# Integration of Highly-Automated Driving Functions with Fail-Operational Properties

**Philipp Schleiß**

**safe.tech 2017**

Tel. 089/547088-398
philipp.schleiss@esk.fraunhofer.de

Fraunhofer
ESK

# Upcoming Availability Requirements of Automated Driving

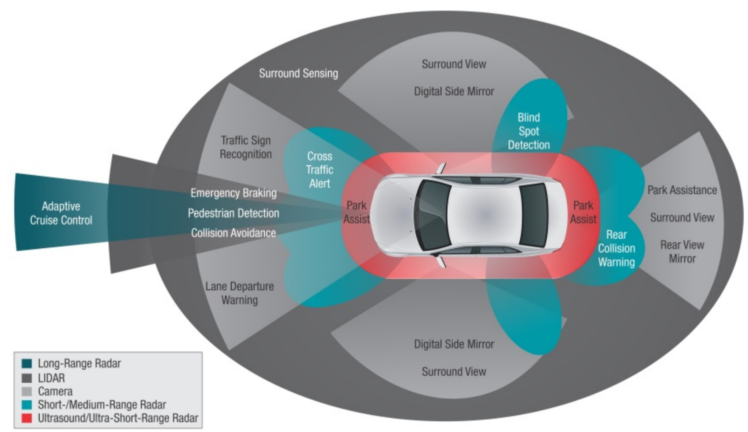
## System properties

- Systems must remain operational after failure
- Driver is not always part of control-loop
- Time required to regain control (multiple seconds)
- Transition from SAE automation level 3 to 4+
  - Requirement for fail-operational behaviour
- Cost-sensitive industry

## Safe state & failure handling

- Very infrequent failure of components
- Fail-operational only required for a short period
- Automated halting
- Pass control to driver

➢ **Failure modes increase complexity**



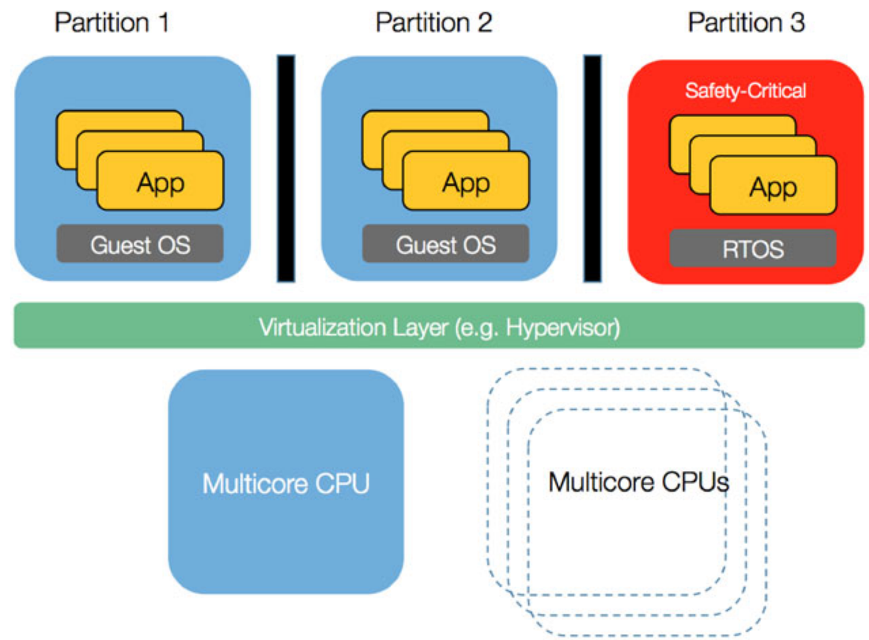

*Source: Texas Instruments*



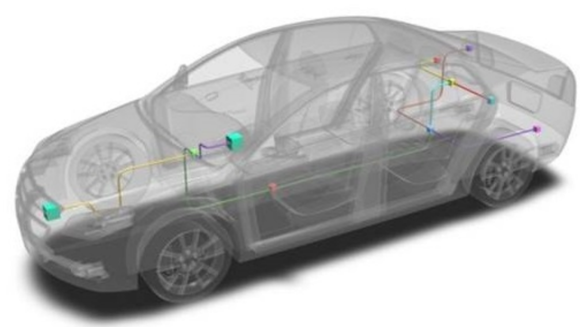
Fraunhofer ESK

# Integration Challenges (Mixed-Criticality & Availability)

- **Highly integrated systems**
  - Multi-Domain- and Area-ECUs
  - Mixed-criticality & flexibility
  - Increased computation demands (radar, camera, …)
  - Data integrity requirements
  - SW must be isolated in the memory & time domain
- **Ensuring high-availability**
  - Availability through redundancy
  - Cost-sensitive (how much redundancy is required?)
  - Failure modes: sensors, computing ECUs & network




Source: Grammatech



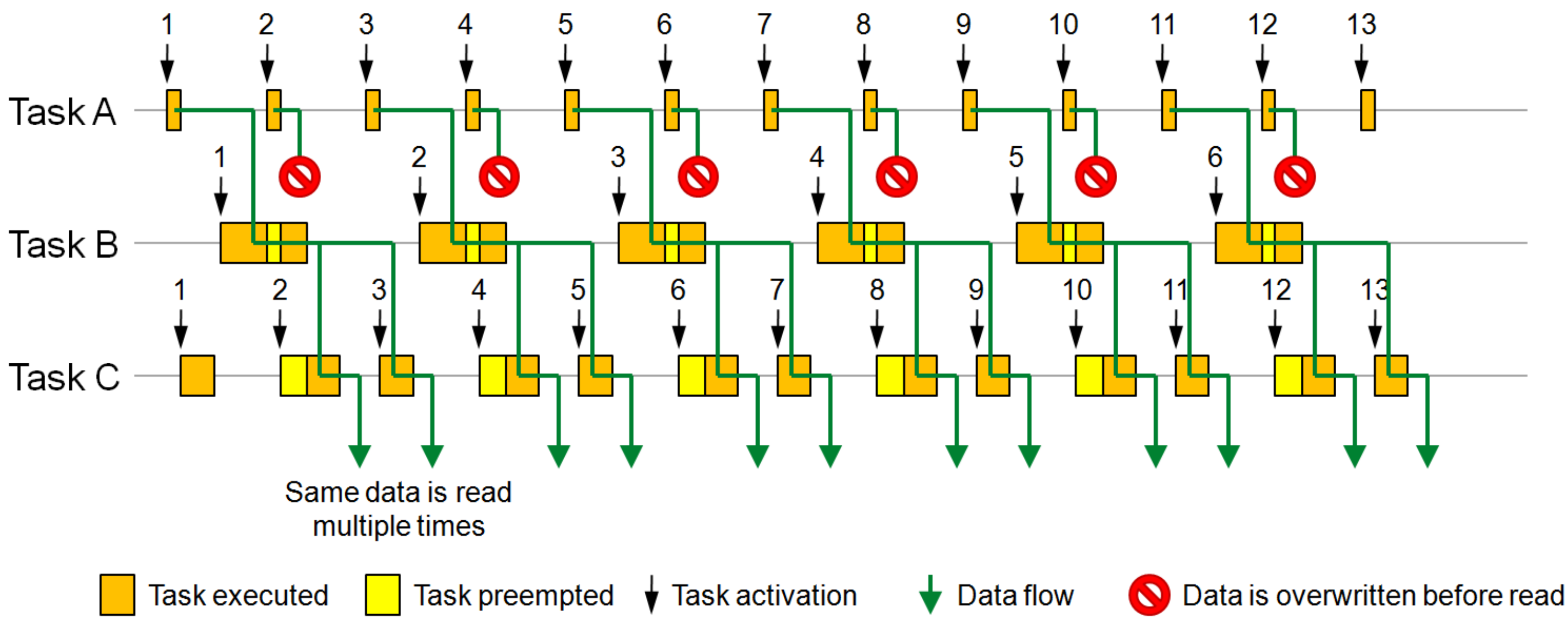
➢ **Substantial manual effort during system integration**



