DSN 2006

Workshop on Architecting Dependable Systems (WADS)

Fault-tolerant Smart Sensor Architecture for Integrated Modular Avionics

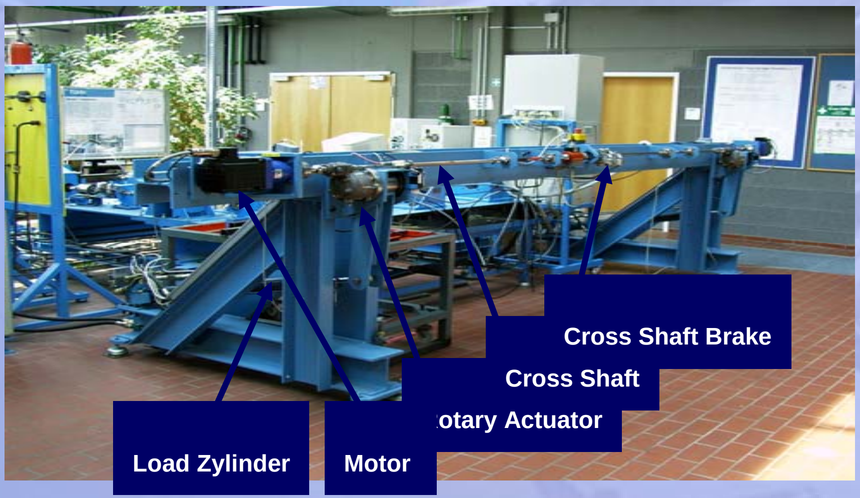
Stefan Schneele, Klaus Echtle, Josef Schalk

