Time Triggered Protocol (TTP/C): A Safety-Critical System Protocol

Literature Review EE382c Fall 1999

Howard Curtis
Global Technology Services
MCC

Robert France
Global Software Division
Motorola, Inc.

The Evolution of Automotive Electronics

1960's

- Button Rectifiers
- Positive Crankcase Ventilation
- Power Steering

1970's

- Unleaded Gas
- 2 & 3-Way Catalytic Converters

1980's

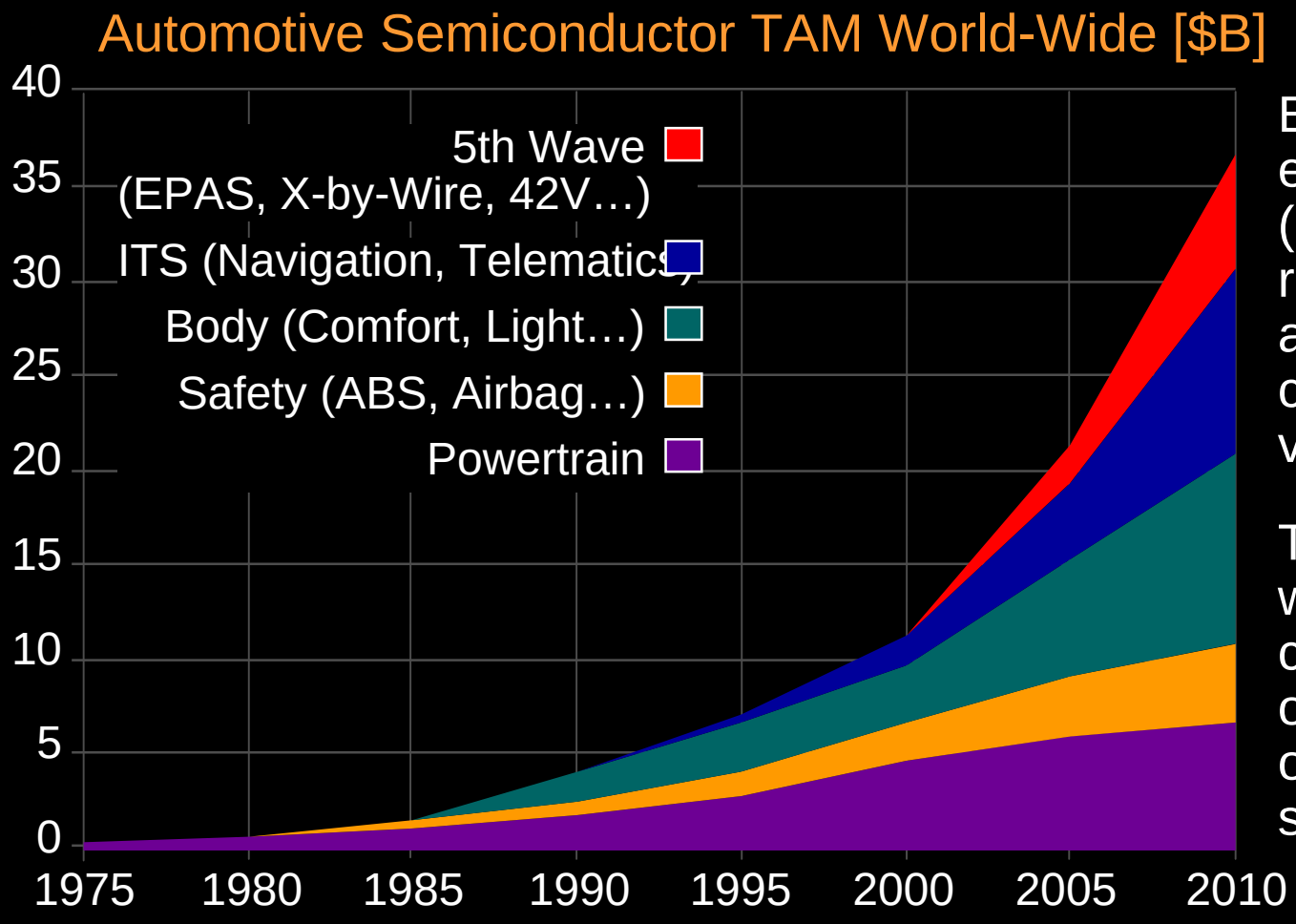
- Engine Control
- Fuel Injection
- Fuel Mix Sensors
- MPU's