Fraunhofer ESK

# Integration Challenges (Timing)

- Sporadically occurring timing errors often only detected late

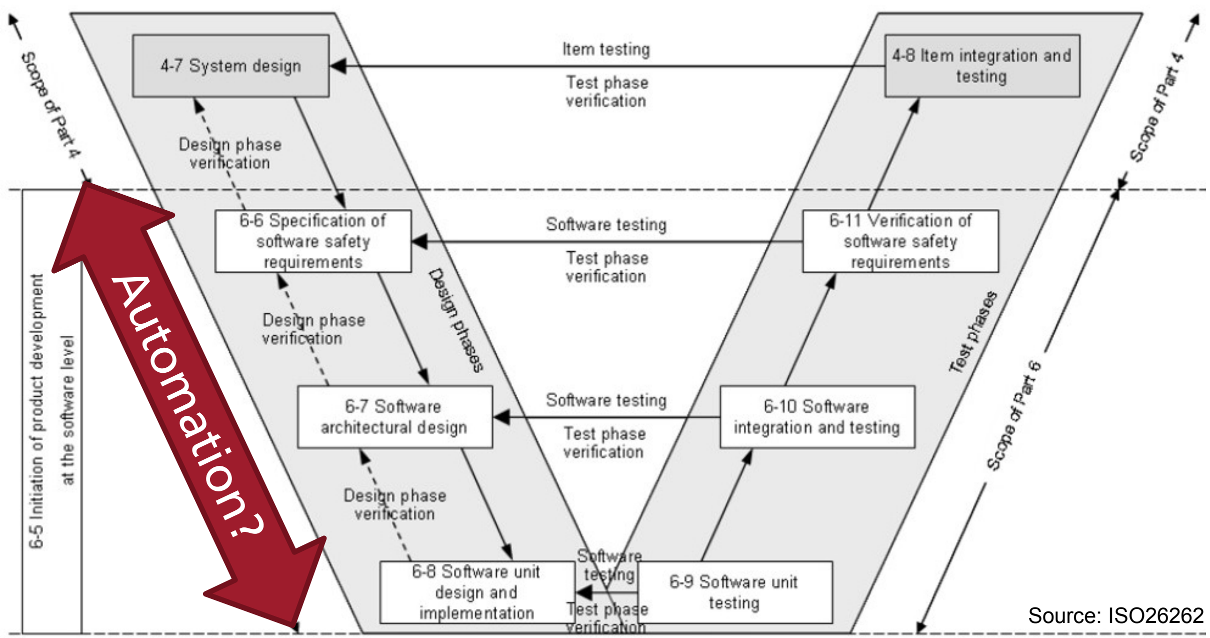



Source: Autosar

➢ Timing contracts and automated scheduling help eliminate errors (front loading)

# Automation Potential

- **Labour-intensive development process**
  - Deterministic behaviour requirements cause high testing & verification effort
  - Failure modes & availability requirements

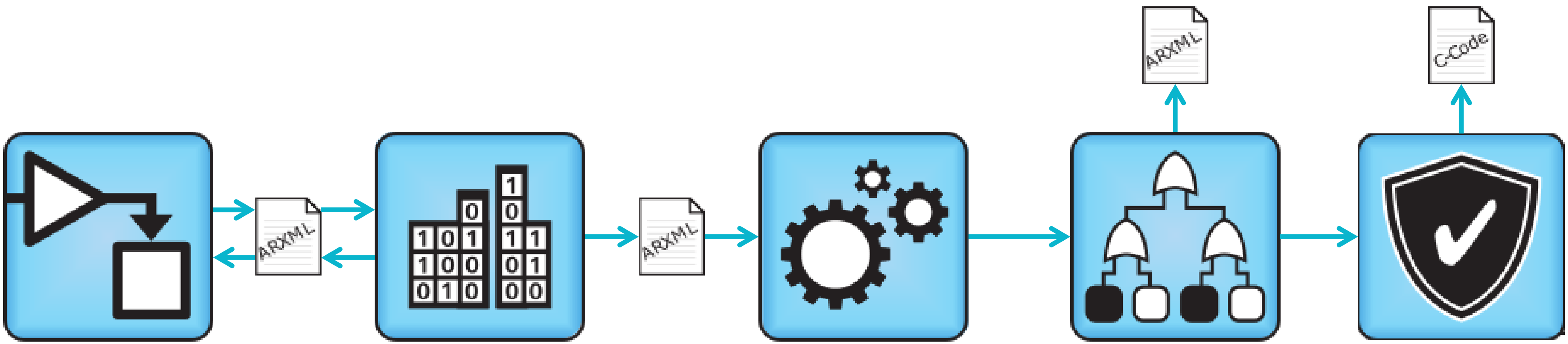


Source: ISO26262

➢ **High automation potential for reducing development effort**

# Solution: Automating AUTOSAR Integration Process

- Formal specification of failure modes & required functionality
- Tooling to schedule AUTOSAR systems (runnables & bus frames)
- Automated configuration of selected BSW modules (RTE, OS, Watchdogs, …)
- Configuration of generic availability management module (SAPC)




