Technische Universität Wien

A Maintenance-Oriented Fault Model for the DECOS Integrated Diagnostic Architecture

P. Peti, R. Obermaisser, A. Ademaj, H. Kopetz

TU Vienna

Real-Time Systems Group

Overview

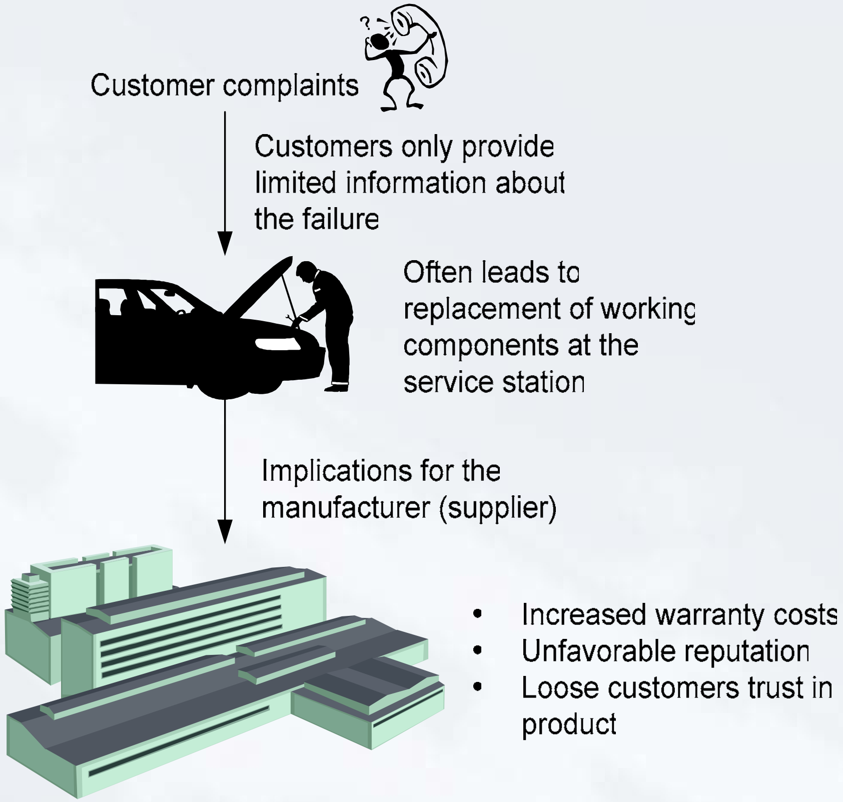
- Introduction
- Hardware/software faults
- DECOS integrated architecture
- Maintenance-oriented fault model
- Maintenance actions
- Conclusion

Introduction

- Effective diagnostic systems stay behind recent increase of electronic systems
- Today the service technician has to rely upon imprecise information
- This results frequently in the replacement of working components
- Emerging X-by-wire solutions will have a lasting effect on the mechanics work
- Statistics: the number one breakdown cause for cars are electronic problems (negative media coverage)

Trouble-Not-Identified Phenomenon

- Trouble-not-Identified phenomenon
  - Increasing number of component failures cannot be traced back to a fault
  - Replacement of correct components
  - Defective component remains unchanged
- Affecting both automotive and avionics domain
- Increased warranty costs
- Image of OEM