1990's

- Reformulating Gas
- High speed MCU for realtime control
- Cold Start
- Onboard Diagnostic level 2
- Valve timing control
- Airbags
- Electric power steering
- Adaptive cruise control
- ABS with traction control and vehicle stability
- First available EVs and hybrids

Source: Motorola, 1999

Automotive Electronics Market Development

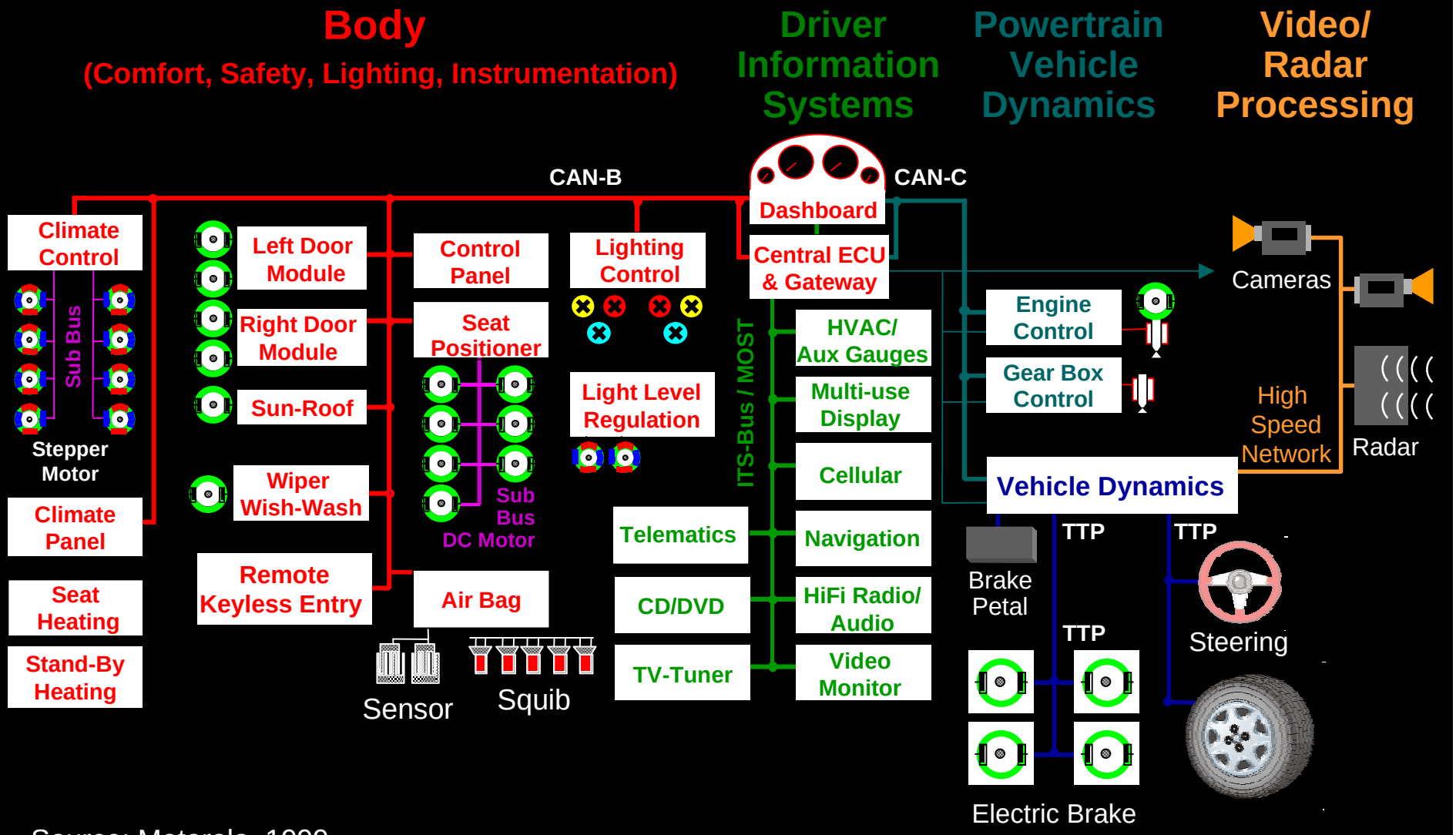


Electronics and electromechanics ('Mechatronics') are replacing hydraulic and mechanical components in vehicles.