**Application Design**
- Timing requirements
- Availability req.

**Architecture**
- Graceful degradation
- Failure modes
- Timing details

**Planning**
- Schedules
- Failure modes
- MILP/Heuristics

**Configuration**
- System modes
- Schedules
- Timing guarantees

**SAPC**
- Availability
- Runtime

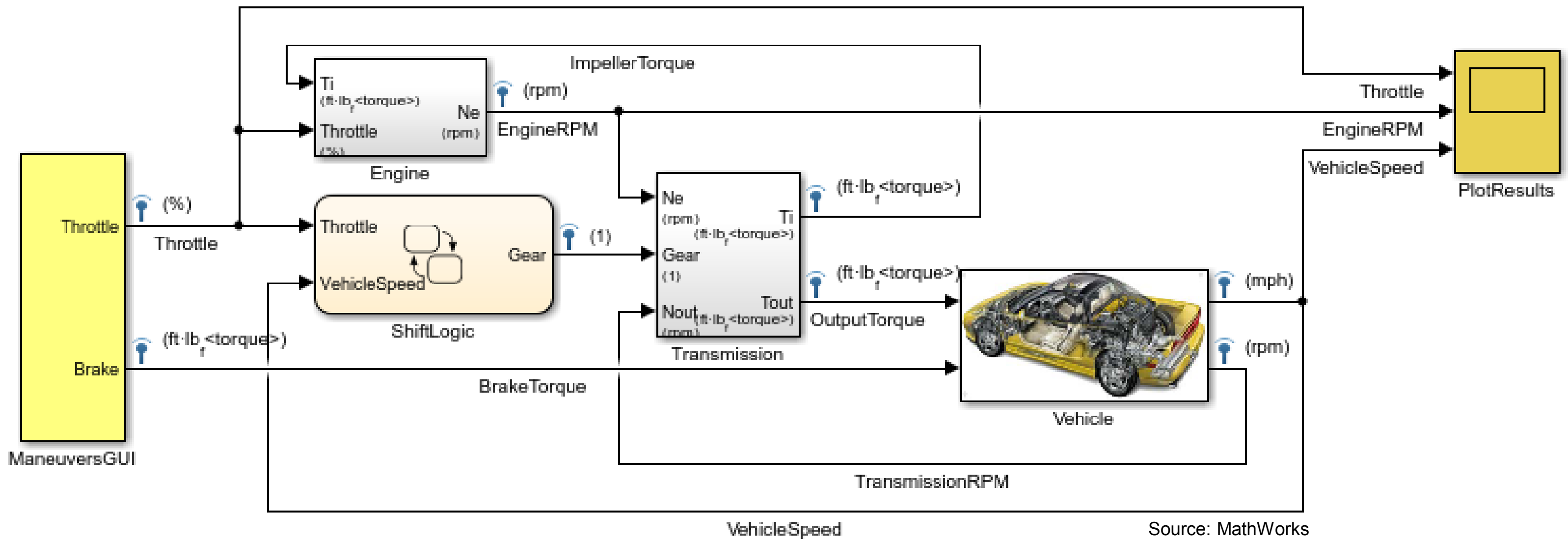




Fraunhofer ESK

# Required Information in Application Design

## Design of individual functions (export as AUTOSAR system description)




Source: MathWorks

## Availability requirements

- Failover times
- Link to FMEA & FTA
- Example: steering system

*Source: Tecnalia*

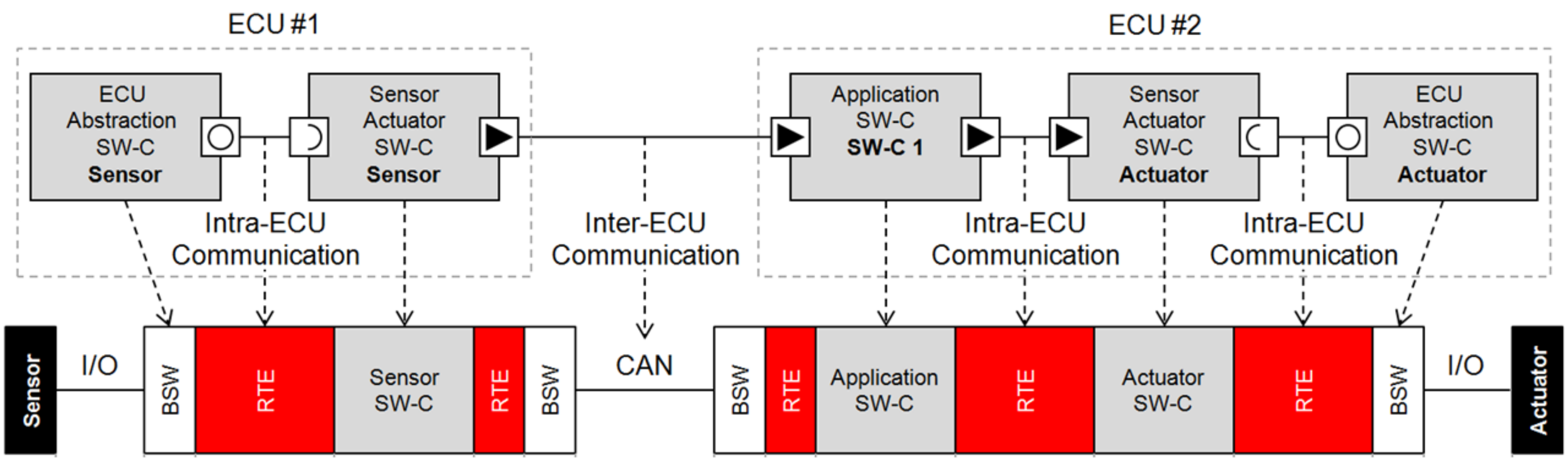




Fraunhofer ESK

# Formalised System Model

- **Rich system model within AUTOSAR**
  - Hardware, software & network architecture
  - End-to-end timing requirements
  - WCETs

