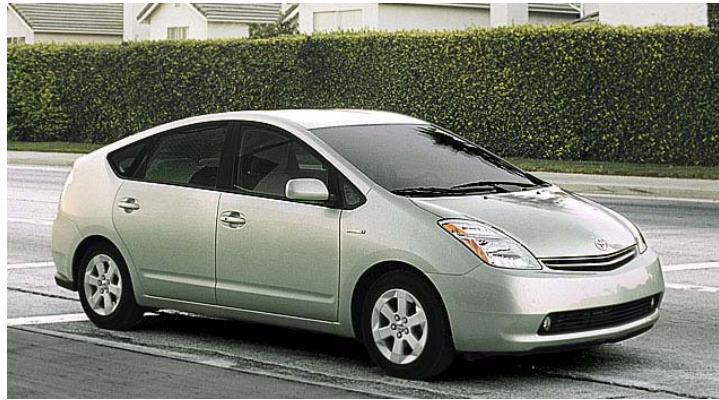


High Confidence Powertrain Control Software Development

Hakan Yazarel, Tomoyuki Kaga, Ken Butts



- NEW YORK (CNN/Money) - A **software problem** is causing some Toyota Prius gas-electric **hybrid cars to stall or shut down while driving at highway speeds**, according to a published report.
- Toyota spokesman Sam Butto told the newspaper the auto manufacturer identified a **"programming error"** in the computer systems of 23,900 Prius cars last year and sent owners a service notice advising them to bring the cars into dealers for **an hour-long software upgrade**.
- Source: http://money.cnn.com/2005/05/16/Autos/prius_computer/

- Automotive control system became a **Large Scale Control System**

- Engine control
- Traction control
- Auto-cruise control

- Modules designed and tuned by individual engineers over the years and integrated to **legacy structure**

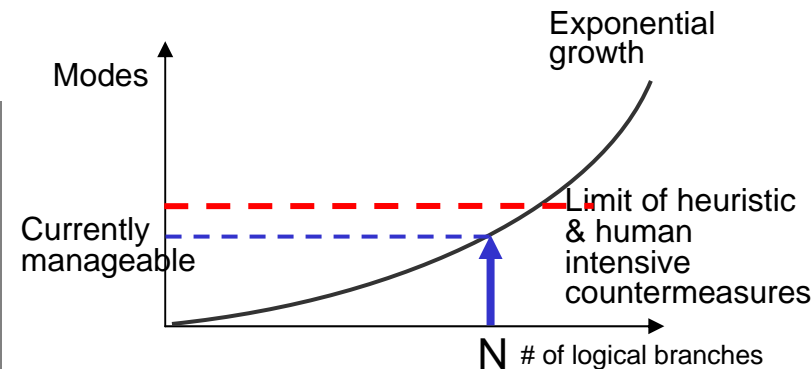
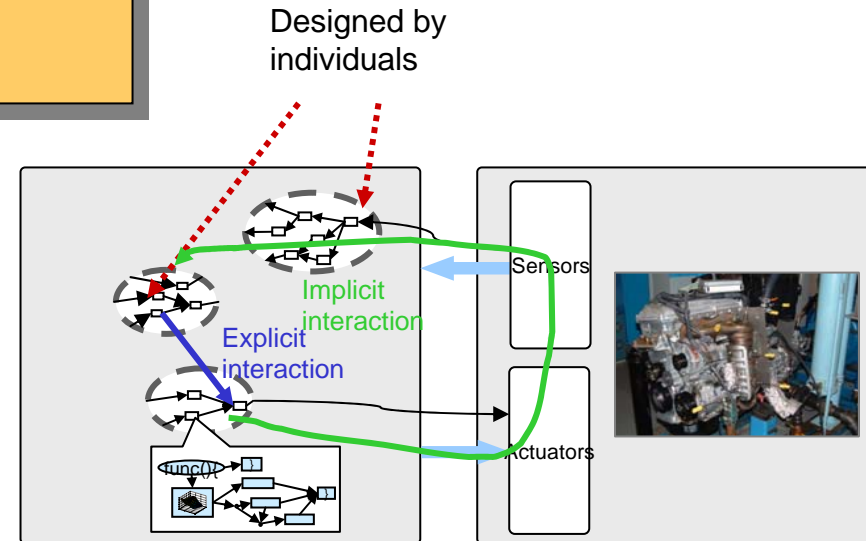
- Lack of understanding of whole structure
- Lack of predicting the effect of modification

- Complex software structure

- Hundreds of modules interact with each other
- Many modes of operations e.g. if-else, switch-case
- Many lookup tables
- Hybrid nature of system

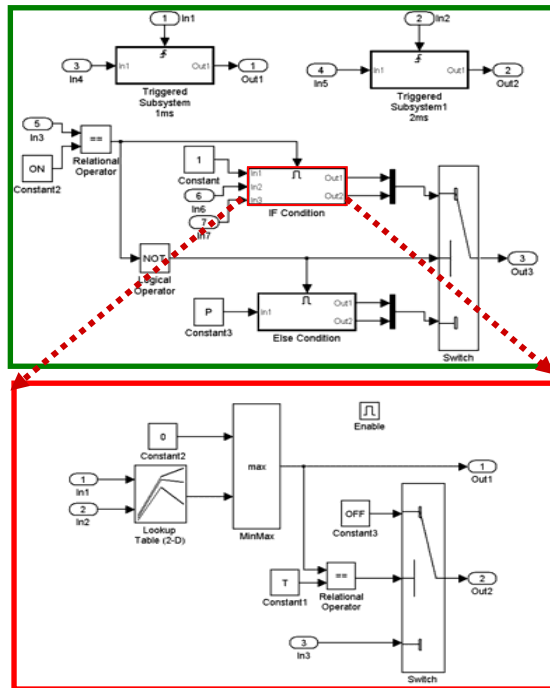
- Number of tests grow exponentially as new functionalities are added

- Identifying the root-cause of even a known problem is very time consuming
- Becomes chicken-egg problem in closed-loop feedback control



Summary: Advanced Design and V&V processes should be incorporated

- Currently Simulink/Stateflow
- Formally defining **multiple layers of abstractions** for a **control system software** that captures component interactions, data-access rules, explicit/implicit dependency structures etc., e.g. AADL
- Formally specifying control system properties (designer's intended behaviour) to help V&V



- Currently, not clear definitions of feature and module

- Feature-level (high level components)
 - Interactions between modules
 - Time/Event triggered subsystems
 - Enabled subsystems
 - If-then-else branches
- Module-Level (low level components)
 - Arithmetic computations
 - If-then-else branches

- V&V tool sets for design steps
- Hierarchical verification
 - Module, feature, system levels
- Test generation for closed-loop feedback control system
- Assertion based verification
 - Components of an assertion for a control software
- Evaluating compatibility of a modified/new module within the structure

Conclusion

The main obstacles to high confidence control system

- Lacking a formal hierarchical structure
 - To build large scale control systems
 - Easy verification and validation
- Incrementally developed legacy structure
- Complexity: Mainly due to number of logical decision branches