COTS Technology & Issues Automotive

H. Kopetz

June 2003

Outline

- ♦ Introduction
- ♦ What is Different in the Automotive Sector
- ♦ How are Standards Made
- ♦ Approach to Safety
- ♦ Needs of the Automotive Industry
- ♦ Conclusion

Example of Electronics in an Upscale Car:

- Different level of controls:
  - Power train (engine, transmission)
  - Brakes, Suspension
  - Body electronics
  - Multimedia
- Federated Architecture with up to 70 nodes (Electronic Control Units--ECUs) in an upscale car
  - Essentially, every new function requires a new box
- Different networks
  - LIN fieldbus (< 20 kbits/s)
  - CAN (< 500 kbits/s)
  - MOST (Multimedia > 10 Mbits/s)

What is Different in the Automotive Industry?

- ♦ Large number of cars (50 million/year)
- ♦ Minimization of recurring costs in a mass market
- ♦ Very high level of dependability at affordable cost
  - Majority of recalls are hardware related failures
- ♦ Few independent automotive companies in the world
  - Large enough to make their own COTS
- ♦ Attitude: *We own the world* --and in some respects they do
  - Example CAN
  - Convergence Conference on Automotive Electronics
  - Absence of academics at relevant SAE meetings (e.g. Naming)
- ♦ Difficulties when it comes to interfacing with the worldwide information infrastructure: example MOST

Example: MOST Multimedia System

BMW, Daimler Chrysler, Audi, Volkswagen et al. got together to make a

- New automative standard for multimedia communication within the car
- Defined their own silicon chips
- Installed in some upscale models

But

- Conflict with multimedia groups (Firewire) in the consumer industries
- US car manufacturers reluctant to join
- Can a stand-alone multimedia standard survive?

How are COTS Standards Born: CAN

1990ies

Germany: Bosch CAN

French: VAN

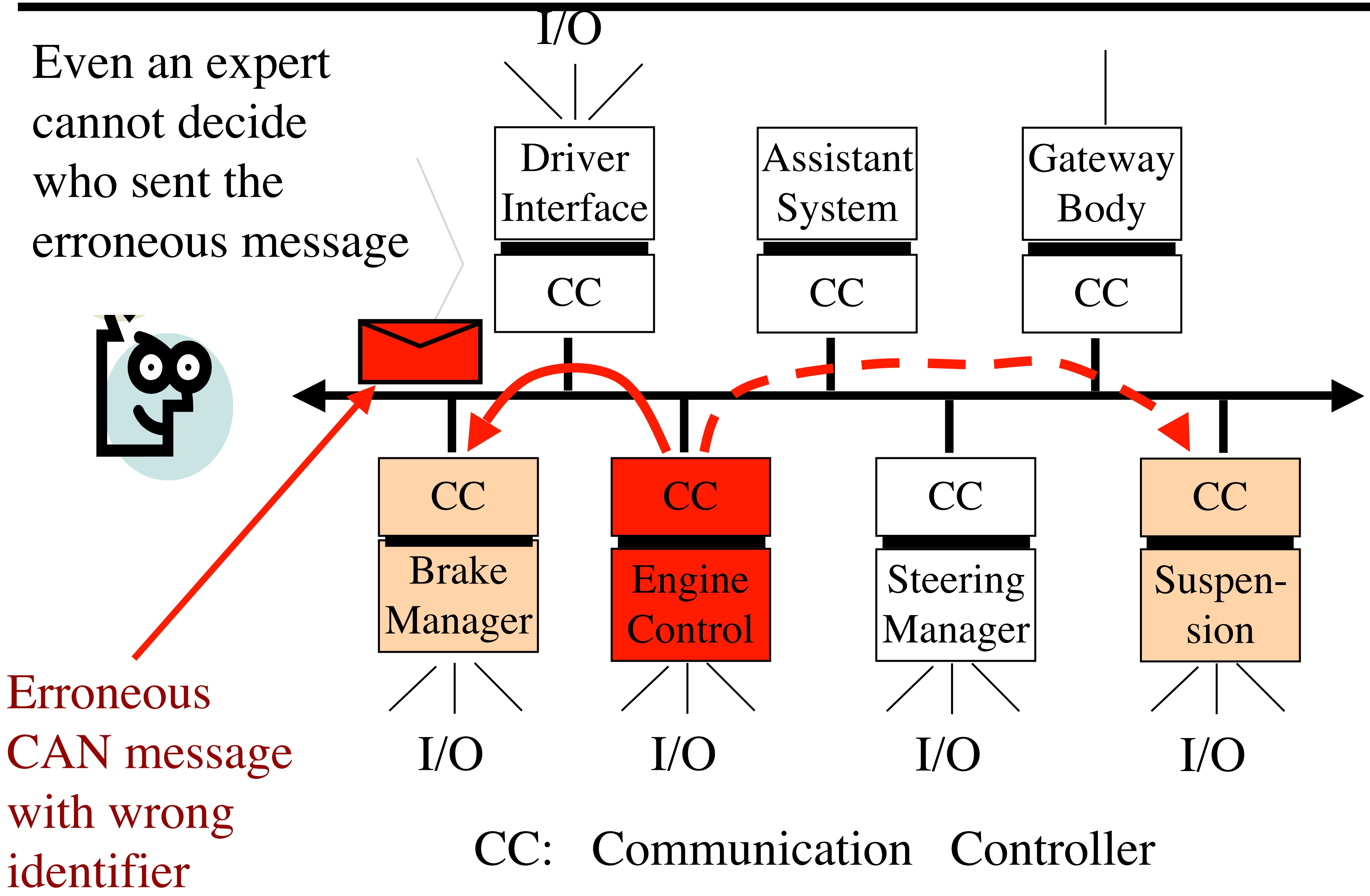
US: SAE J1850 (is a combination of three standards, one from GM, one from Ford, one from DaimlerChrysler)

