Sharing technology for a stronger America

Verification Challenges in Automotive Embedded Systems

William Milam

Ford Motor Co

Chair USCAR CPS Task Force

10/20/2011

What is USCAR?

The United States Council for Automotive Research LLC (USCAR) is the umbrella organization for collaborative research among Chrysler LLC, the Ford Motor Company and the General Motors Corporation. Founded in 1992, the goal of USCAR is to further strengthen the technology base of the domestic auto industry through cooperative research and development.

USCAR Mission

- Create, support and direct U.S. cooperative research and development to advance automotive technologies

- Be responsive to the needs of our environment and society and include the appropriate public and private stakeholders as required

Why Automotive?

Automobiles are the most complex consumer device in the world.

The automobile may well be the poster child for cyber-physical systems.

The automotive industry does aerospace complexity on a very limited budget.

It's not a software problem, it's a system engineering problem.

Brief History

- In the beginning the world was mechanical.
  - Carburetors, Distributors and vacuum.
- Once we reached the limit of mechanical solutions, we went to computers with assembly language and integer only processors.
  - Initially spark control, then moved to fuel and egr.
- Again we reached a limit with that level of abstraction and moved to floating point processors and C.
  - Variable cam timing, electronic throttle, transmission control (CVT).

Today: Model Based Design

- With the advent of yet more complicated control with increasing pressure on robustness and time to market.
  - Move on to model based design of controls.
    - Graphical programming
    - Data and control flow
    - Automatic code generation
  - Distributed control
    - Stability control
      - Steering, brakes and torque control with AWD

What's missing?

- System analysis – Limited complexity
- Requirements Capture and Analysis
- Multiple Modeling Languages – Unable to share models across tools
  - Composition of languages based on formal semantics and model of computation
- Interface to Legacy – We cannot afford to hit the reset button every time someone invents a 'new' tool.
- Validation of Tools – How will tools be validated?

What is the next level of abstraction?

- We can design complex controls, however it is still in a virtual mono-processor world.
- How do we reason about performance impacts of system design?
  - Distributed controls/computing
    - Multi-Core processors
  - Network communications impact
  - End to end scheduling
  - Failure modes
  - Composition of separately designed and developed control algorithms

What's CPS got to do with it?

- Fundamental marriage of physical components and embedded computer processing.
  - Smart material
  - Intelligent composition of sub-systems
    - It's more than signal compatibility
  - Composition at multiple levels
    - Vehicle platooning
    - Semi/fully autonomous vehicles
    - Vehicle highway coordination
    - Combined end to end multi-modal transportation
    - Context sensitive operating modes
      - High density area carbon tax
      - Powertrain mode operation tied to geography.

Verification and Validation

- Composition of sub-systems to create systems
  - Mixed criticality
  - Trusted systems with untrusted components
- Human in the loop – How to represent human behavior
- Physics – how to analyze discrete and continuous behaviors
- Abstractions – what is the appropriate level?
- Bridging the gap between natural language requirements and automaton representation

Modeling languages and tool chain development

- Need to combine multiple DSML to create system model.
  - Engineering domains have different views of the system
  - The composition of the views gives us the system
- Need to address '*debug*' capability for CPS
  - How do we set 'breakpoints'?
  - What does it mean to single step a CPS system
  - What does 'debug' even mean here?
- Managing and tracking artifacts
  - Data mining to find appropriate existing entities
  - 35 applications for one model year. (Gasoline only)
    - Each application has approx 141 features/components

Dependable and Secure Automotive Cyber-Physical Systems

- Workshop was held in Troy Michigan on March 17 and 18.
- There were 97 registered participants from academia, government and industry.
- Breakout groups for:
  - Secure and High Confidence Platforms
  - Open Experimental Platforms
  - Driver in the Loop
  - Safety Critical Design Process

Secure and High Confidence Research Challenges

- **Software Complexity**
  - Impossible to validate sufficiently through testing as number and complexity of modules increases and need to be integrated
  - New business-models with many suppliers and developers
- **Assurance (Safety and reliability)**
  - Cost effective Fail-Operational Systems
  - Moving from Fail-Safe to Fail-Op
  - Protect against common mode of failures
  - (EMC, Power Supply, Lighting, …)
- **Cyber-Physical Security**
  - More connectivity into our vehicles
  - More safety critical controls (towards autonomous driving and by-wire)
  - Open-source platforms (for Infotainment)
  - Open protocols: ODBII, Right to Repair

Secure and High Confidence Platforms Assurance Roadmap

- Formal analysis techniques
- Real-time analysis
- Probabilistic techniques
- Model-based testing and validation
- Moving from diagnosis to prognosis
  - Predicting failure before it happens to avoid the malfunction of the system/network.

Secure and High Confidence Platforms Assurance Roadmap

- Cost effective approach to Fail-operational
- The effects of architectures on Assurance, Safety and Security.
- Dynamic reconfiguration of functions (in distributed systems)
- Reconfigurable Hardware platforms(Multi-Core)
- Deterministic Redundant Platforms
- Cyber-Physical System Co-design
  - Combining physics based principles with computer science
  - Resource Aware Control Methods
- Formal Methods
  - Scalability
  - Mixed modes (temporal vs discrete vs continuous)

Safety Critical Design Process Research Challenges

- Emergence: Competing (safety) goals of separately safe systems. E.g. ACC wants to speed up as the car ahead speeds up to avoid a merging vehicle, but a collision avoidance wants to slow down.
- Non-deterministic behavior - how do we learn from components and analyze/compose them?
- Requirements Analysis - In combinations of separately developed subsystems, how do we identify and handle conflicting and/or missing requirements, prior to integration level testing?
- ISO26262 is a functional safety (electrical/software) reference, but insufficient for total system safety. ISO is a quality office issue. How do we track the safety aspects beyond the scope of ISO-26262?

Safety Critical Design Process
State of the Art

- FMEA, Concept FMEA (inductive, like a top-down FTA), Design FMEA (deductive, after a design is complete).
- USTAG required ISO26262 standard to include ***functional interaction failures*** (emergent properties). This modified the original definition of safety analysis from component failure to unsafe malfunction.
- VDA EGAS – German developed standard for throttle by wire, asymmetrical CPU hardware monitoring (enhanced watchdog).
- Formal methods - inefficient for large scale systems
- Tools for system safety analysis (e.g. formal methods) are not commonly in use by all engineers.
- Integrity monitoring is useful to safety
- Simulink/Stateflow is platform dependent and cannot verify timing
- Learn over time & retrofit (e.g. FAA).

Safety Critical Design Process
Promising Opportunities for Research

- 3-5 Years
  - Theories of Monitorability is an area to develop. Safety specification of the monitor, is the system predictable, observable? What about in the presence of noise?
  - Timing needs to be part of the V & V. Realtime guarantees of deliveries of packets for sensor – extend this approach to the safety system and analysis.
- 10 Years
  - Integration of different safety methods, tools, approaches.
  - Integration of analyses, top-down (new functions) and bottom-up (legacy components, new components)
- 20 Years
  - ***Emergence:*** Competing (safety) goals of separately safe systems. E.g. ACC wants to speed up as the car ahead speeds up to avoid a merging vehicle, but a collision avoidance wants to slow down.

LAST SLIDE!

Thanks for listening!

Contact:
William P. Milam
Ford Motor Co.
E-mail: wmilam@ford.com
Office Phone: 313-323-8681