The role of the driver will (gradually) change from machine operator to supervisor of a transportation system.

Source: Motorola, 1999

Total Connectivity in the Vehicle



Source: Motorola, 1999

Event-Triggered vs Time-Triggered Systems

- Event-triggered systems react to events
  - Reception of a message
  - Termination of a task
  - External interrupt
- Time-triggered systems derive actions from the progression of a globally synchronized time base
  - Transmission of messages
  - Task execution
  - Monitoring of external states

Time-Triggered Protocols

- TTP: Family of TDMA based, fault tolerant protocols.
- TTP/C: A communication protocol specifically designed for safety-related automotive applications.
- The development of TTP and TTP/C has been led by Prof. Hermann Kopetz, Technical University of Vienna.
- The commercial development of TTP/C tools and products is led by TTTech.
- Existing protocols J1850 and CAN meet the the bandwidth specification for an SAE Class C protocol, but not the fault tolerant requirements.

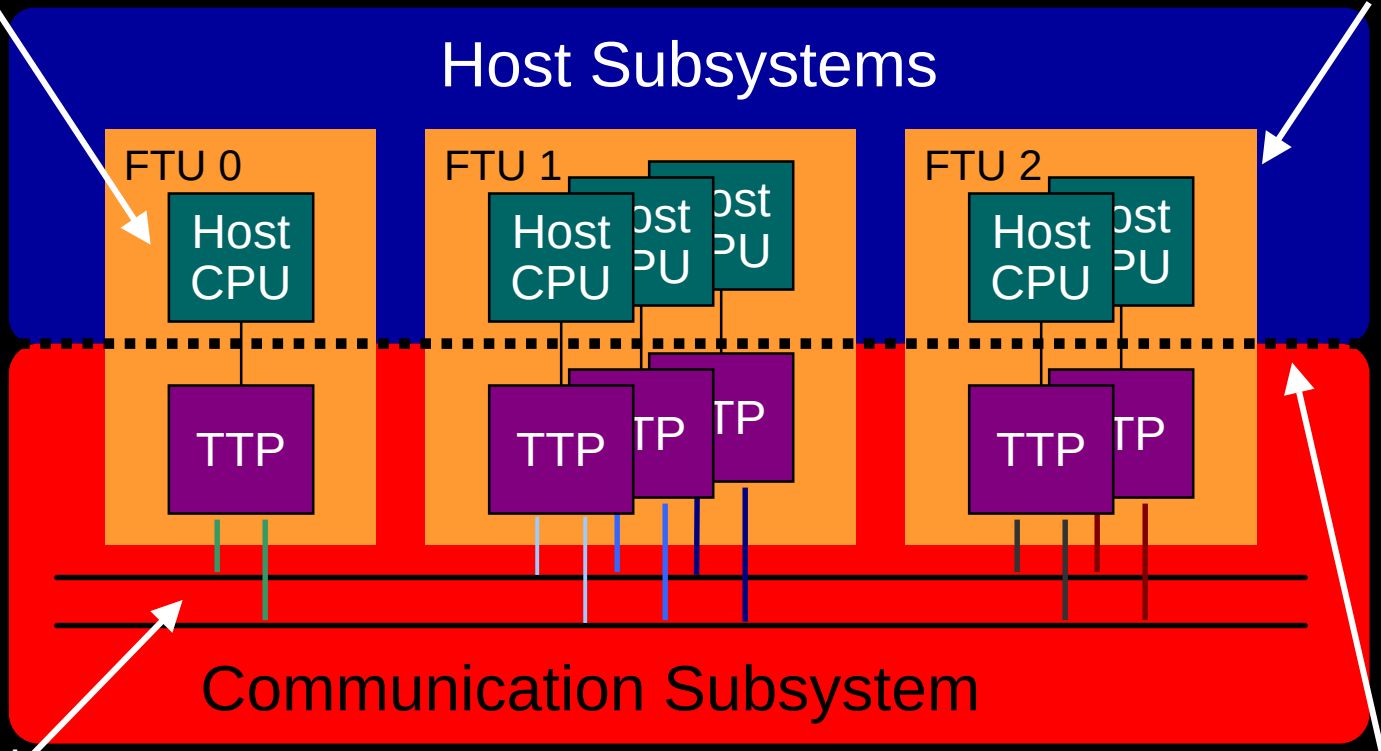
TTP/C Node Architecture

- Host
  - The Host runs the application software.
- Controller Network Interface (CNI)
  - De-couples the applications-level software from the network using dual ported RAM.
  - Contains the Message Descriptor List (MEDL) controlling bus access.
- TTP/C Communications Controller
  - Provides the actual connection between the TTP/C node and the shared network.
  - "…the TTP/C controller provides guaranteed transmission times with minimal latency,
    jitter, fault-tolerant clock synchronization, and fast error detection."
    (Ross Bannatyne, "Time Triggered Protocol ...," *Wescon 1998*, p. 88.)
- Replica Determinant
  - Allows multiple parallel nodes for fault tolerance
- Fail Silent
  - Enforced by bus guardians.

TTP/C Cluster

Nodes are Smallest Replaceable Units (SRUs)

Fault Tolerant Units (FTUs): Groups of actively replicated nodes



Duplicated broadcast busses

Communication Network Interface (CNI):
- System partitioning: autonomous TTP controllers, host CPUs
- Hides communication subsystem behind memory abstraction
- Predictable interface behavior achieves composability