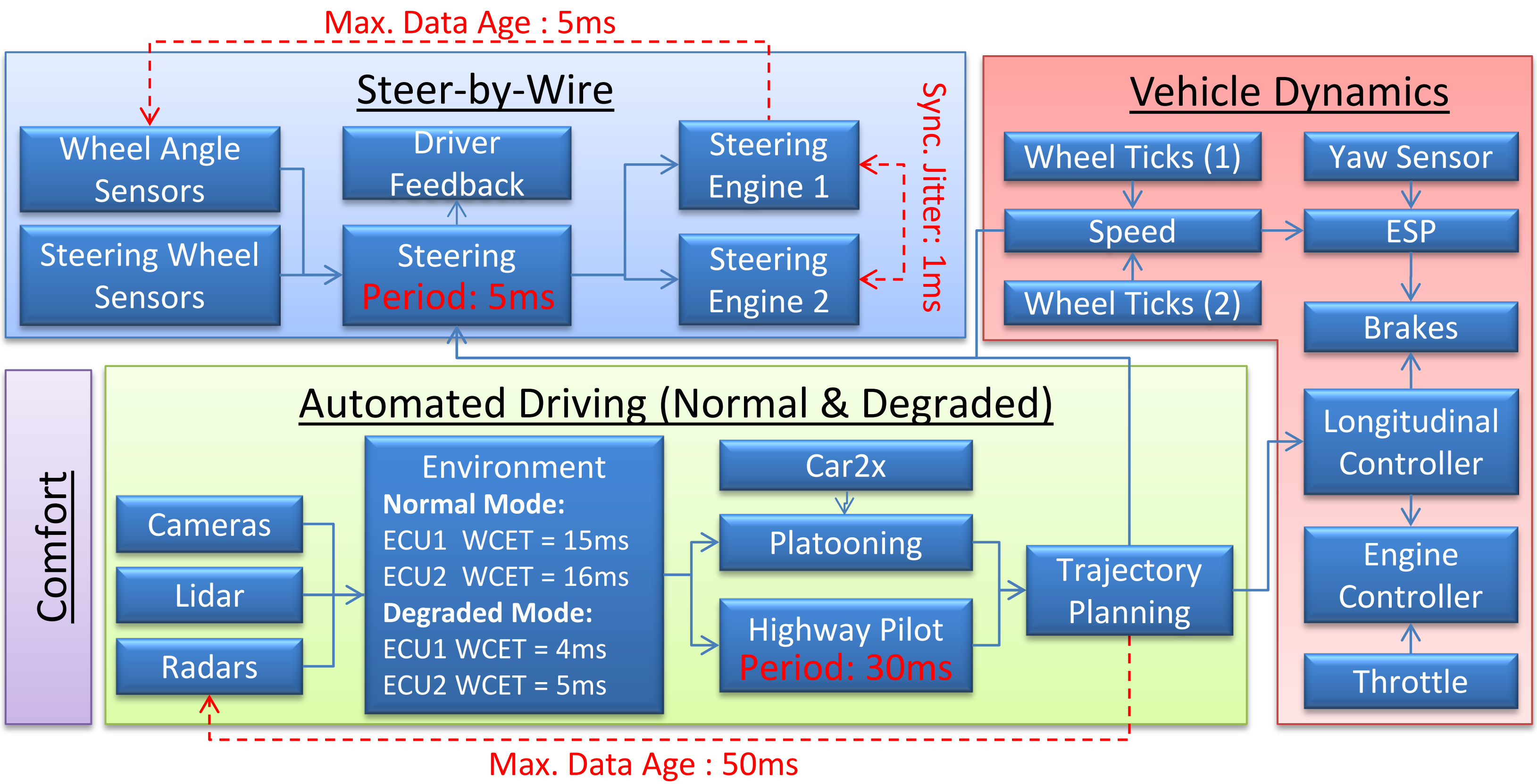



Source: AUTOSAR

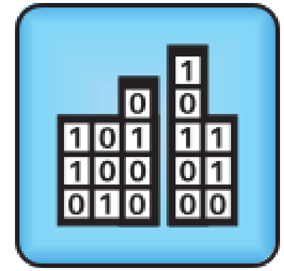
➢ **Availability requirements & failure modes missing in AUTOSAR meta-model**

# Example of Formalised AUTOSAR System Model

- Multiple variants of a functionality (e.g. normal and degraded)
- Hierarchical software architecture, complex data flows & timing information



# Representation of Availability in AUTOSAR Model

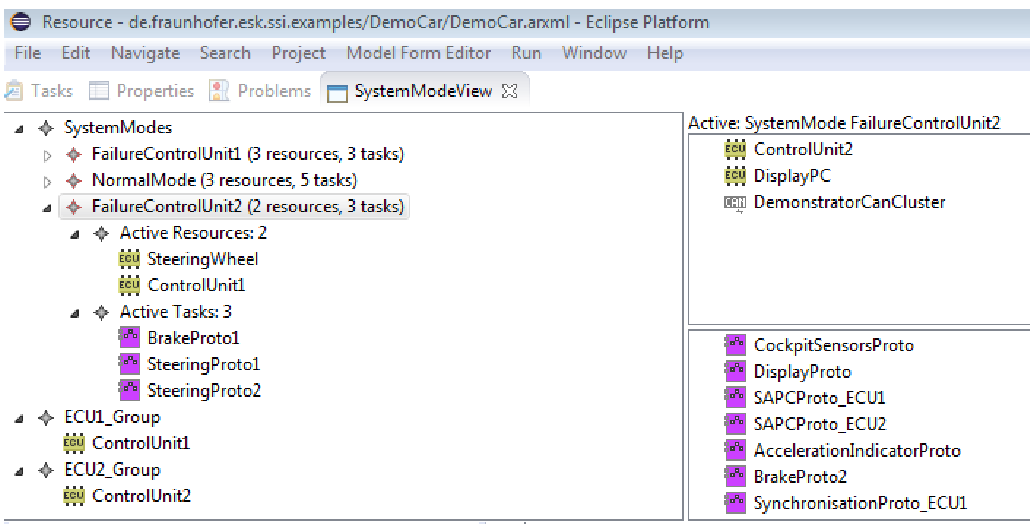


## Operational modes & graceful degradation

- Extension to AUTOSAR meta-model
- Editor for failure modes considering degradation within features

Replaces

| Auto. Driving (Degraded) | Veh. Dynamics | Steer-by-Wire | Auto. Driving (Normal) | Comfort |
|---|---|---|---|---|
| System Modes: failures | System Modes: all | System Modes: all | System Modes: all | System Modes: all |
| Priority: 1 | Priority: 1 | Priority: 1 | Priority: 2 | Priority: 3 |