Customer complaints

Customers only provide limited information about the failure

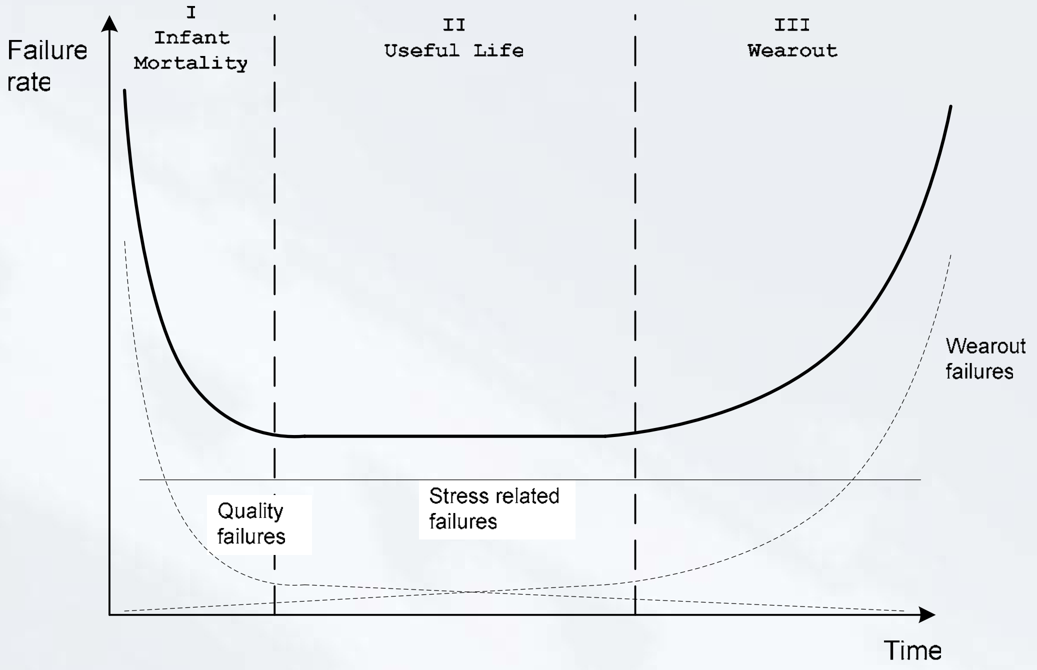
Often leads to replacement of working components at the service station

Implications for the manufacturer (supplier)

- Increased warranty costs
- Unfavorable reputation