Source: Motorola, 1999

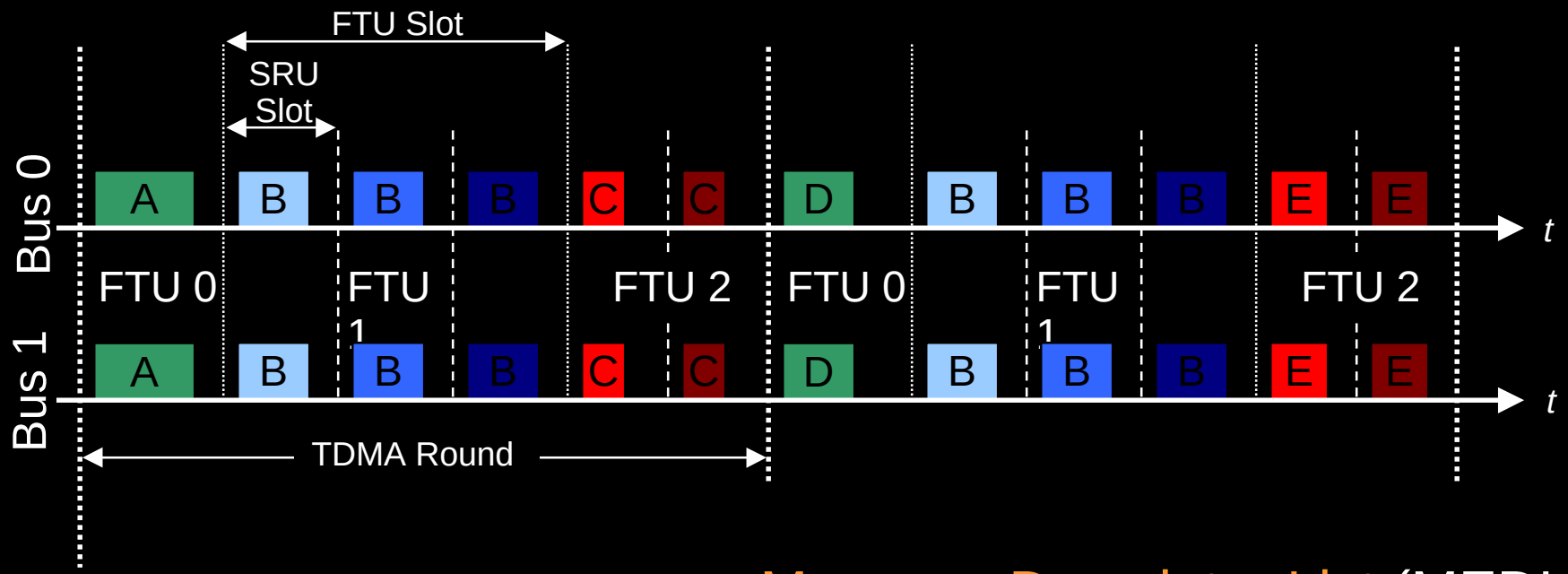
TTP/C Communication Properties

- Static Scheduling
  - Guaranteed delivery times with known variance (jitter).
- Clock Synchronization
  - All nodes synchronized to within one microsecond each TDMA round.
- Composability
  - TTP/C nodes are temporally composable as well as functionally composable. This is a key property of being replica determinant.
- Fail Silent
  - The bus guardians ensure transmission only during the correct timeslot, in all cases.
- Membership
  - Every node's membership is available during each TDMA round.

TTP/C Bus Access Scheme

Time Division Multiple Access

- Fixed assignment of slots to nodes
- Every node periodically