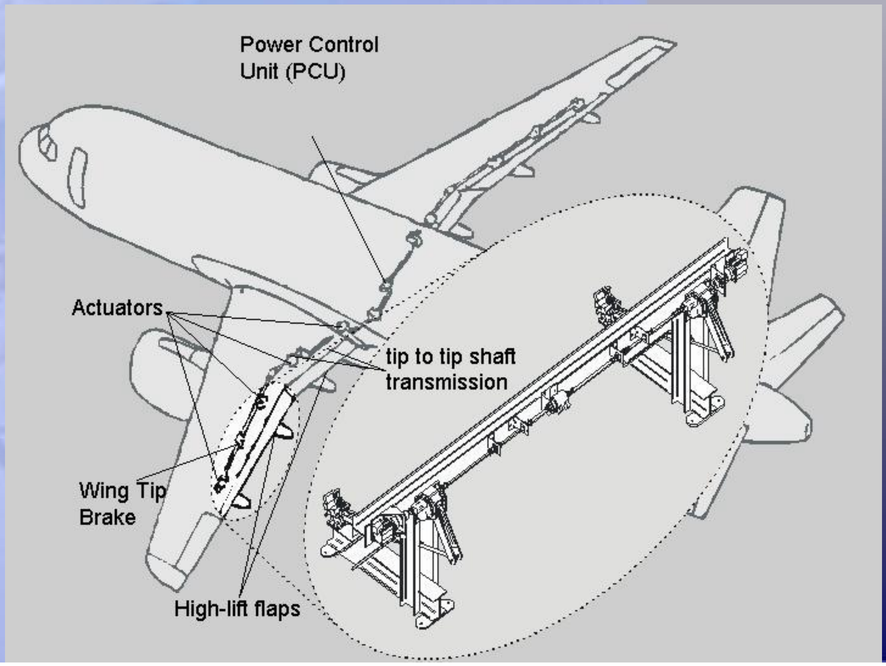
June 27th, 2006

DECOS – Application Aerospace

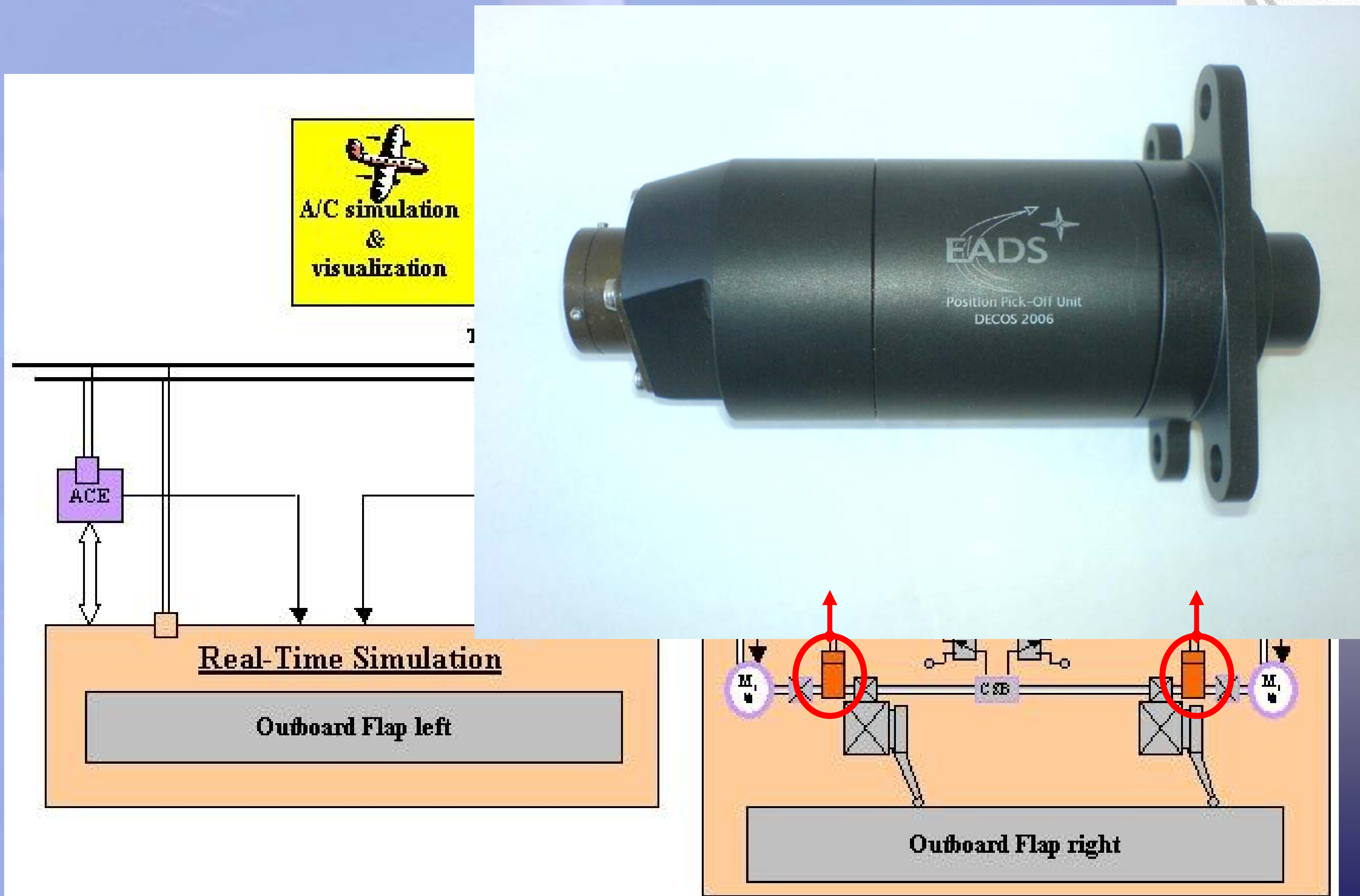
SP6-Approach: Electronically Synchronized Flaps

- A (time-triggered) bus system will be used between the flap panels instead of the mechanical shaft
- A System Control Unit (SCU) has to control and monitor the time-triggered communication, instead of the Central Motor Unit
- For redundancy reason each flap panel will be powered by 2 Motors
- Cross Shaft Brake to hold system
- Development and usage of new, smart sensors, interfaces and gateways supporting TTA





Application Aerospace - Work Share



The Challenge

- Build a smart sensor that meets:

- Functional Requirements
  - Reliable
  - Higher Resolution (90° → ±0,1° (6 ‘))
  - New Single-Turn coverage
  - Built-In Test capability
- Project Requirements
  - Use DECOS Tools & Methods
  - Integrate DECOS design approach
  - Use DECOS Hardware
- Industrial Requirements
  - Efficient (costs, weight, size, Integration, complexity)
  - Airworthy

Proof of Airworthiness I

- **Reliability Modeling and Analysis of fault tolerant Flap Control System based on the to be developed DECOS technology**
  - HW, SW and communication components
  - Fault tolerant structures: redundancies for fault diagnosis and reconfiguration purposes
  - Signal diversity for highly fault tolerant flap control system
  - Reliability analysis and evaluation of flap control system models based on different top events
  - Probabilities: top events satisfied / not satisfied
  - Degraded system states:
    - ‘fail ^n -operational’ capabilities
    - probabilities of degraded system states

Proof of Airworthiness II

- **Redundancy Management of fault tolerant Flap Control System based on the to-be-developed DECOS technology**
  - Redundancy Management: Assessment of different reconfiguration processes based on a hybrid system model (reliability block diagram and finite state machine).

Identify benefits & risks of system evolution by using DECOS technology

Safety Requirements

- **The US Federal Aviation Regulations and the European Joint Aviation Requirements provide detailed system safety regulations:**
- degraded positioning rate of a specific control surface as consequence of one failed channel.