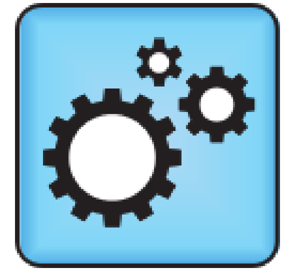







Fraunhofer ESK

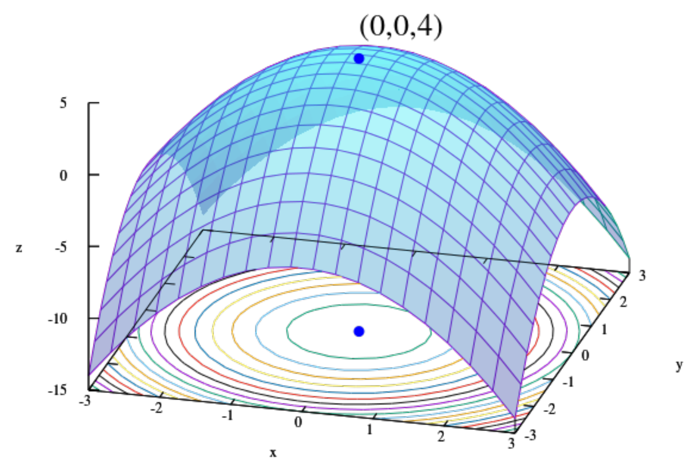
# Planning with Mixed Integer Linear Programme



## System represented as Mixed-Integer-Linear-Programme (MILP)

- Search for valid configurations
- Time- & event-triggered
- Support for preemptive scheduling
- Transition between modes (failover times)

$$\begin{aligned} &\text{maximize} && \mathbf{c}^{\mathrm{T}}\mathbf{x} \\ &\text{subject to} && A\mathbf{x} \le \mathbf{b}, \\ & && \mathbf{x} \ge \mathbf{0}, \\ &\text{and} && \mathbf{x} \in \mathbb{Z}^n, \end{aligned}$$




Source: Wikipedia

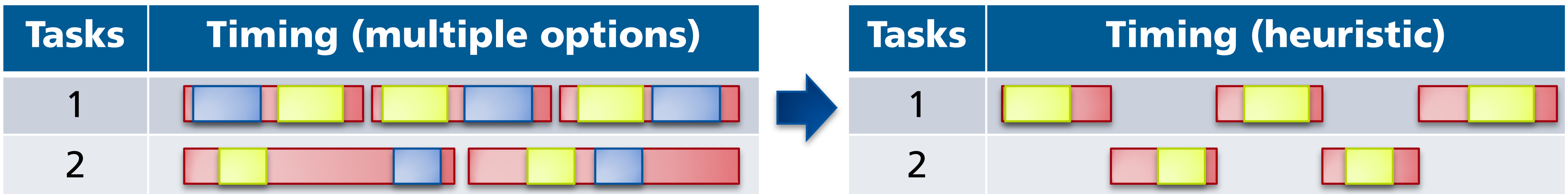
- ➢ **Rapid growth of mathematical representation**
- ➢ **NP-hardness, need for heuristic/domain knowledge**



Fraunhofer ESK

# Results: Planning Heuristics

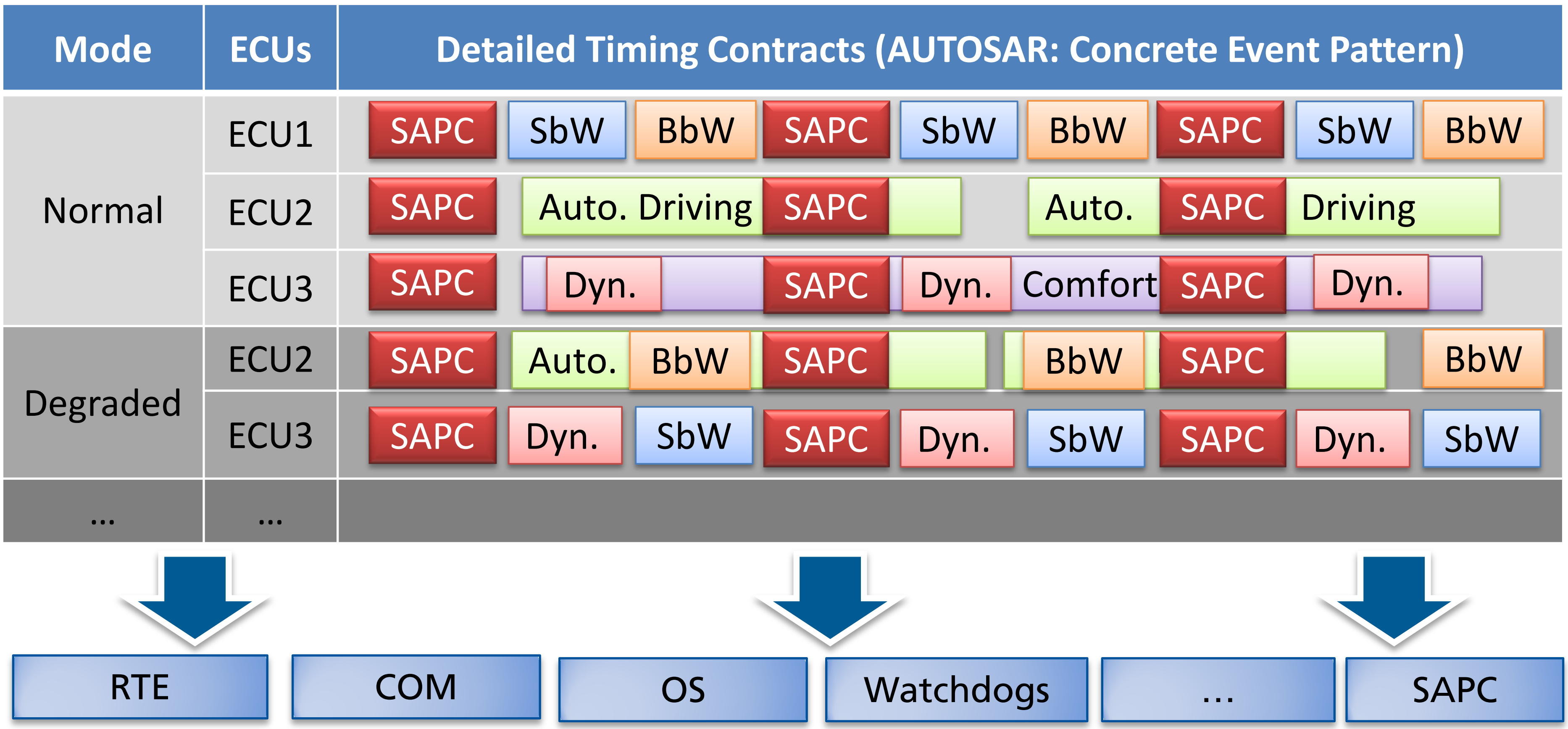
- **Heuristics as mitigation of NP-hard problem (scalability)**
  - Clustering of Jobs/Runnables (e.g. by sequence or period)
  - Pre-assignment of Runnables to resources (e.g. CPU core or ECU)
  - Reduction of binary decisions through pre-sorted executions




- **Performance results**
  - 3000 jobs in one hour
  - Further improvement with tuning of heuristics

