The Diagnostic Architecture of the PEGASUS Project Car

P. Peti, R. Obermaisser, H. Paulitsch
Vienna University of Technology

Real-Time Systems Group

Overview

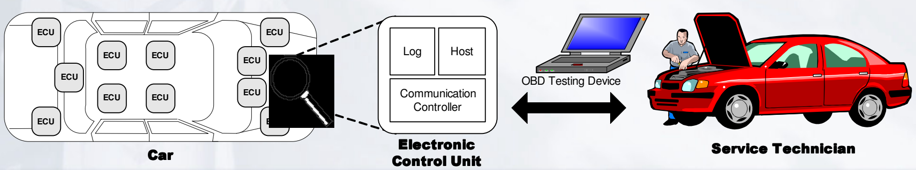
- Introduction and Problem Definition
- Today's Automotive Maintenance
- Requirements for a Future Diagnostic Solution
- Overview on the Diagnostic Architecture
- Discussion

Problems

- Effective diagnostic systems stay behind recent increase of electronic systems
- Statistics: the number one breakdown cause for cars are electronic problems (negative media coverage)
- Increasing number of component failures cannot be traced back to a fault
  - Replacement of correct components
  - Defective component remains unchanged
- OEM: Increased warranty costs and image problems

Today's Automotive Maintenance

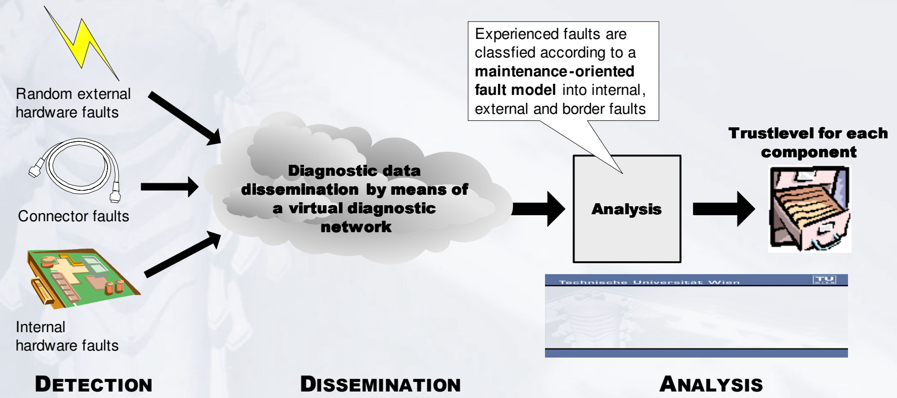
- In case of failure
  - Typically only local information is stored (making analysis of correlated failures extremely difficult)
  - Entry into persistent memory (i.e. *freeze frame*)
- Information retrieval via KWP2000 at service station using testing device
- Service technician depends on the accuracy of the information



Requirements

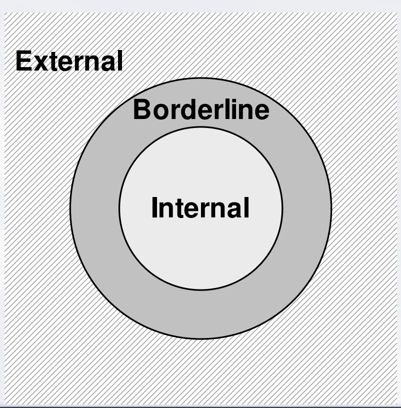
- Focus on transients → Online diagnosis for maintenance
- Detection of correlated failures → Mechanism operating on distributed state in order to trace correlated failures
- Assessment of fault-tolerance mechanisms → No addendum solution at application level
- Avoidance of probe effect → No additional hardware for diagnosis
- Service technician assistance → Substantially improved accuracy by exploiting the error containment capabilities of the underlying time-triggered architecture

Overview on the Diagnostic Architecture



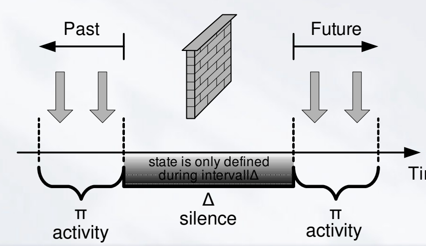
Maintenance-Oriented Fault Model: Hardware Faults

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



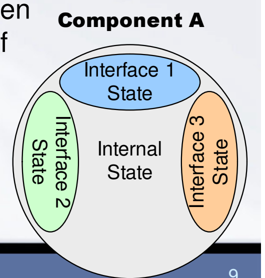
Detection: Distributed State

- In abstract system theory (Mesarovic, 1989), the notion of state is introduced in order to separate the past from the future
- Sparse time model: partitioning of the continuum of time (durations of action and silence)
- Action lattice
- Interval of silence
  - Interval when the distributed state of the system is defined



Detection: Interface State

- A component is a self-contained composite hardware/software subsystem
- A component is used as a building block in the design of a larger system
- The interface state contains the history of the component that is relevant for the future behavior of the component as seen from this interface
- Subset of the state of the component and should be accessible from the interface
- Interface state is defined between the intervals of activity on the sparse time base



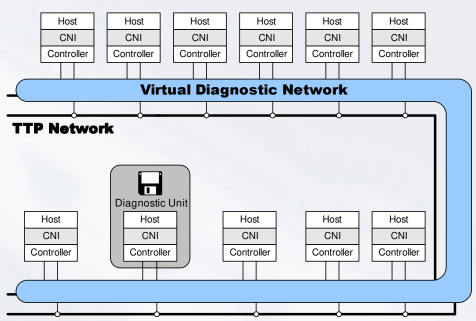
Consequences of Faults on the Distributed State

- Characteristic manifestation of a fault in the time, value and space domain
- We denote such a manifestation on the distributed state a *fault pattern*
- Patterns in interface state that are characteristic for particular classes of faults

Dimension	Fault Patterns	
	Wearout	Massive Transient
Time	increasing frequency as time progresses	approximately at the same time
Space	one component only	multiple components with spatial proximity
Value	increasing deviation from correct value, at the verge of becoming incorrect	multiple bit flips

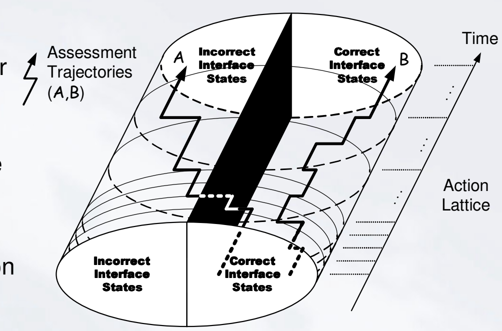
Virtual Diagnostic Network

- Overlay network on top of time-triggered core network
- No probe effects
  - No additional wiring
  - No additional contact points
- Real-time traffic is not compromised in any way



Assessment Strategy

- Analysis process according to maintenance-oriented fault model
- Diagnostic evidence gathered over time allows to detect fault patterns on the distributed state of the system
- By operating on the interface state we
  - Hide the internals of components
  - Need not modify the application software
  - Satisfy industrial requirement for intellectual property protection



Conclusion

- Today we experience significant diagnostic problems
- Diagnostic architecture
  - Maintenance-oriented fault model stops the fault-error-failure chain at the FRU level
  - Detection on interface state of components
    - Systemic
    - Application-specific
  - Virtual diagnostic network introduces no probe effect
  - Online diagnosis on distributed state allows a holistic view on the health state of the system (correlation)