$$\lambda_{FC1} < 10^{-3} \ \ per\ hour\ of\ flight\ (FH) \qquad (1)$$

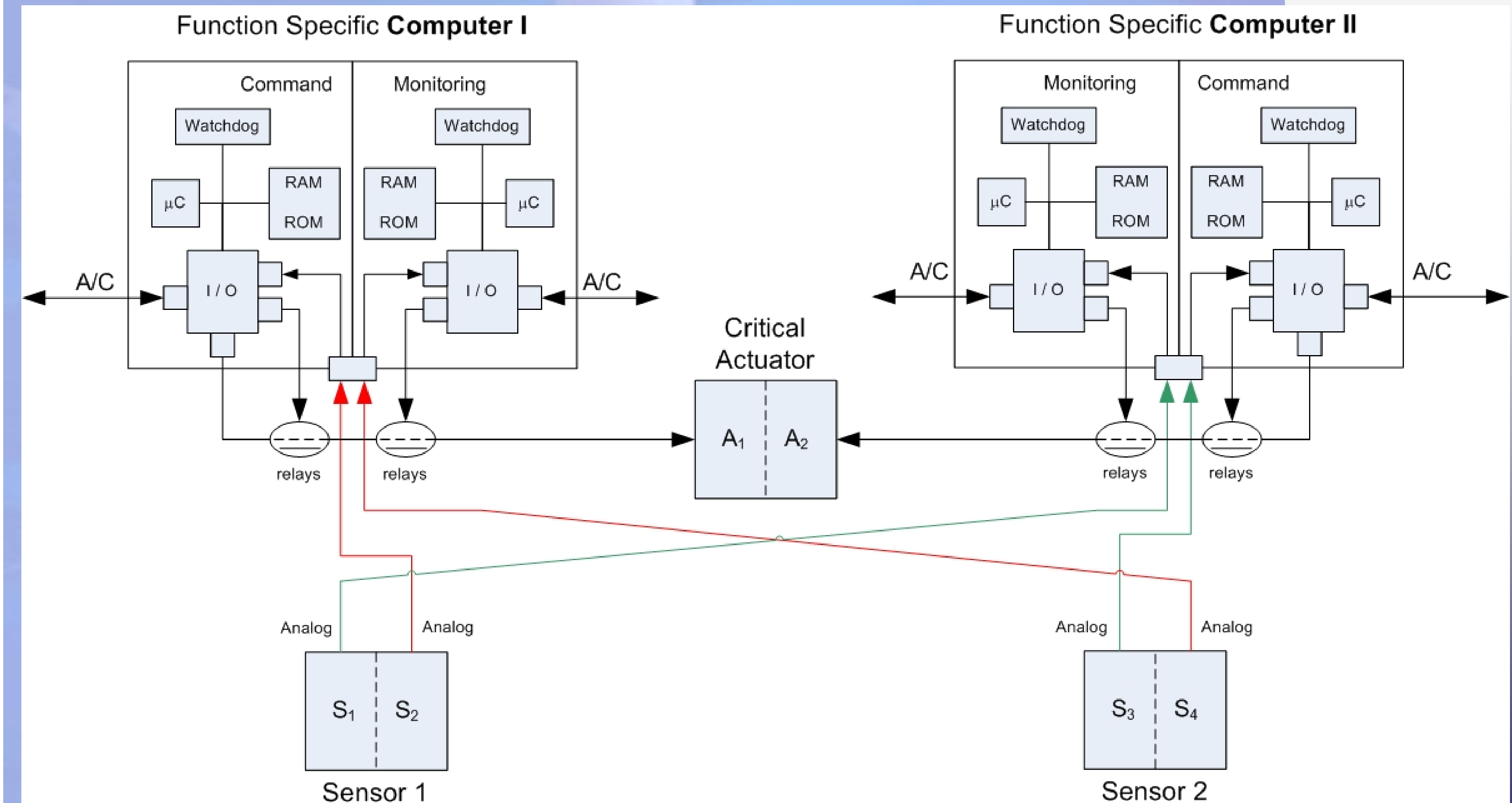
- The second failure case of our interest is loss of operation of a specific control surface as consequence of failures in both channels.

$$\lambda_{FC2} < 10^{-6} \ \ per\ hour\ of\ flight\ (FH) \qquad (2)$$

- fault regions SFRx:

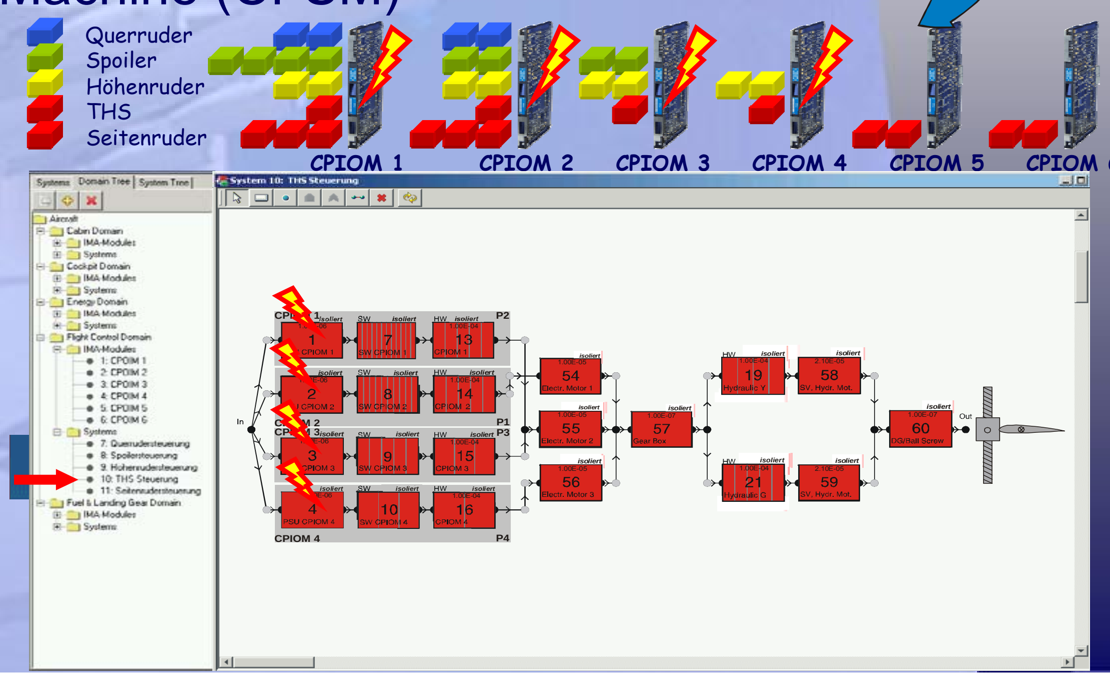
$$SFR_x = \{sensor_x, connector_x, analogline_X, connector_x\} \qquad (3)$$