Japanese; Beans (Toyota)

2003:

CAN, extended to TT-CAN

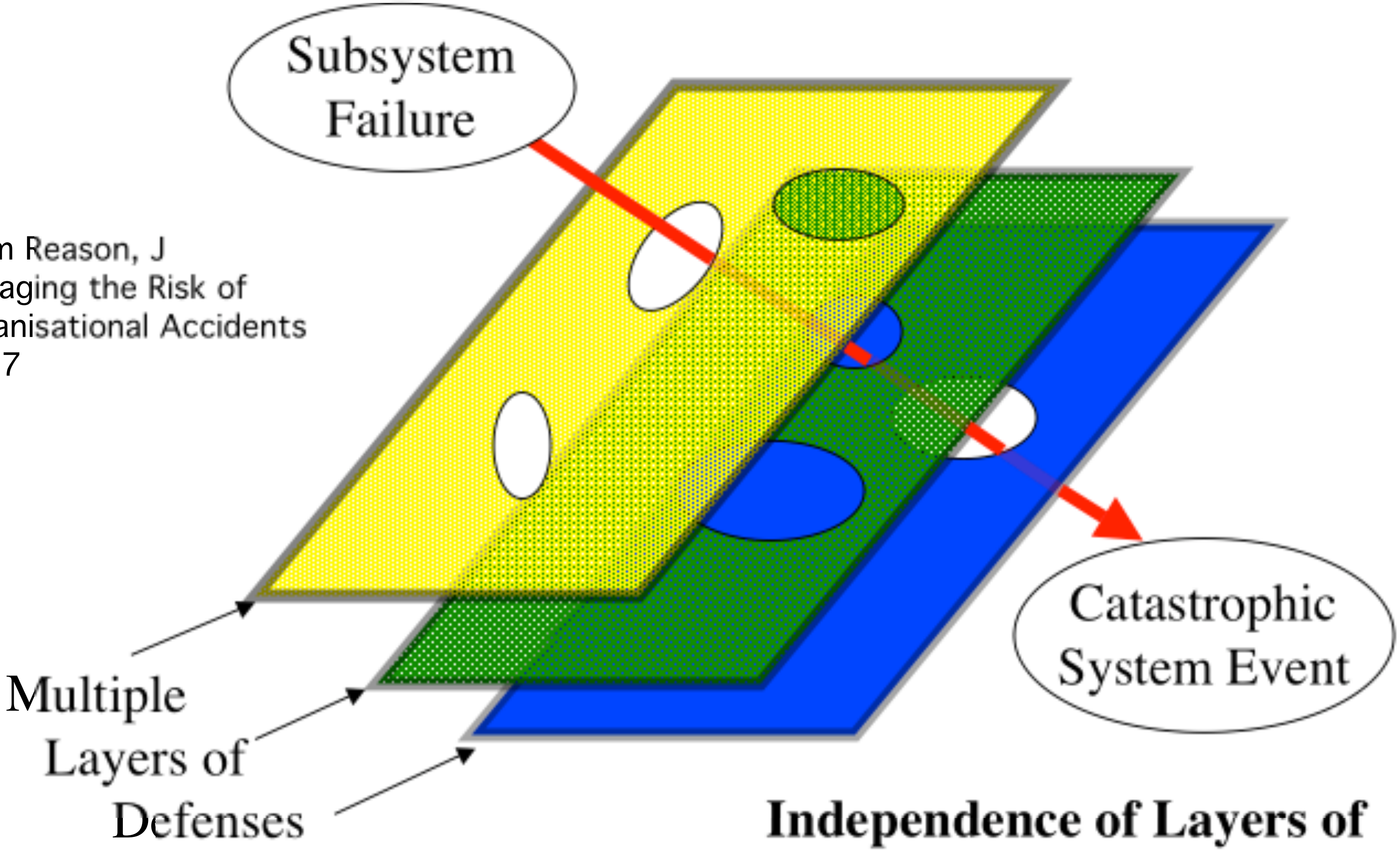
An Example: Diagnostic Deficiency in CAN