# Automated ECU Configurations

- Graceful degradation & cold standby
- Deterministic runtime reconfiguration (SAPC)



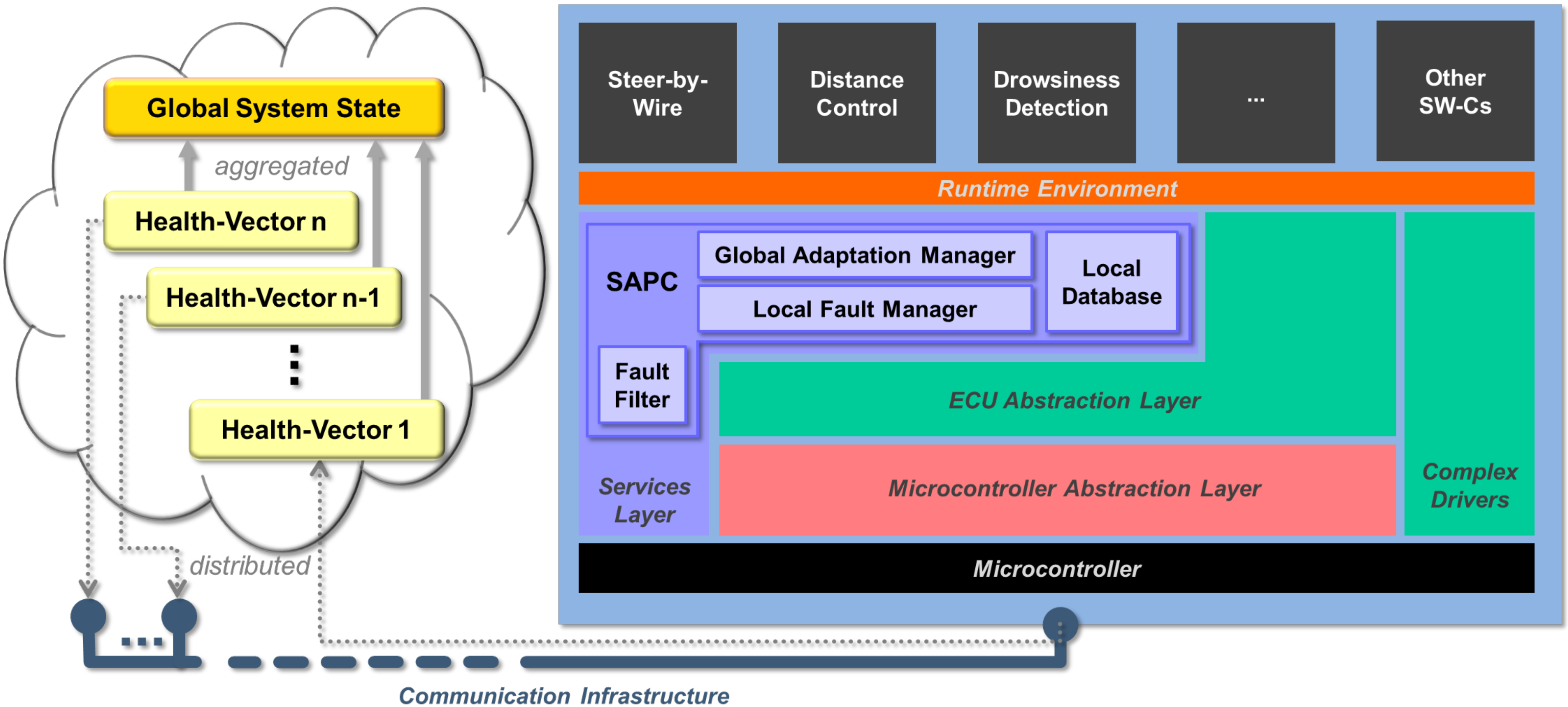





Fraunhofer ESK

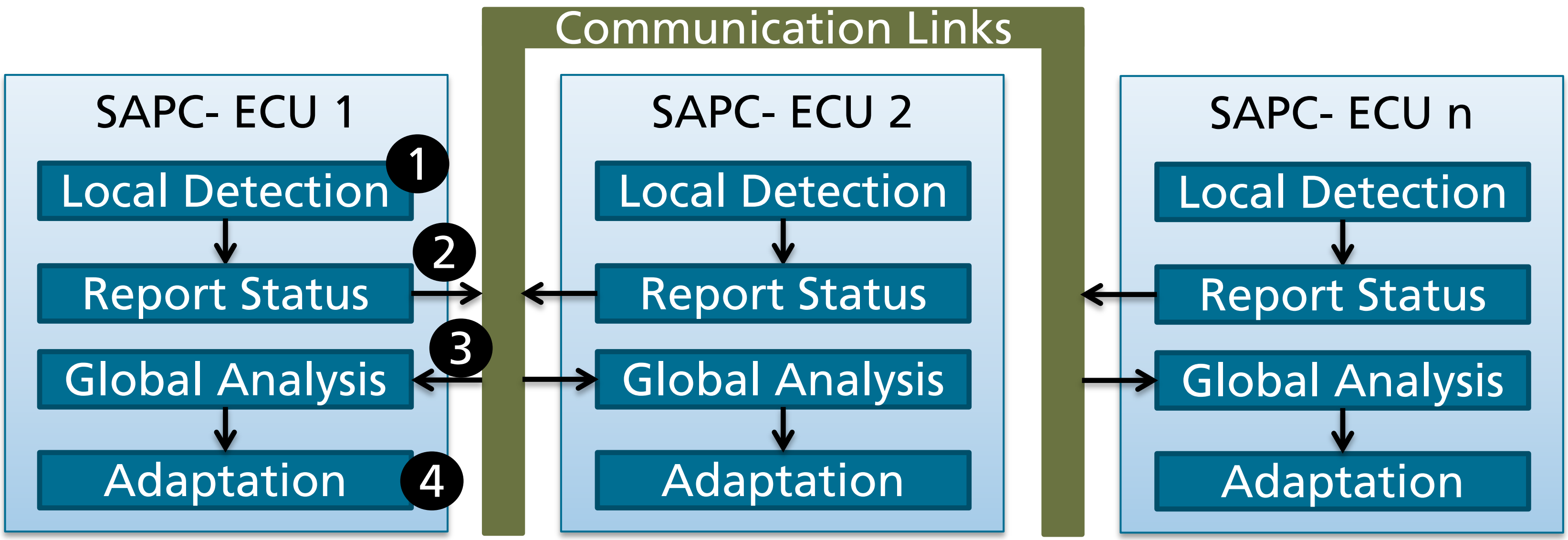
# Runtime Implementation in AUTOSAR

- Reuse of reconfiguration logic by multiple functionalities (SEooC)
- Generic (sub)system-wide management of failure states (SAPC)



