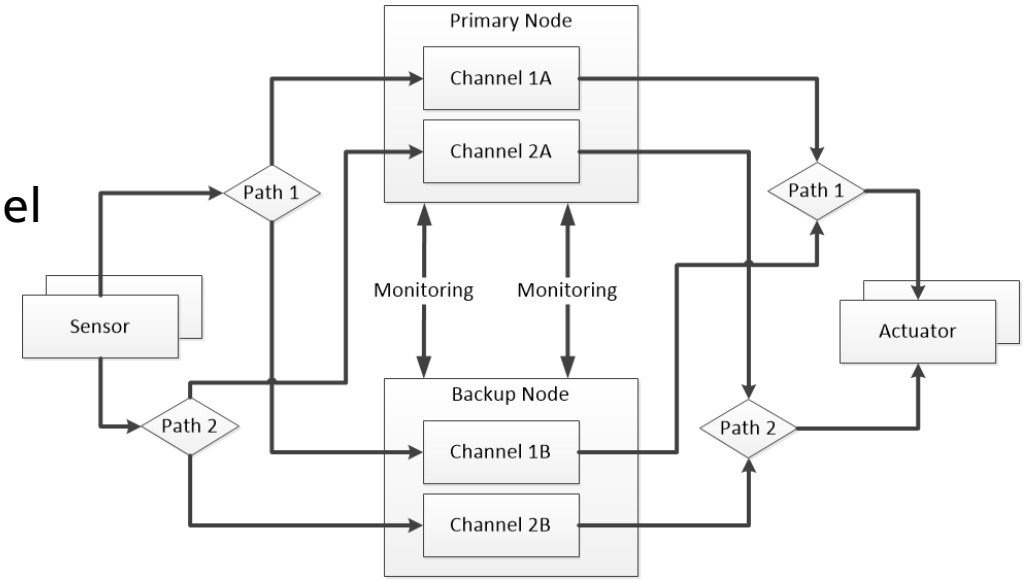
- Passivate primary node
- Detect passivation & reconfigure backup node
- Warn driver

1oo2D Design

- 1oo2 voting within node
- Diagnostics: cross node & cross channel

Graceful Degradation

- Utilise backup node for other tasks
- High resource utilisation



Fraunhofer ESK

Potential Hazards & False Trips

Two Masters

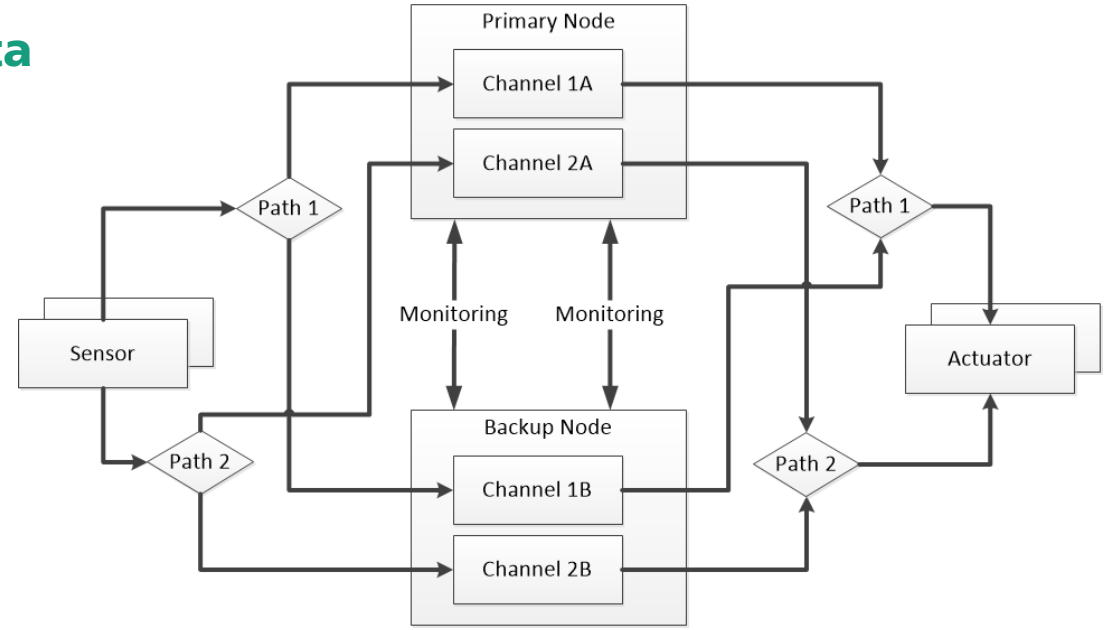
- Requires missing heartbeats on both paths
- Requires incorrect & congruent value on both channels