Message Descriptor List (MEDL):

- Static data structure
- Message dispatching table

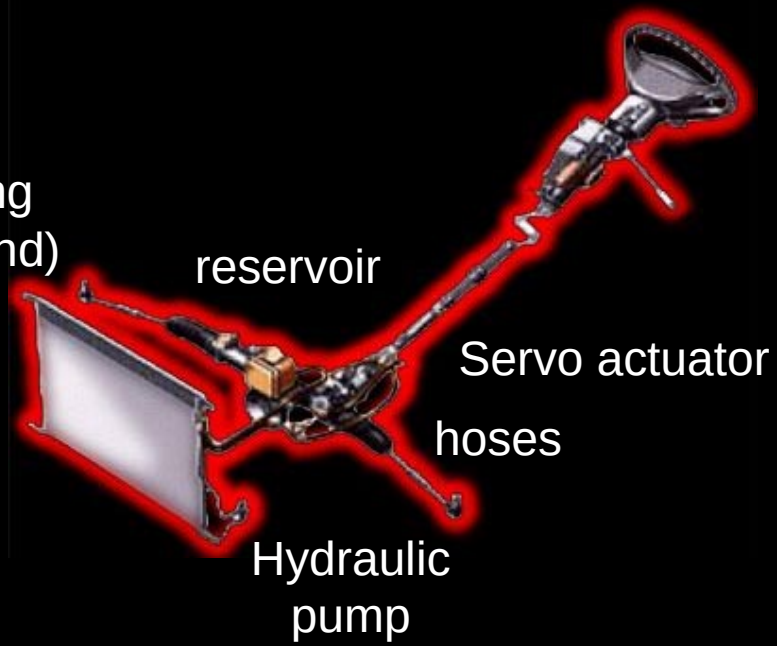
Source: Motorola, 1999

X-by-Wire Systems

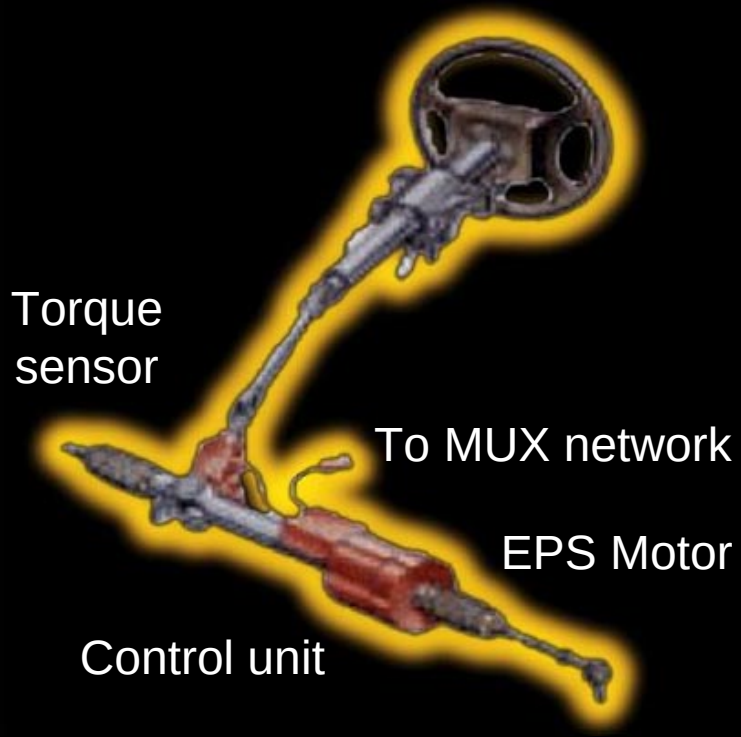
- Mechanical & hydraulic subsystems controlling safety-related functions are replaced by computer control systems
  - Examples: brake-by-wire, steer-by-wire, vehicle dynamics control, active suspension
- Advantages: Cost reduction, weight reduction, easier design, assembly and maintenance, passenger safety and comfort
- Safety-critical applications require:
  - Fault tolerance: no single fault may lead to a system failure
  - Predictable and timely system behavior
  - Synchronized time base (global time)