# Details: Runtime Reconfiguration Module (SAPC)

- Decentralised awareness of system state (e.g. hardware failures)
- Synchronised monitoring and reconfiguration between ECUs
- Deterministic failure management & globally consisted state
- Global system state based on states of individual SWC instances



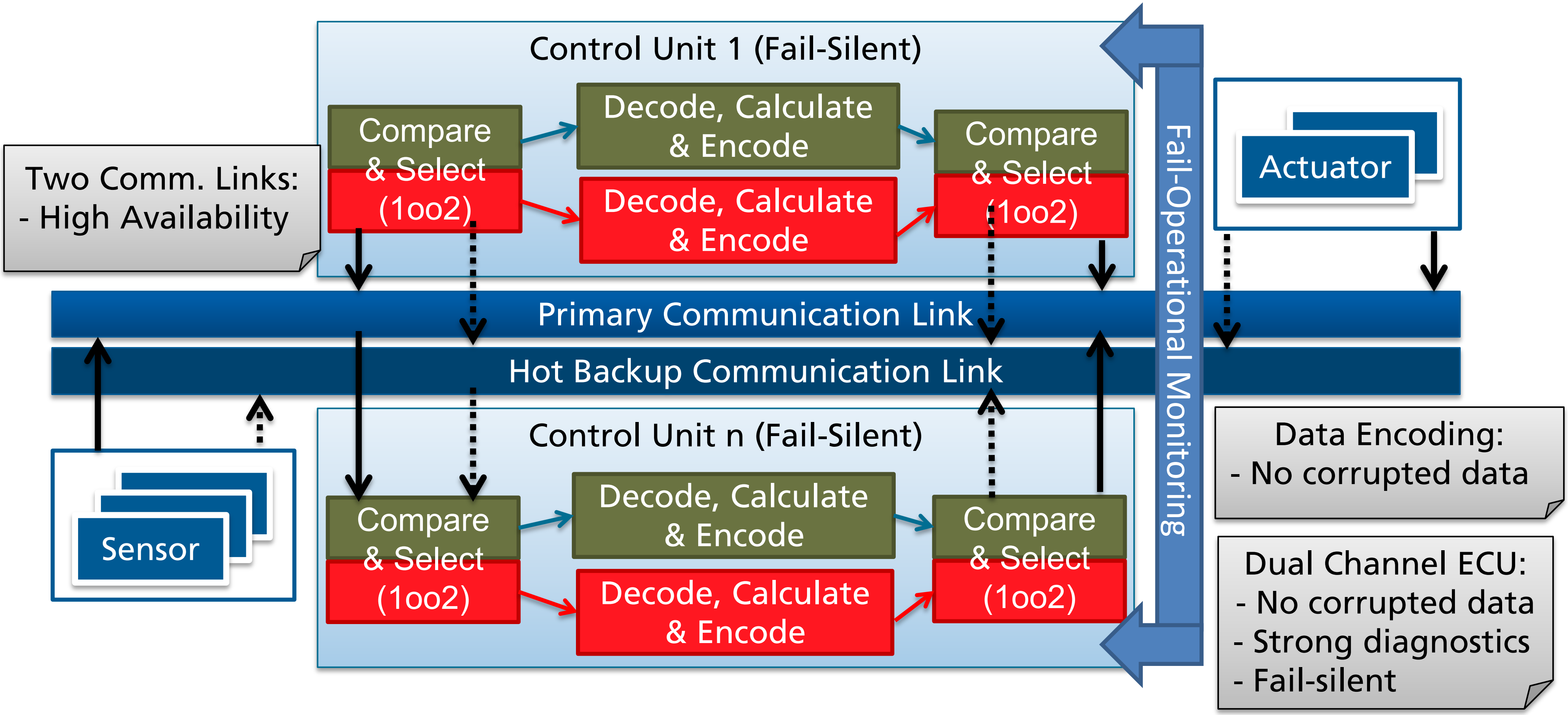




Fraunhofer
ESK

# Example for Fail-Operational Hardware Architecture

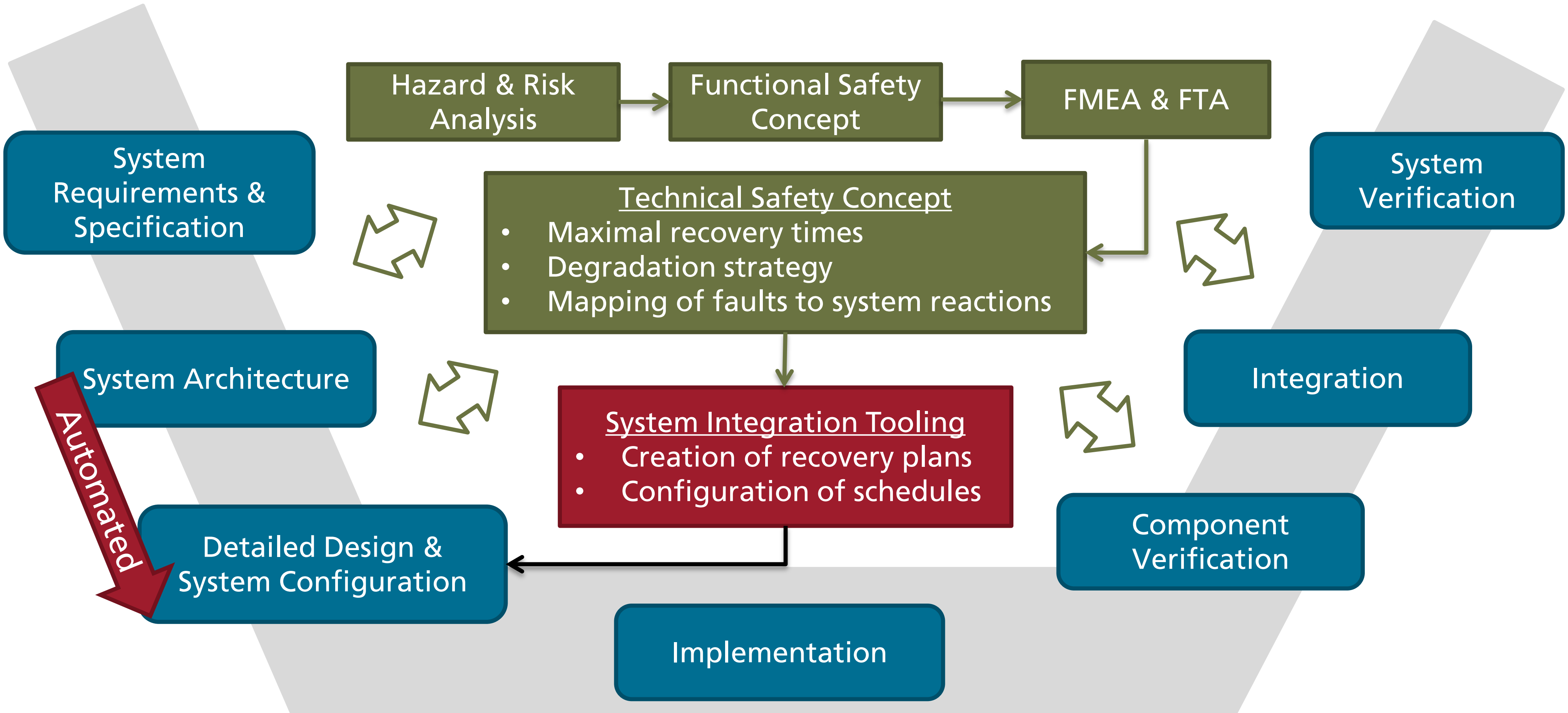
- 1-out-of-2 with strong diagnostics (1oo2D)