Evolution of System – Federated Architecture



The Tool - Syrelan

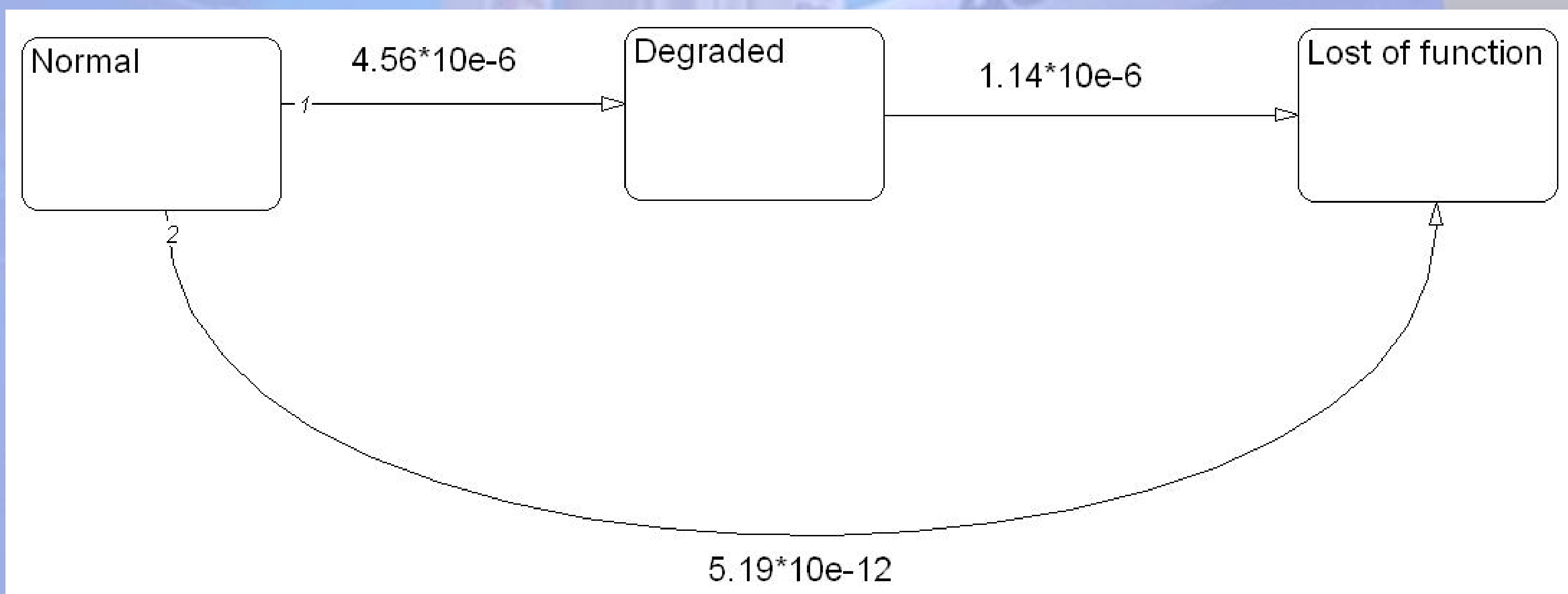
- Developed by Dominick Rehage, University Hamburg-Harbug
- Supports:
  - Reliability Block Diagram (RBD)
  - Concurrent Finite State Machine (CFSM)
- For:
  - Reliability Analysis
  - Degradation Analysis