Evolution of Steering Systems

Hydraulic Power Assist (Conventional Steering)

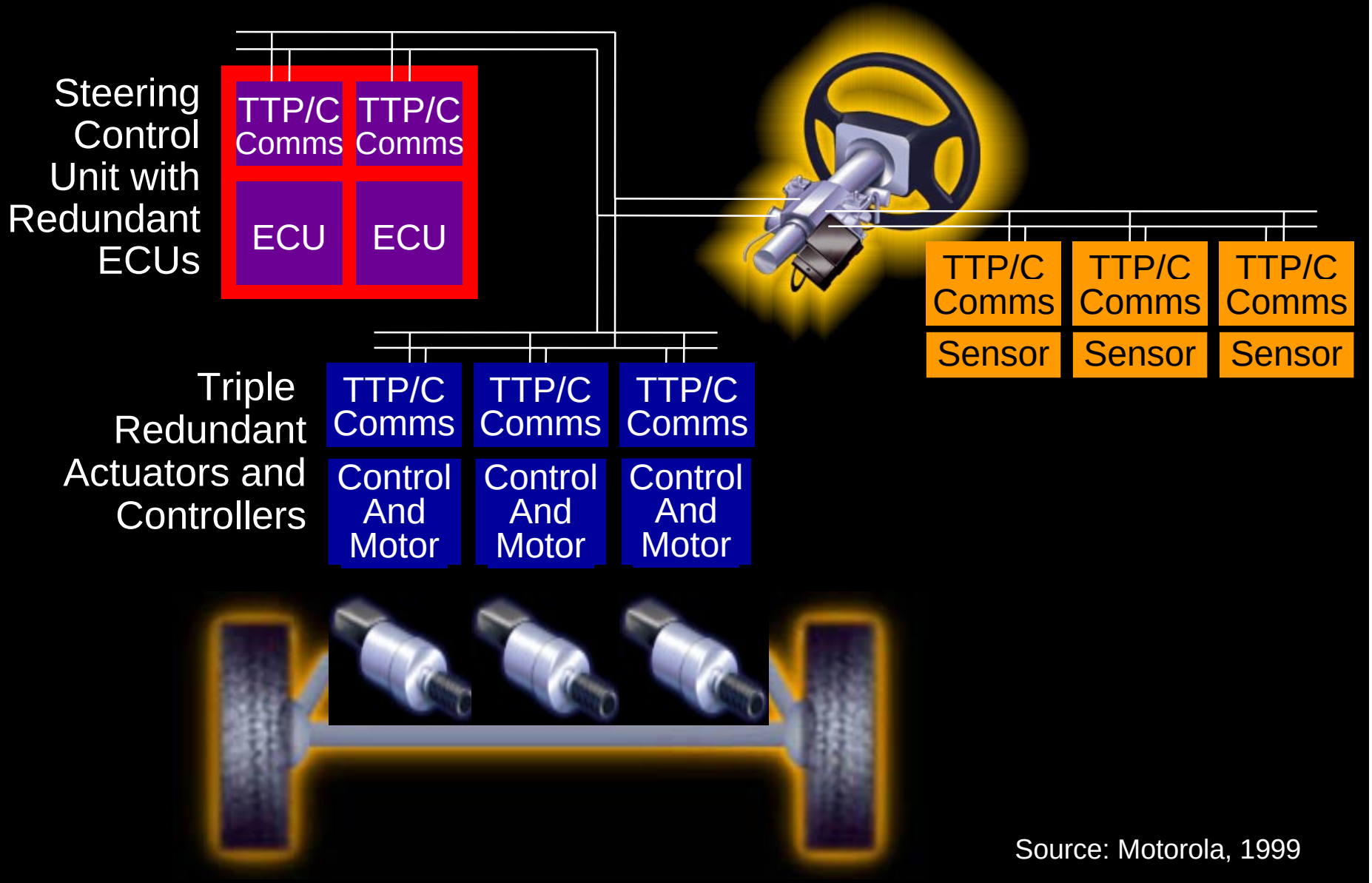


Electric Power Assist (Newest Technology)