CC: Communication Controller

Approach to Safety: The *Swiss-Cheese* Model

From Reason, J
Managing the Risk of
Organisational Accidents
1997



Independence of Layers of Error Detection are important

Approach to Safety

- Incremental approach to the implementation of safety-critical functions
- Get field experience with fail-safe designs before the implementation of fail-operational designs
- Provide safety mechanisms outside the computer system (field an extra wire)
- If safety margins gets too small-->force limp home.
- Do not open the safety relevant designs to scrutiny by the scientific community--see DSN 2003 panel
- The legal department helps!

Open Questions on Safety of *X-by-Wire*?

- What are consequences of this *ad hoc approach to safety* for the complexity of full *X-by-Wire* Applications?
- Is it reasonable to delegate many of the error detection and redundancy management tasks to the application level and avoid an *architecture based* approach to safety?
- Can you design a fault-tolerant *X-by-Wire* system without a precise specification of the fault hypothesis (fault-containment region, failure modes, etc)?

The Economic Dimension: Diagnosis vs. Safety

Diagnosis

- About 2 % of the cost of a car is spent on diagnosis and maintenance of the electronic systems
- This amounts to about 300 $/car
- 50 Mio cars --> 15 Billion $

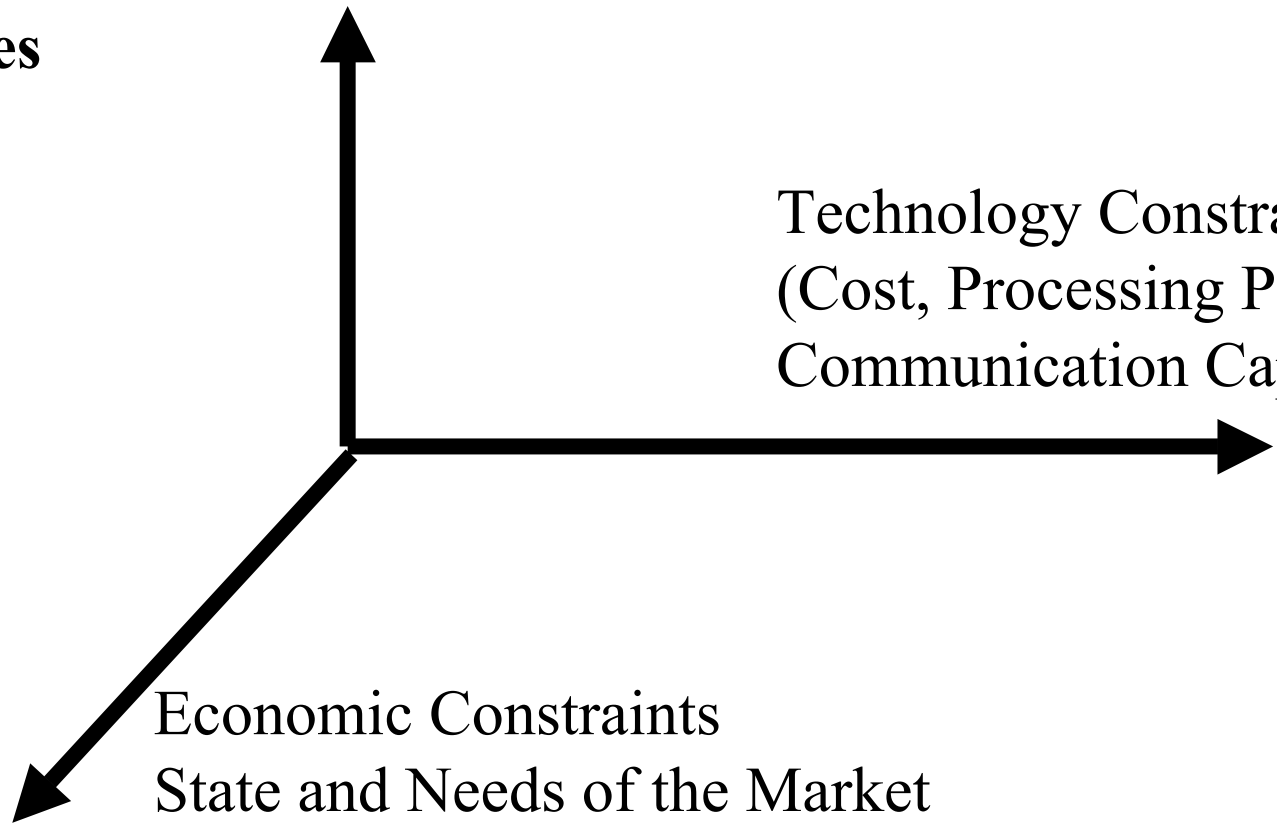
Safety

- How many documented accidents have been caused by computer system failure?
- What is the cost?

Window of Opportunity for COTS

Functional Requirements
User Needs

All three axes change with time



Technology Constraints
(Cost, Processing Power,
Communication Capabilities)

Economic Constraints
State and Needs of the Market
(Dominance, Maturity)