- Loose customers trust in product

Hardware: Shift in Technology

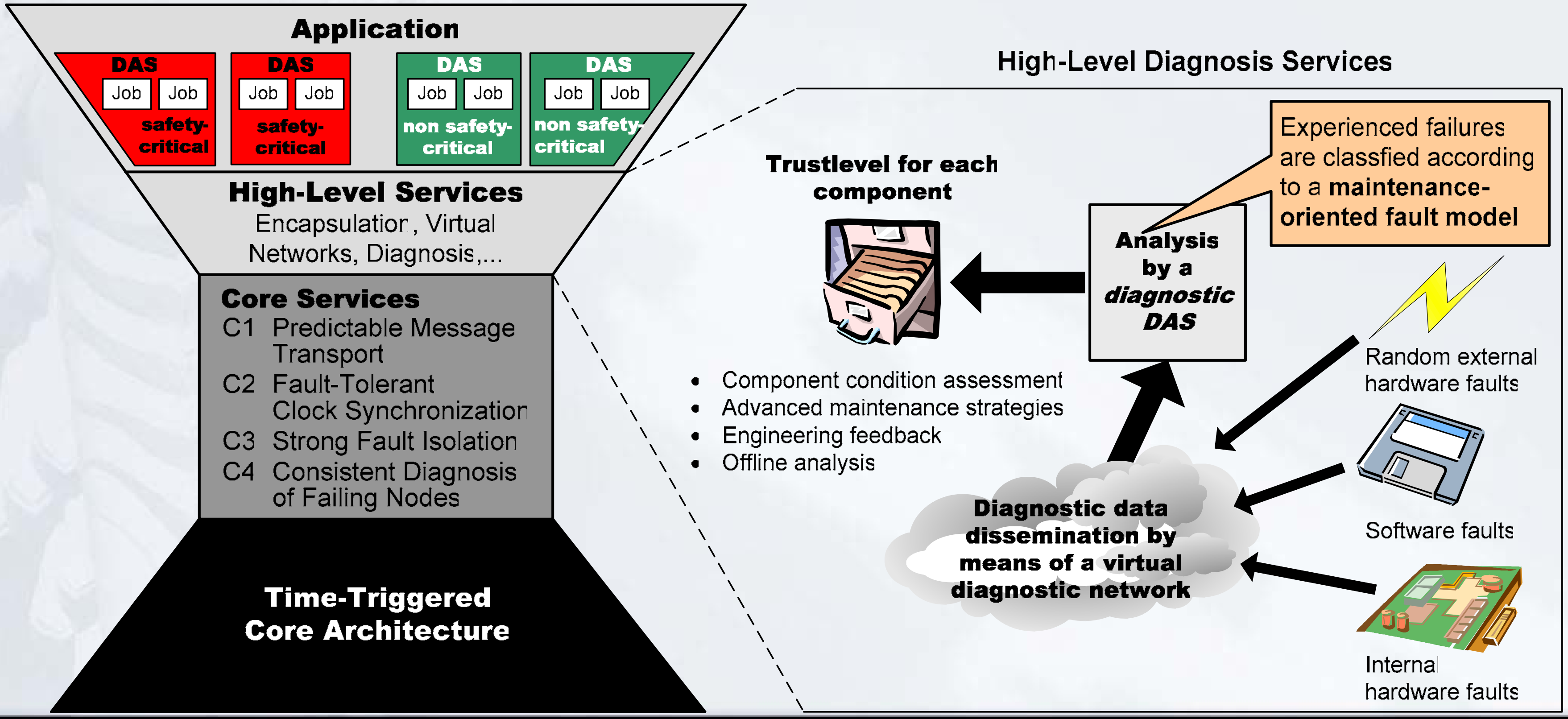
- Low permanent failure rate (significant improvements)
- Increasing rate of transient failures due to
  - Shrinking geometries
  - Process variations
  - Manufacturing residuals
- Need to focus on transients!