Source: Motorola, 1999

Steer By Wire Systems



Source: Motorola, 1999

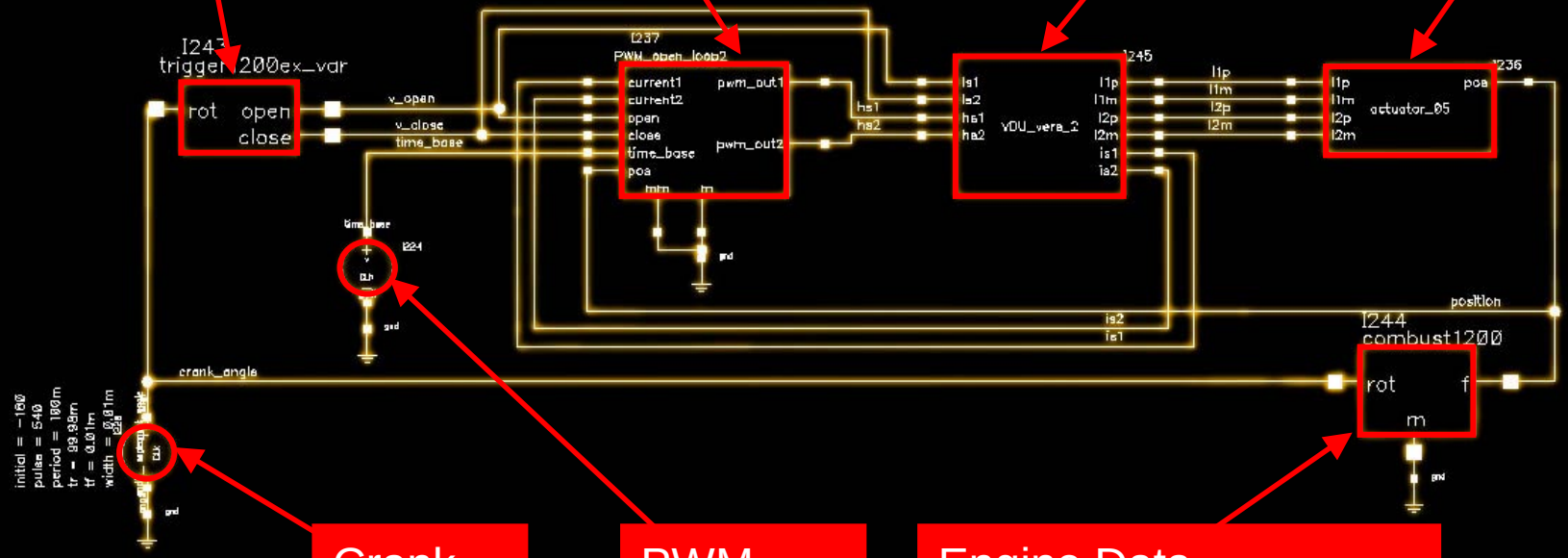
Modeling & Simulation in Automotive Design