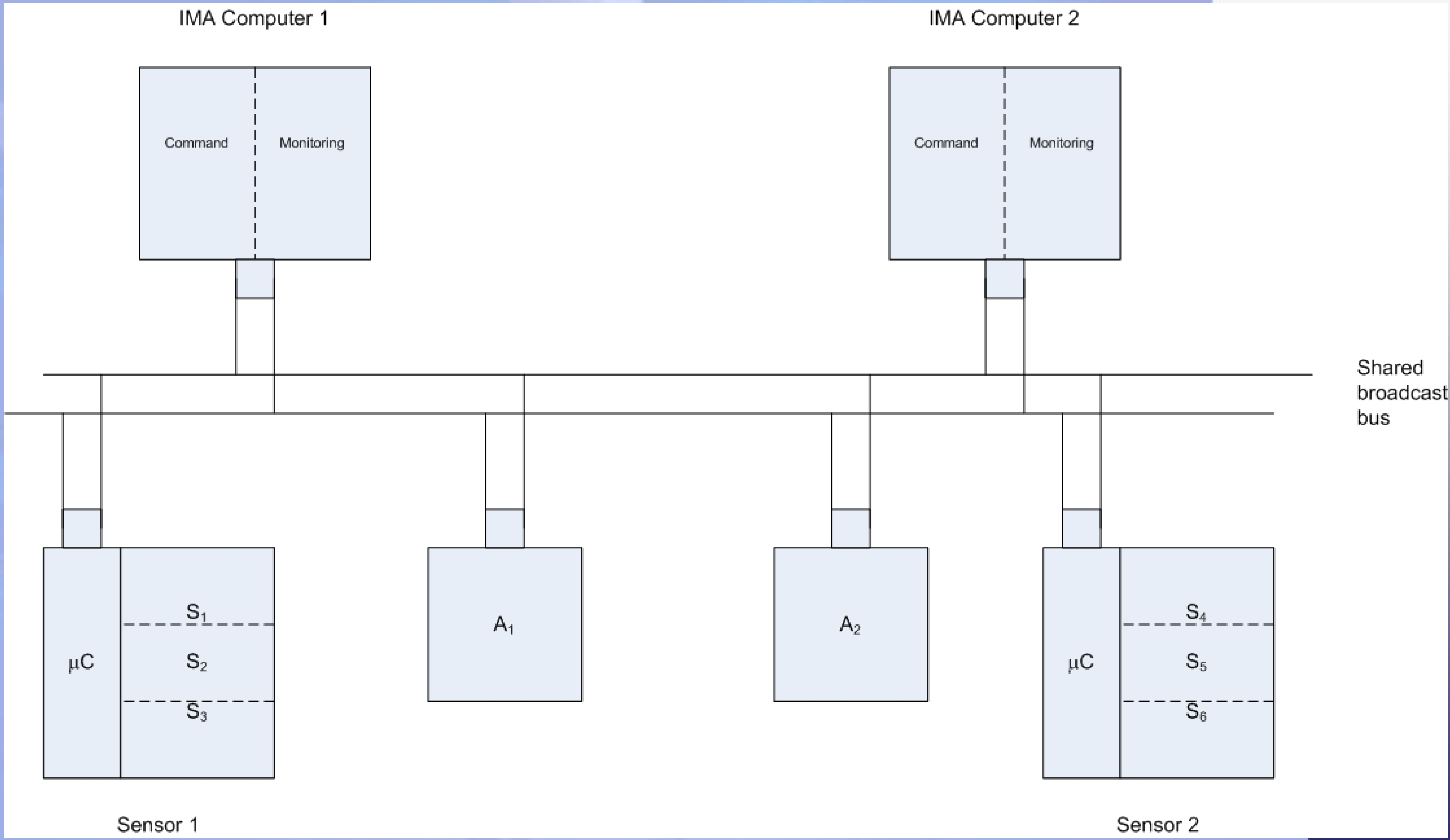
Failure Modes of Conventional Sensor

- Failure Rates of components:

$$\lambda_{Sensor} = 10^{-6}; \lambda_{Analog} = 3.94 * 10^{-8}; \lambda_{plug} = 4.99 * 10^{-8} \quad (4)$$



Evolution of System – Integrated Architecture



Design Rules for Smart Sensors – Common Cause Failures

Although the structural reliability numbers of smart sensors can meet the ones conventional systems

→ additional failure modes are introduced to the system (COMPLEXITY).

→ Risk of common modes.

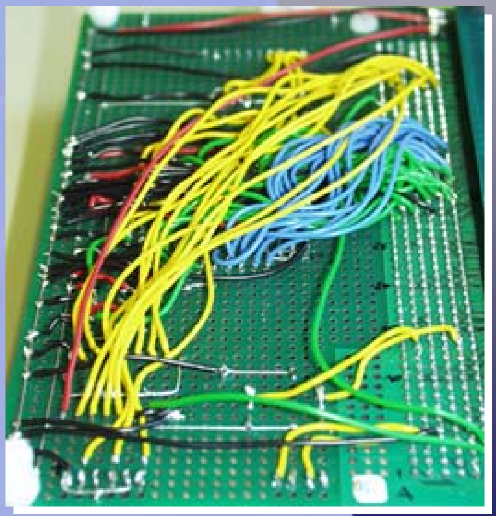
→ For worst-case consideration, the β-Factor - representing the chance of common cause failures in different channels – is set to 0.4.