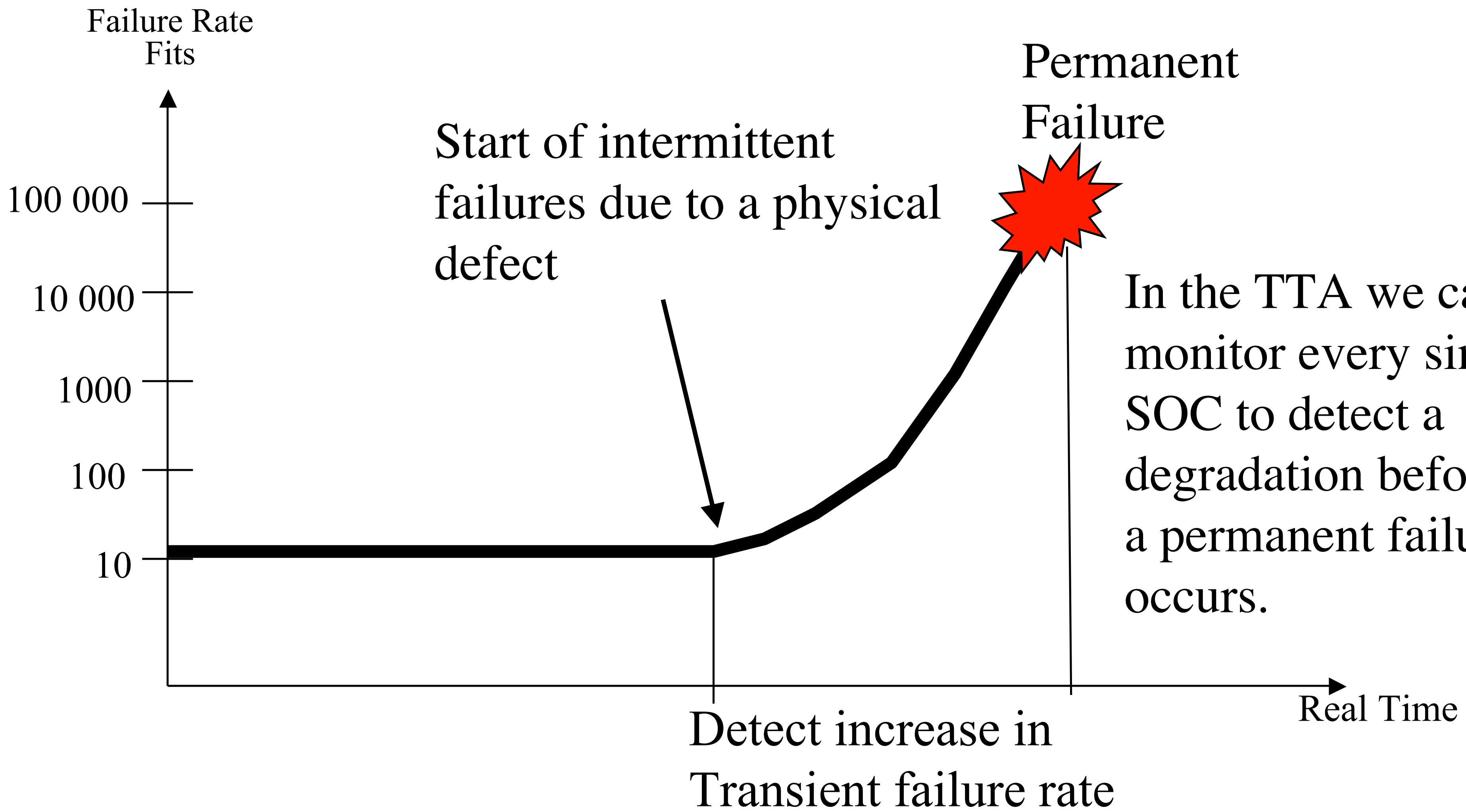
Technology Constraints: Silicon

- At the end of this decade, we will see purely digital Systems-on-a-Chip (SOC) that will host up to one billion transistors.
- Mixed signal IC s that may include MEMS sensing and actuator elements will have a significantly lower logic density.
- From an architecture point-of-view, we will have very powerful processing nodes and smart transducers, connected via field-buses, with a limited processing power

Technology Constraints: Dependability

- The permanent failure rate of automtive chips will be staying where it is today--around 1000 years MTBF.
- The transient failure rate is and will be orders of magnitude higher.
- An increasing transient failure rate (intermittent failures) are an indicator for an upcoming permanent failure.
- In high-dependability applications, it is not justified to assume that a single die can host more than one fault conainment region.

Basic Idea: Intermittent Failures



In the TTA we can monitor every single SOC to detect a degradation before a permanent failure occurs.

Economic Constraints

- ♦ The design of a new SoC requires an investment in the order of 10 Mio € (design cost, mask costs, etc.)
- ♦ The production cost of an SoC are in the order of 10 €.
- ♦ Only applications that require millions of chips can afford the design cost.
- ♦ In the domain of dependable embedded systems only the automotive applications command a sufficiently large market.

Current Issues in the Automotive Industry:

- The wide deployment of intelligent driver-assistance systems has the potential to significantly reduce the number of accidents and to save many human lives.
- Sooner or later, *X-by-Wire* will happen. The sooner it comes, the more lives will be saved.
- The design of the *X-by-Wire* chips will be decisive for our community, since they will constitute the COTS, i.e., the ***raw material*** future dependable embedded systems will have to be made of.