Software: Increase in Complexity

- Increase in inherent application complexity
- Software faults are causing numerous callbacks
- Avoid additional platform-induced complexity
  - Architectures with error containment
  - High-level services that facilitate independent application development
- Diagnosis typically part of application

DECOS Integrated Architecture



Application

DAS Job Job safety-critical

DAS Job Job safety-critical

DAS Job Job non safety-critical

DAS Job Job non safety-critical

High-Level Services

Encapsulation, Virtual Networks, Diagnosis,...

Core Services

C1 Predictable Message Transport

C2 Fault-Tolerant Clock Synchronization

C3 Strong Fault Isolation

C4 Consistent Diagnosis of Failing Nodes

Time-Triggered Core Architecture

High-Level Diagnosis Services

Trustlevel for each component

- Component condition assessment
- Advanced maintenance strategies
- Engineering feedback
- Offline analysis

Analysis by a *diagnostic DAS*

Experienced failures are classfied according to a **maintenance-oriented fault model**

Diagnostic data dissemination by means of a virtual diagnostic network

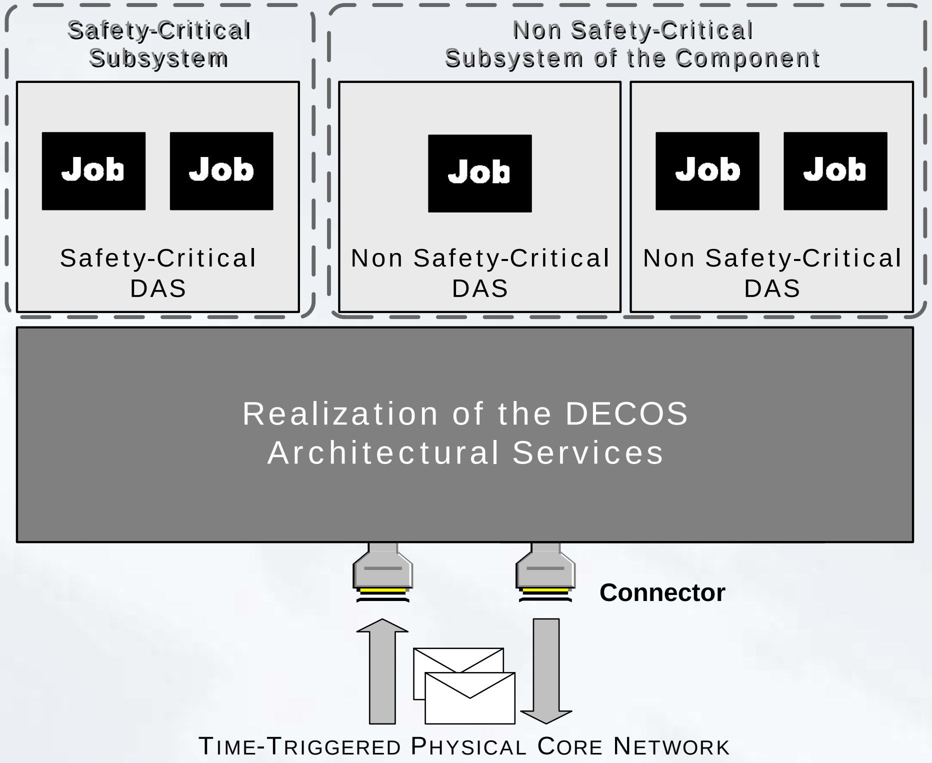
Random external hardware faults

Software faults

Internal hardware faults

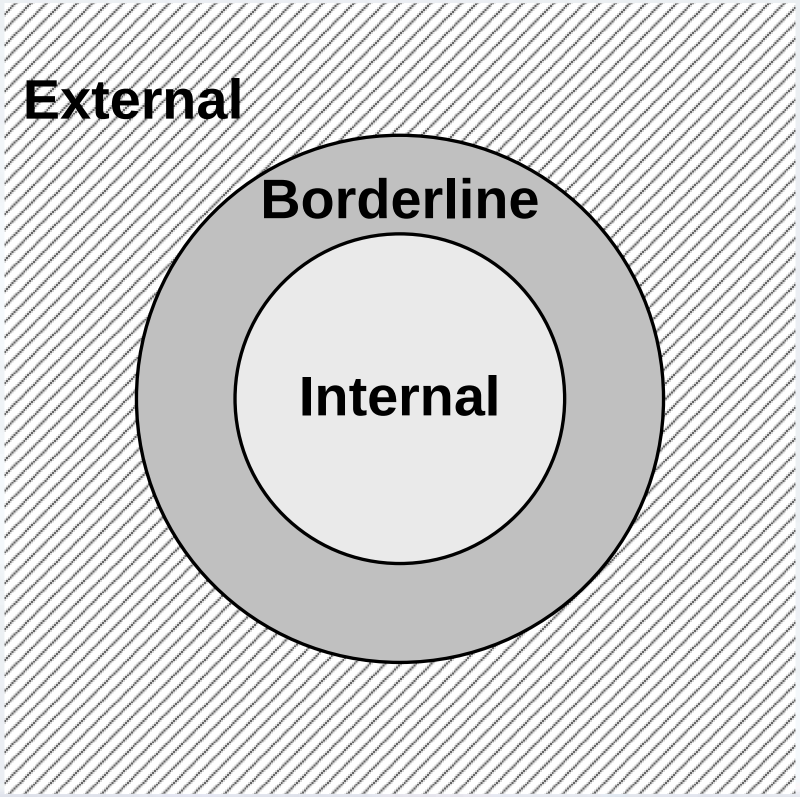
The DECOS Component Model

- Component is a self-contained composite hardware/software subsystem and hosts
  - Subsystems of different criticality
  - Jobs (= software modules) of the Distributed Application Subsystems


Safety-Critical Subsystem
Non Safety-Critical Subsystem of the Component
Job
Job
Safety-Critical DAS
Job
Non Safety-Critical DAS
Job
Job
Non Safety-Critical DAS
Realization of the DECOS Architectural Services
Connector
TIME-TRIGGERED PHYSICAL CORE NETWORK