Missing & Incorrect Output Data

- Output on both links
- End-to-end data encoding

False Trips

- Self-test after vehicle restart
- Inexpensive
- New type of driver warning



Fraunhofer ESK

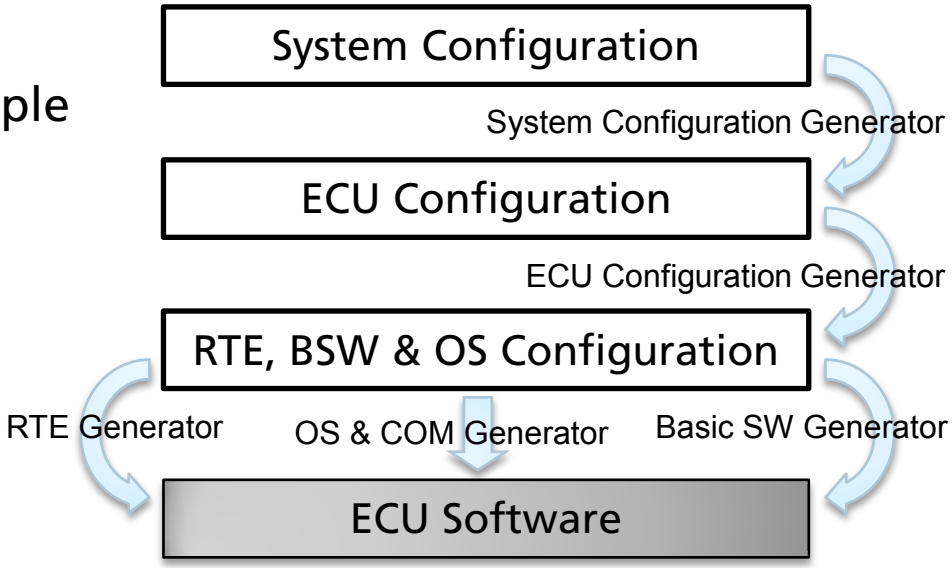
Design Phase (Modelling & AUTOSAR Toolchain)

Automatic Layout & Configurations

- Plan network & ECU schedules (according to timing & failover requirements)
- Primary & redundant instances
- Disposable software (graceful degradation)
- Communication channel in case of failure
- Data refresh channel & heartbeats
- Respect AUTOSAR's static design principle

Safety Requirements in EAST-ADL

- Failover times
- Redundancy (hot or cold standby)
- Monitoring instances
- Importance of features

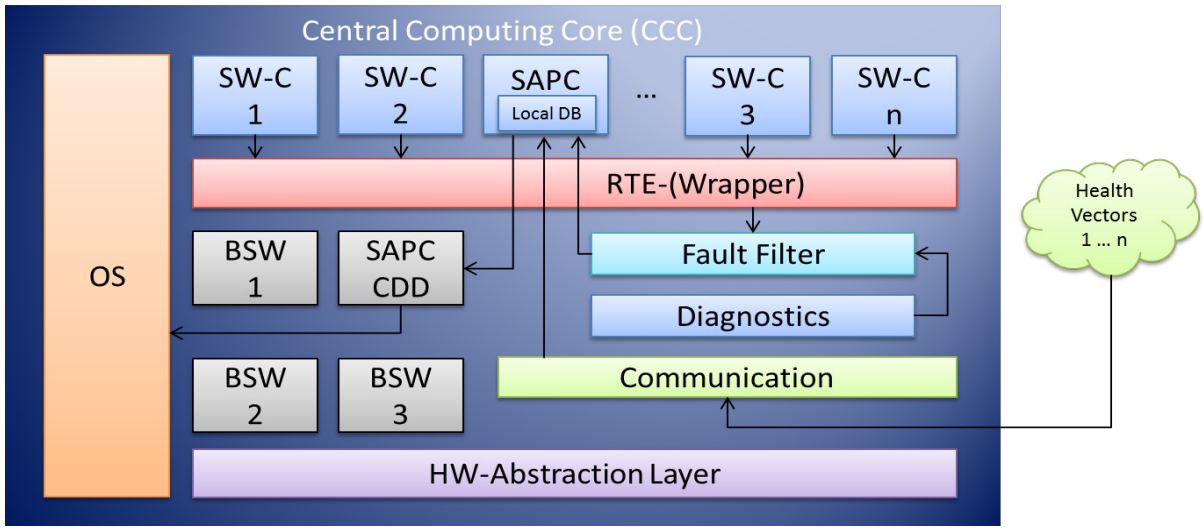


Fraunhofer ESK

Runtime Environment

Platform-Independent Redundancy Manager

- Move safety features into runtime environment
- Mapping of failures onto configurations
- Unified configurations
- Interfaces for platform
- Generalised failure modes
- Heartbeats & monitoring
- Benefit from COTS status

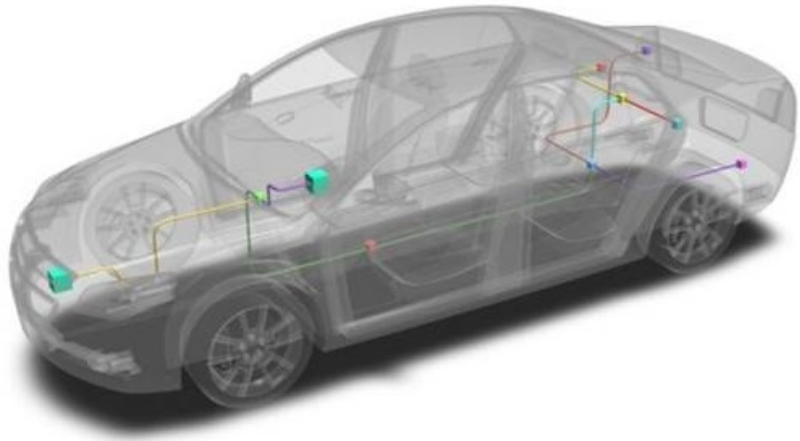


Integrate into AUTOSAR

- Utilise synchronised schedule tables
- Well-defined mode switching
- RTE-interfaces for redundancy management

Summary & Outlook

- **Continuous Support for Safety Requirements**
  - Modelling safety requirements
  - Automatic translation of requirements into code
  - Safety functionality integrated into runtime environment
- **E-Vehicles drive X-by-Wire Technology**
- **Efficient Designs**
  - Reconfiguration for graceful degradation
  - Strong resource utilisation
  - Reuse of safety artefacts
- Project website: www.safeadapt.eu



THANK YOU FOR YOUR TIME AND ATTENTION!

Philipp Schleiß, Research Engineer Automotive Software
Tel.: +49 89 547088-398 | philipp.schleiss@esk.fraunhofer.de

Source: Panthermedia

Follow us on:

Fraunhofer ESK