Delay of *X-by-Wire*

At present, the worldwide automotive industry is delaying the introduction of X-by-Wire Systems by two to four years:

- ♦ Worldwide economic climate does not support the massive investment required for the introduction of new technology
- ♦ The introduction of 42 Volt technology is a heavy financial burden to subsuppliers.
- ♦ At present, the dependability problems with automotive electronics are not fully resolved--need consolidation

What are are currently the main obstacles that hinder the wider deployment of electronic systems in cars?

Currrent Obstacles

After discussions with automotive companies,
we have identified the following five major obstacles

1. Electronic Hardware Cost
2. Diagnosis and Maintenance
3. Dependability
4. Development Cost: Limited Reuse
5. Intellectual Property (IP) Protection

Electronic Hardware Cost

Hardware costs are recurring costs that are decisive for the economic success in a mass market.

- At present, the electronic architecture on-board vehicles is *federated*, not *integrated*.
- In a federated architecture every new function requires a new electronic box (ECU-Electronic Control Unit).
- Today we find more than 70 ECUs in upscale cars.
- In an *integrated* architecture the number of hardware boxes can be reduced significantly, resulting in a significant reduction of the hardware costs.
- **The technology to support an integrated architecture with encapsulated execution and communication services is not yet mature.**

Diagnosis and Maintenance

- ♦ The vast majority of failures in the electronic system of a car is *transient* or *intermittent*, but nor permanent.
- ♦ The present electronic architectures within cars do not support the diagnosis of transient faults in an optimal way.
- ♦ The ratio of *first-time-correct* maintenance actions is in many scenarios below 50 %.
- ♦ **The technology to diagnose correctly transient malfunctions needs to be developed further.**

Dependability

- According to the ADAC statistics in Germany close to 50 % of the failures of cars on the road are caused by defects in the electronic systems.
- Connector failures are an important failure class.
- Fail-operational applications (e.g., X-by-Wire) require a reliability that must be better than the reliability of the mechanical system they replace--a level of electronic system safety that the automotive industry is not used to.
- **The present approach towards the design of safety-relevant systems in the automotive industry must be revisited.**

Development Cost

- The unintended side effects between different application subsystems increase significantly the development and integration efforts.
- There is only a limited reuse of software and existing IP due to the missing composability support of current electronic architectures.
- **As a consequence, modular development, validation and certification are still more on the wish-list than in the real world.**

Intellectual Property (IP) Protection

- Sub-suppliers of the car companies are not very willing to open their IP, because they are afraid of giving up their competitive edge (e.g., software for engine control).
- Without a deep knowledge of the software-internals, car companies are reluctant to accept system responsibility for the correct operation of ECUs that contain software modules from different sub-suppliers.
- **The contractual and legal implication of fault-diagnosis and repair responsibility of multi-vendor ECUs are difficult to resolve.**

What is Needed:

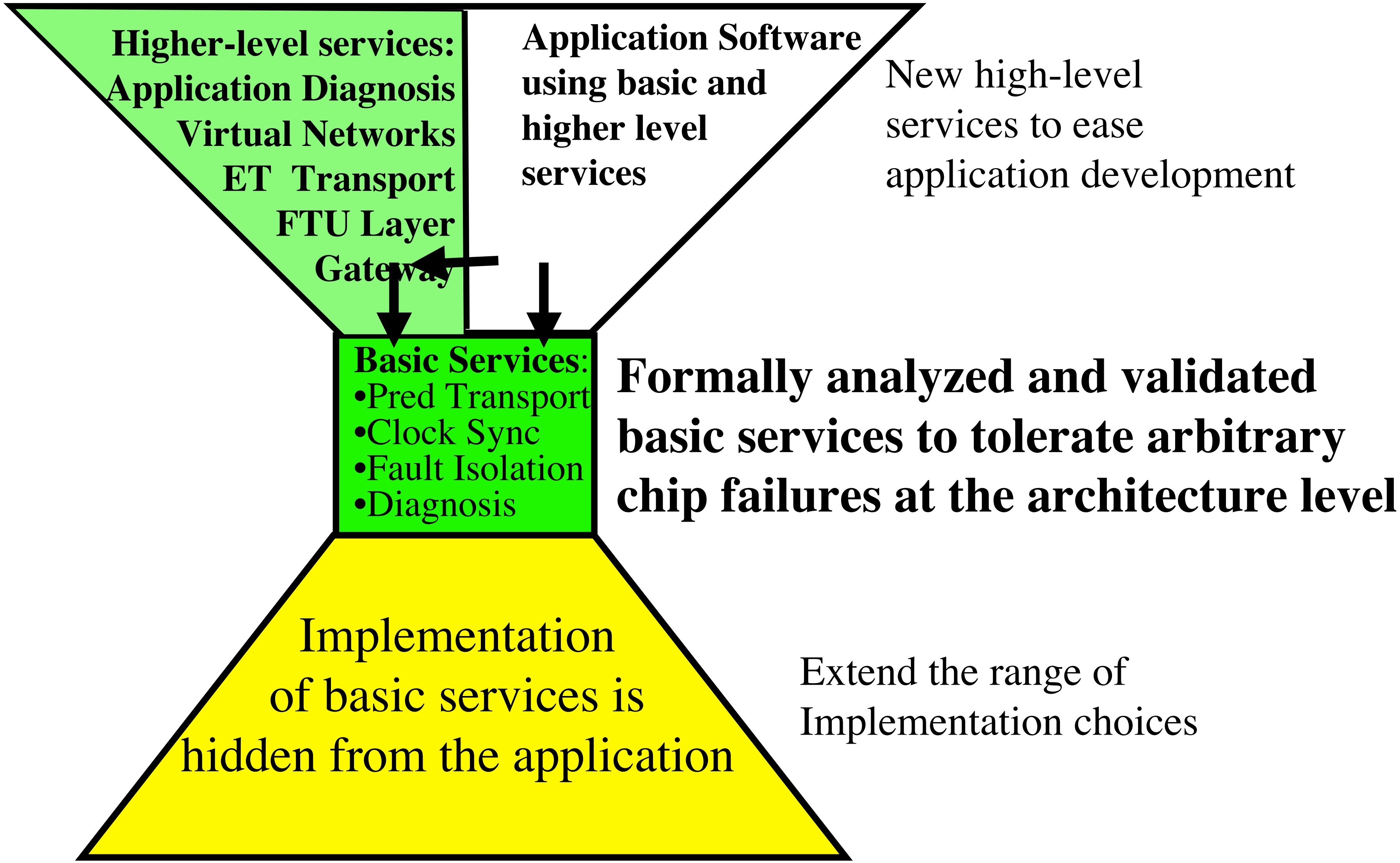
What is needed is an *integrated distributed architecture* where

- ♦ The number of nodes (ECUs) is significantly reduced by providing multiple encapsulated execution environments for different *Distributed Application Subsystems* (DAS) that are integrated within a single physical node and protected from each other.
- ♦ The number of cables and connectors is reduced by providing multiple encapsulated virtual networks on a single wire.
- ♦ Generic services for strong fault isolation and fault tolerance are provided at the architecture level.

What is Needed (ii):

- Architecture support for the precise specification of the temporal and value properties of interfaces.
- An integrated diagnostic service that monitors, detects and diagnoses all transient failures in the distributed execution environment and records every anomaly of an application software module.
- Standard APIs (Application Program Interfaces) that support the integration of legacy software in the form of compiled object modules.

Minimal Crtical Services for Safety



Conclusion

- Sooner or late, *X-by-Wire* will happen on a grand scale.
- The COTS components introduced by the automotive industry will form the *raw material* for dependable embedded systems in most other application domains.
- The dependability problem must be solved at the system level, not only at the component level--although high-dependability components help a lot.
- At the moment, the automotive industry is in the formative stage for defining the *X-byWire* Architecture and the respective COTS components
- The Research Community should get deeply involved in this formative stage.