→ Do not receive any data,

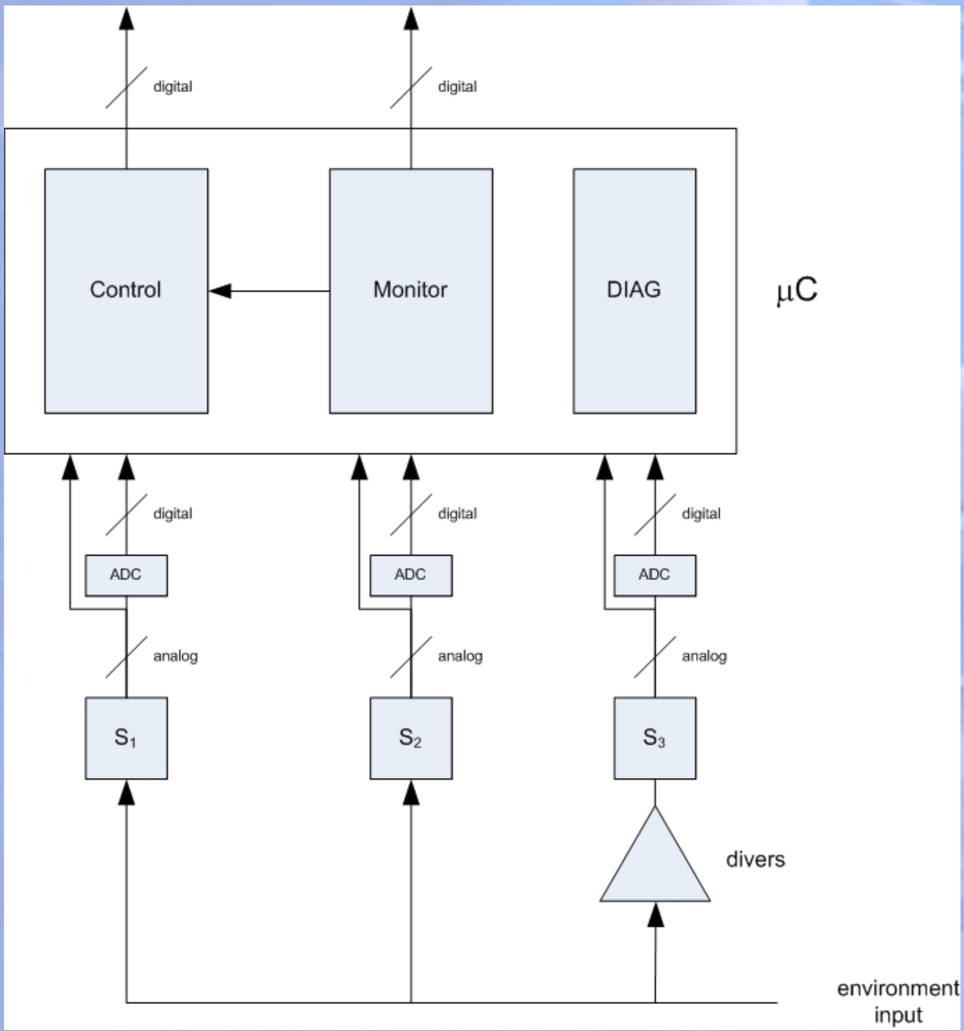
→ very few numbers of operational modes

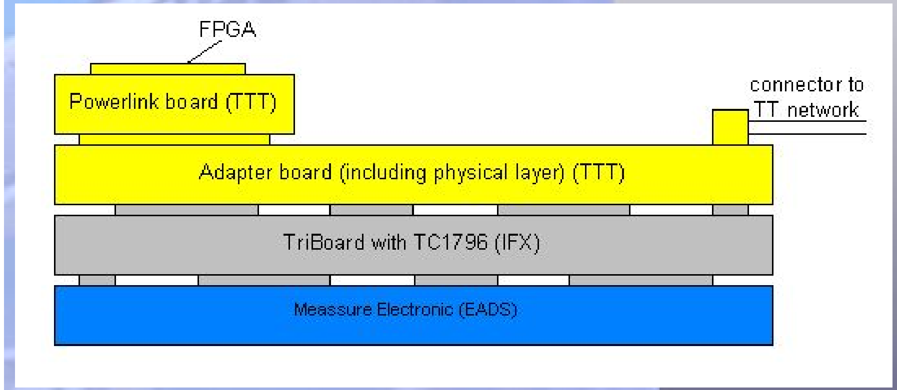
→ suitable simple composition of components

→ Everything should be made as simple as possible, but not simpler.