Trigger, Crank Angle based

Matlab/Simulink Control Algorithm

pre-Driver
Signal Conditioning
Power Module
Thermal Behavior

Electro Mechanical Valve



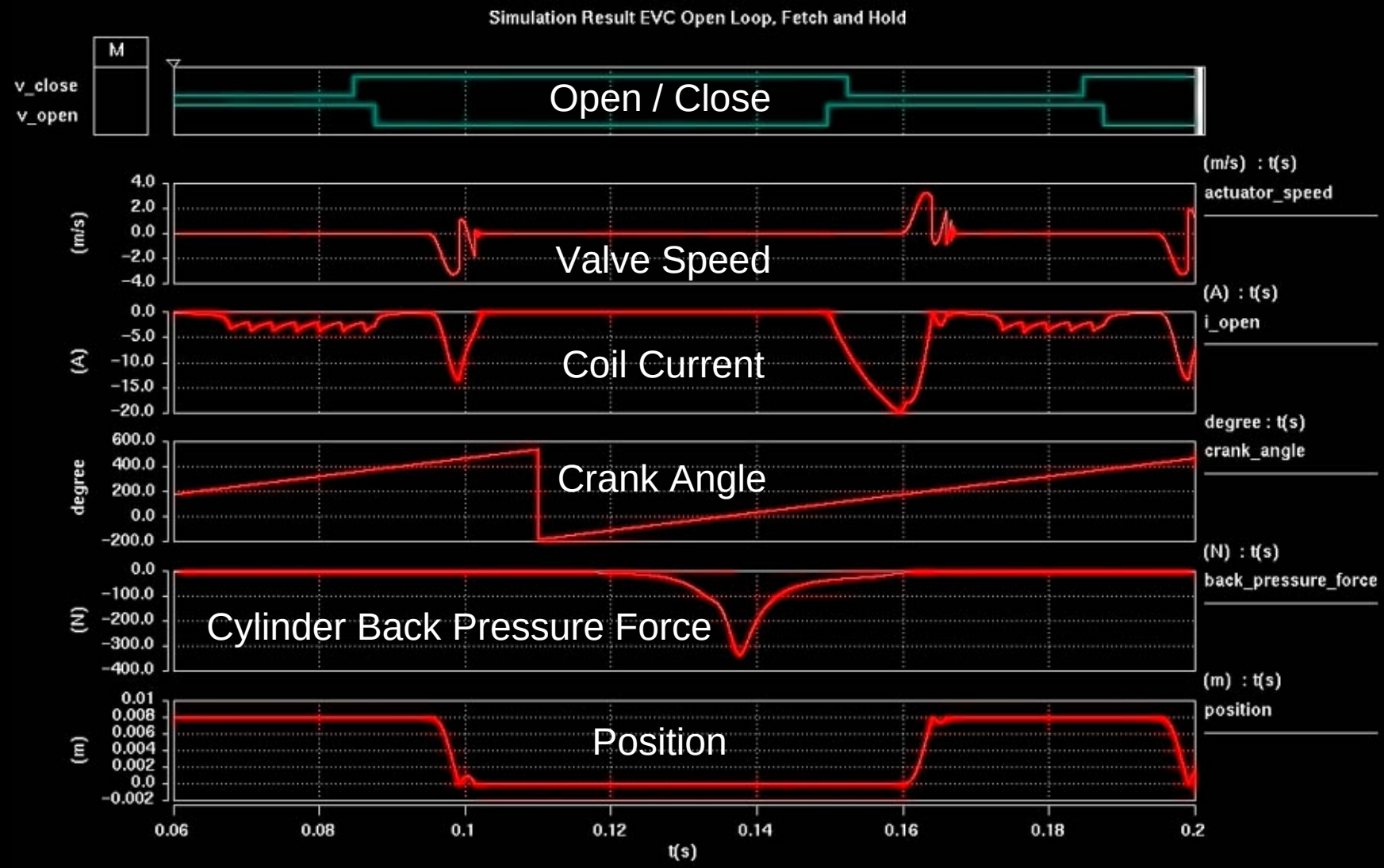
Crank Angle Source

PWM frequency

Engine Data, Combustion Chamber Back Pressure

Source: Motorola, 1999

Simulation Results



Source: Motorola, 1999

Summary & Conclusions

- Safety critical systems are the next big development area in the automotive industry.
- TTP/C provides the basic features needed for implementing safety critical systems.
- Modeling and Simulation are increasingly important to designing highly complex, safety critical systems affordably.

- Proposed project to implement a partial high level model of TTP/C in Ptolemy as proof of concept.
- Prof. Hermann Kopetz lecturing at UT, Nov. 18.