Fraunhofer ESK

# Summary: What Can Be Automated?








Fraunhofer ESK

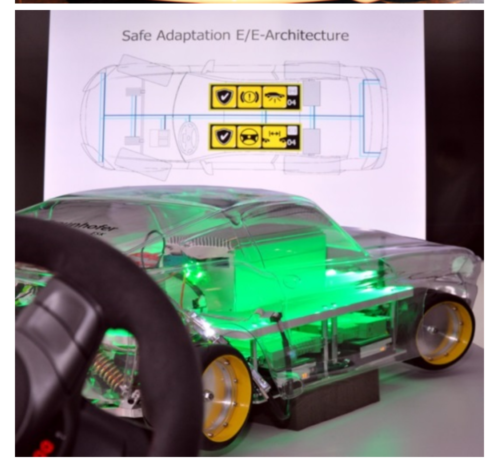
# Summary

- **Error-prone & labour-intensive system design (timing & availability)**

- **Automated synthesis of fault-tolerant control systems**
  - Schedule for multiple resources (CPU core, ECUs, bus, …)
  - Consideration of graceful degradation & failure modes
  - Guarantee of correct timing behaviour

- **Benefits**
  - Quality of design process (less human errors)
  - Development cost, variant diversity & time to market
  - Pre-verifiable configuration for operational modes
  - Modular reuse of individual process steps & technologies

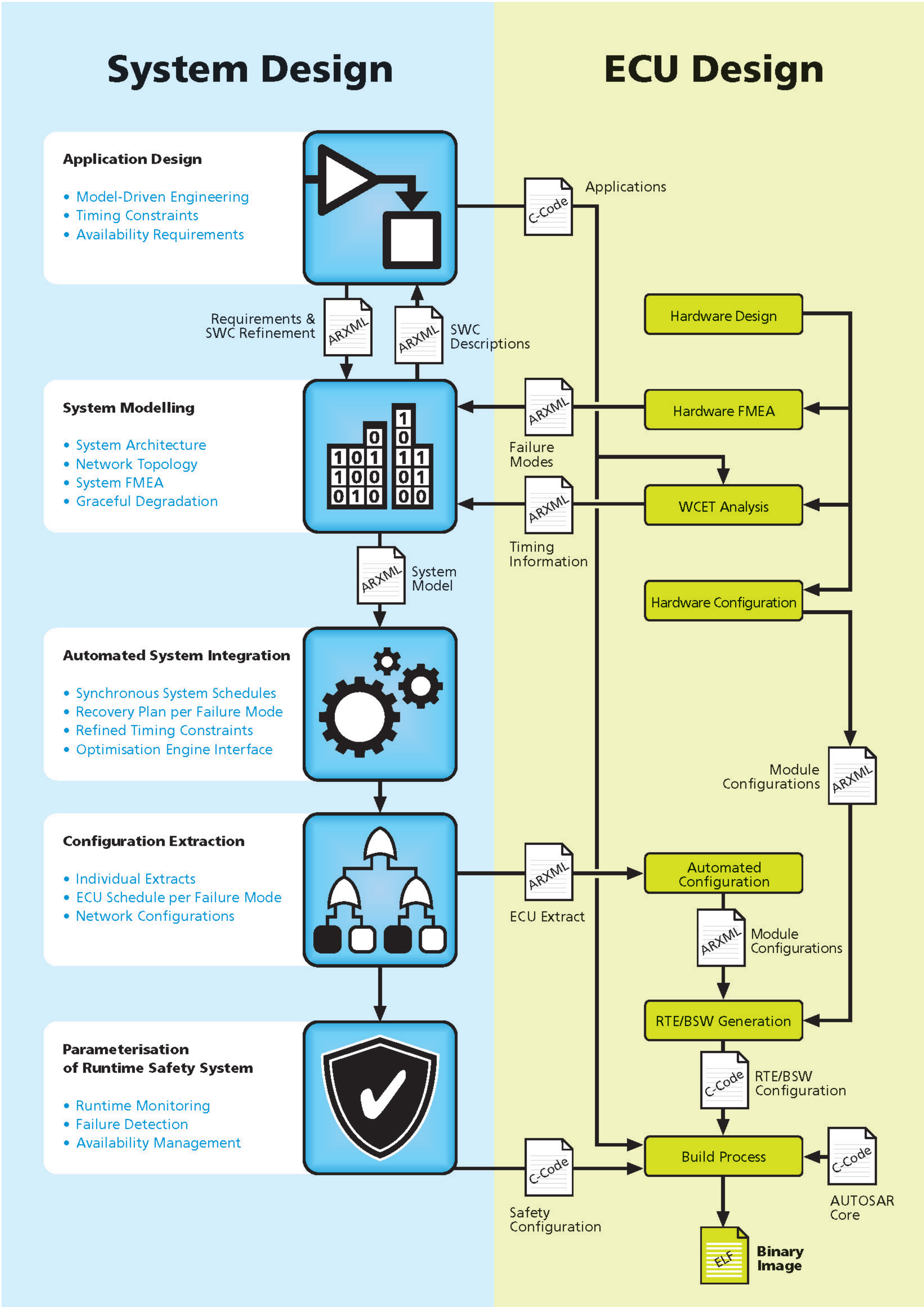
- **Proof of concept in model & full-scale vehicles**






Fraunhofer ESK

# Appendix: Automated Integration








Fraunhofer ESK