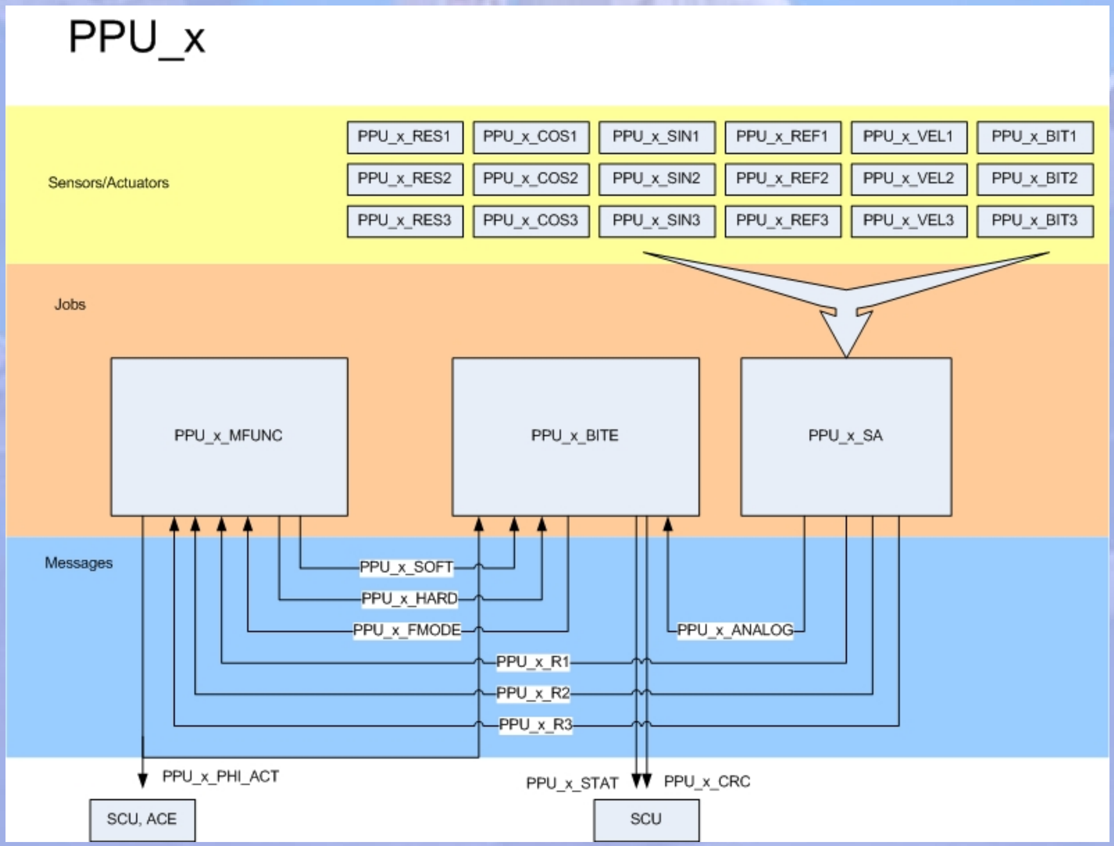
Smart Sensor - Components





Position Pick-Off Unit – Software Design

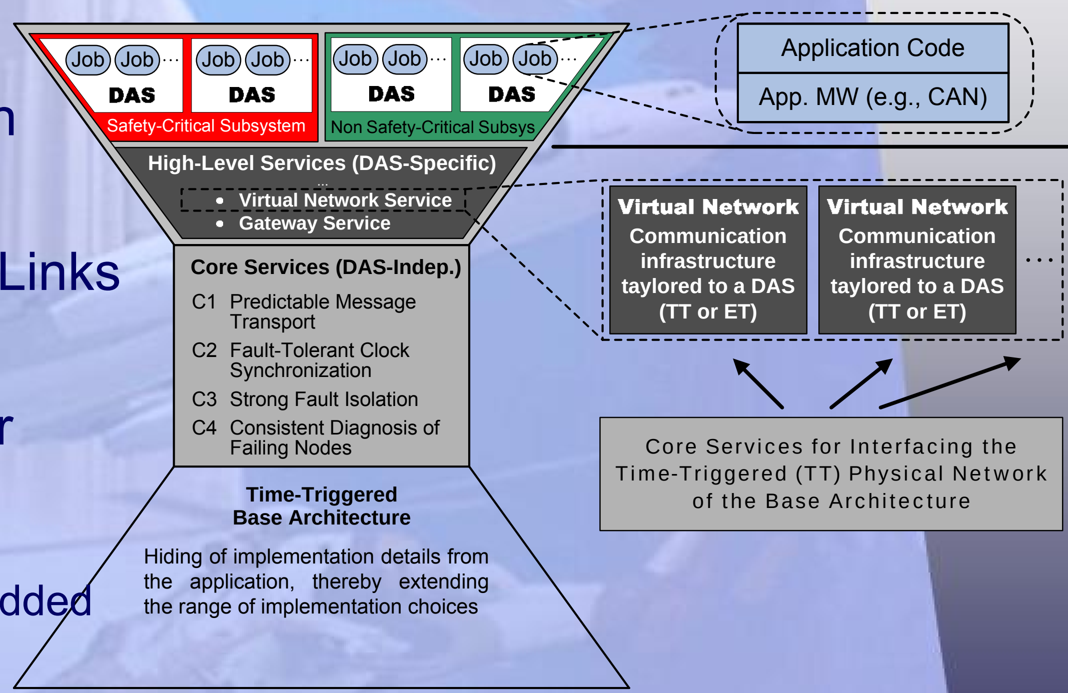
- To achieve fail-safe behavior, usually failure masking with n-out-of-m failure masking is used → efficiency constraints
- The presented architecture can only provide two different values. Therefore an approach is selected, which is based on an online selftest for failure detection.



 Stefan Schneele June 2006

DECOS - Integrated Distributed Execution Platform

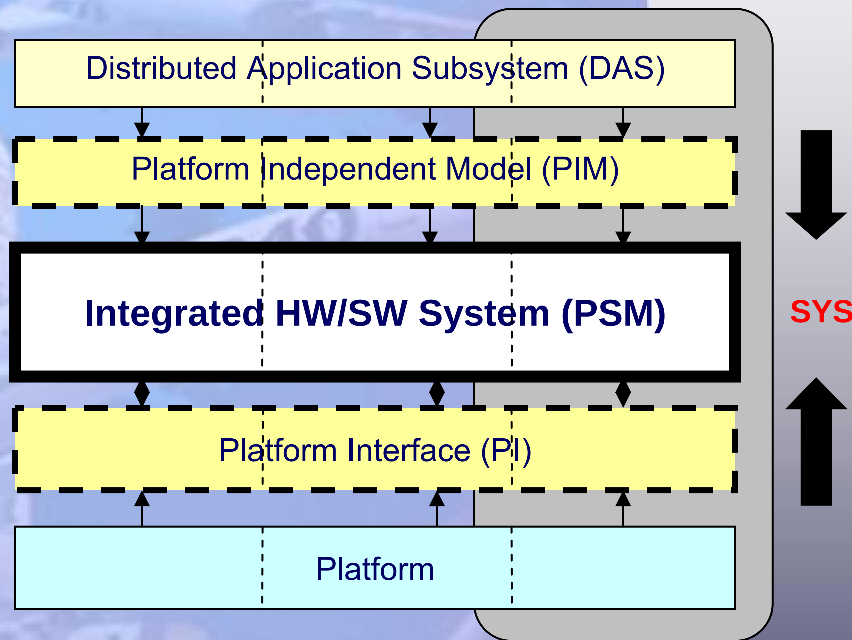
- Specification of Requirements and Design of:
  - Encapsulated Execution Environment
  - Virtual Communication Links and Gateways
  - Platform Interface Layer



- DECOS = Dependable Embedded Systems and Components

DECOS - Methods and Tools

- Modeling Distributed Application Subsystems
- Specification of the Platform Independent Model (PIM)
  - PIM Metamodel,
  - Design methodology
- Specification of the Resource Layer
  - Hardware specification model
- Software-Hardware Integration
  - Specification of PSM development tool