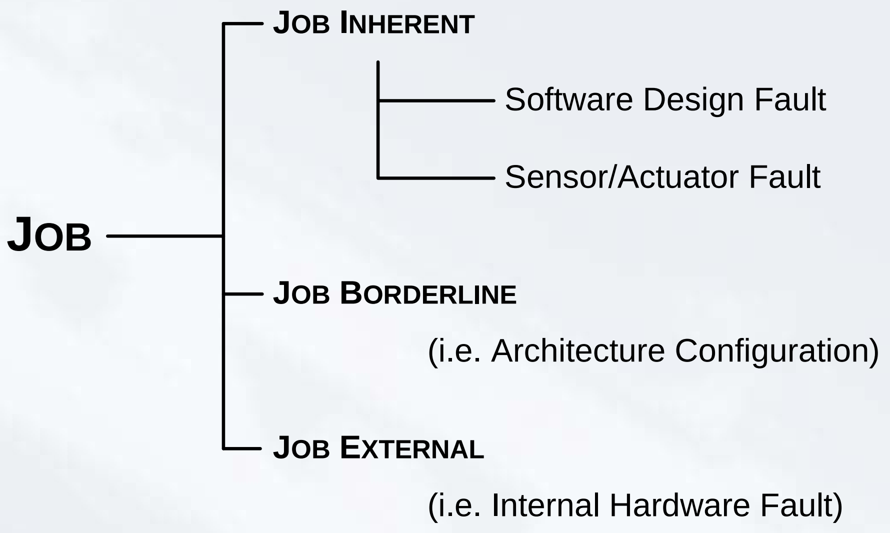
Maintenance-Oriented Fault Model: Hardware Faults

- Component as unit of replacement for hardware faults
  - – Internal (e.g., crack in PCB, faulty processor)
  - – Borderline (e.g., Connector failures)
  - – External (e.g., EMI)