DAS: **D**istributed **A**pplication **S**ubsystem
PIM: **P**latform **I**ndependent **M**odel
PSM: **P**latform **S**pecific **M**odel
PI(L): **P**latform **I**nterface

 Stefan Schneele June 2006

µ-Controller – single point of failure

- Modern µ-Controllers provide suitable operation life-time of up
- to 20 years in controlled temperature racks.
- Concerning the use in extremely harsh environment with high amplitude

  of temperature and pressure chances, we expect:

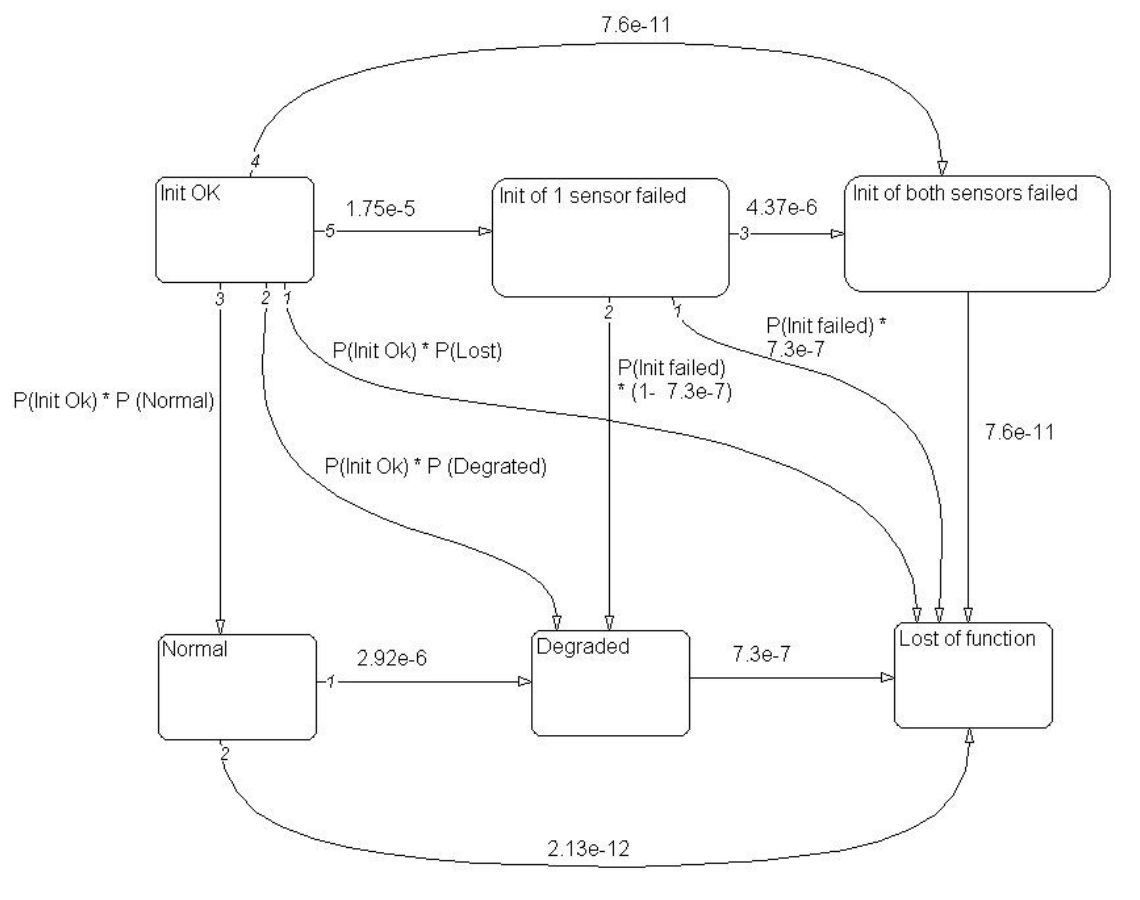
$$\lambda_{Controller}\ [1/Fh] = 1,46 * 10^{-6}\ [7]$$

- Self-checks on power-on can be interpreted as frequent maintenance intervals, making this failure rate plausible.
- This maintenance interval should be equal to the mission time.
- → Redundancy cause of efficiency constraints not a suitable approach for smart sensing devices

Failure Modes of Smart Sensor - Hardware

- Failure Rates of components:

$$\lambda_{Sensor} = 2 * 10^{-6}; \lambda_{ADC} = 2.7 * 10^{-7}; \lambda_{Osz} = 5 * 10^{-6} \quad (5)$$



More states because of Initialization

Benefit of DECOS Technology

- **For Reliability Analysis, Smart Sensor must fulfill:**
  - Fail-safe behavior
  - appearance as an atomic unit
  - No failure propagation

  → Guaranteed by DECOS node design (to be proofed)

- **Minimization of Design faults and handling of complexity**

  →Addressed by Model based and Hardware Independent system design approach

- **Partitioning in time and space domain**

  → Addressed by Encapsulated Execution Environment and Time-Triggered Protocol

Conclusion

- the novel DECOS architecture is applied to a smart sensor design.
- The justification of the sensor concept was given on a structural level.
  – sensor design meets the reliability constraints
- a remarkably small subset of components can fulfill both efficiency and reliability constraints
- This concept is implemented in

real hardware, and evaluated on a realistic test-bench.

Thank you !