Maintenance-Oriented Fault Model: Software Faults

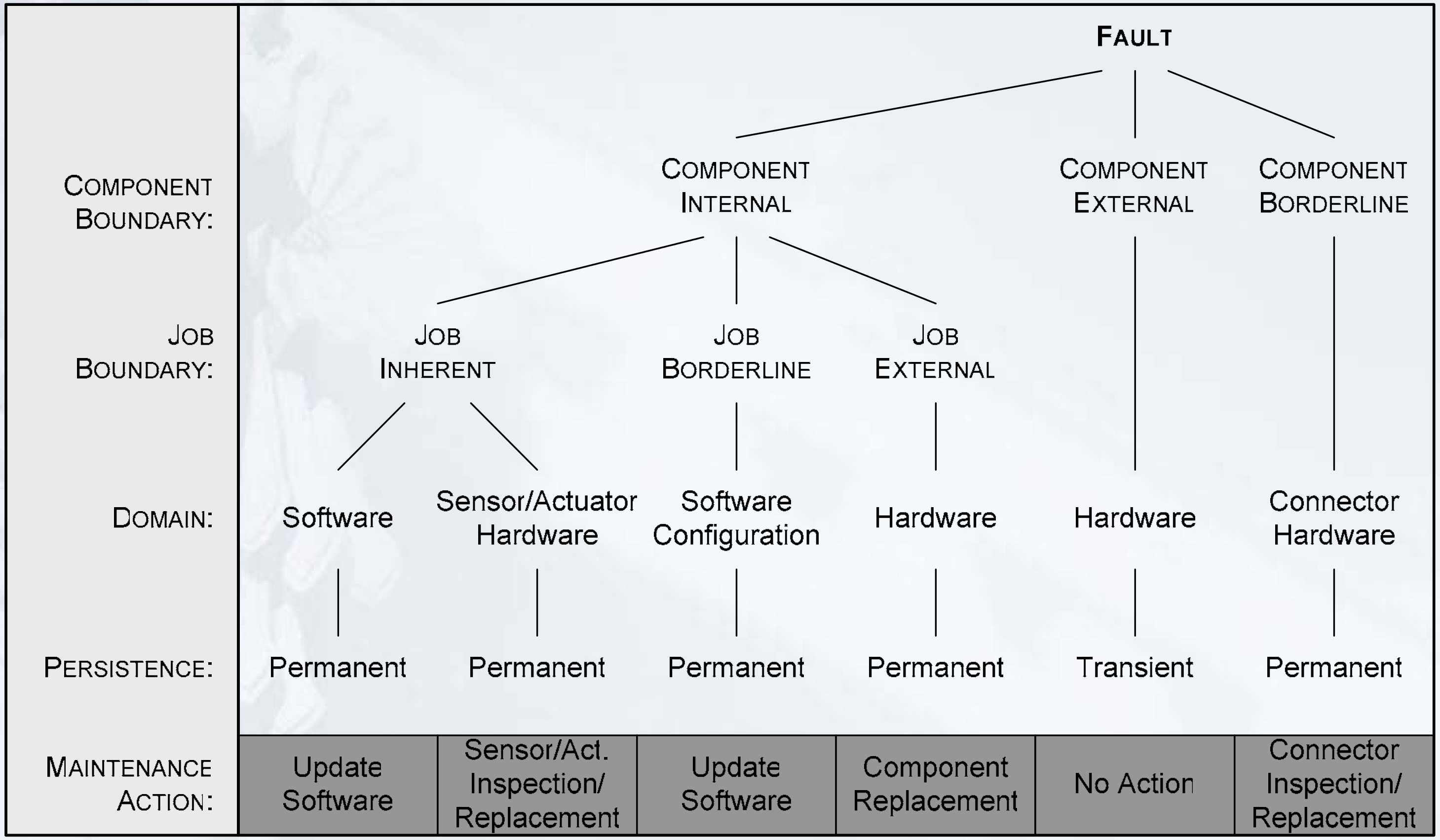
- Job as unit of replacement (update) for software faults:
  - Inherent
  - Borderline
  - External



Assumptions

- The **permanent failure rate** of FRU with respect to hardware faults is considered to be in the order of 100 FIT, i.e. about 1000 years
- The **transient failure rate** of a FRU with respect to hardware faults is assumed to be in the order of 100.000 FIT, i.e. about 1 year
- **Correlated FRU failures**, i.e. a fault affecting more than one FRU at the same time, are assumed to be experienced within a bounded interval of time. Example: according to the ISO 7637 standard the duration of an EMI burst is in the order of 10 ms.
- **Software Faults Distribution**. We assume that safety-critical jobs are certified to the necessary degree and thus free of software design faults. In case of non safety-critical jobs, we assume that a minority of the deployed software FRUs is causing the majority of software related failures during operation [Fenton 2000].

Replacement Strategy



	FAULT					
COMPONENT BOUNDARY:	COMPONENT INTERNAL				COMPONENT EXTERNAL	COMPONENT BORDERLINE
JOB BOUNDARY:	JOB INHERENT		JOB BORDERLINE	JOB EXTERNAL		
DOMAIN:	Software	Sensor/Actuator Hardware	Software Configuration	Hardware	Hardware	Connector Hardware
PERSISTENCE:	Permanent	Permanent	Permanent	Permanent	Transient	Permanent
MAINTENANCE ACTION:	Update Software	Sensor/Act. Inspection/ Replacement	Update Software	Component Replacement	No Action	Connector Inspection/ Replacement

Conclusion

- Maintenance-oriented fault model
- We stop “fault-error-failure” chain at Field Replaceable Unit (FRU) level
- Conceptual foundation of the DECOS online diagnostic architecture
- Suitable for both integrated and federated architectures
- Definition of a corresponding maintenance action for each fault class