

Fault Tolerant Embedded Software

William P. Milam

Ford Motor Co.

Research and Advanced Engineering



Why am I here?

- Automobiles are the most complex consumer device in the world.
- The automobile may well be the poster child for cyber physical systems.
- Embedded systems composed of heterogeneous components designed and implemented by different suppliers
 - Both hardware and software components
- The most difficult issues lie not in the design of the software in individual modules, but in the interactions between different components
 - Central lock systems interacts with 18 other systems
 - Airport Test (HIL)



Why is software so hard?

- Software is capable of implementing complex behaviors and functions.
 - **Good:** The character of our vehicles is increasingly defined by the software that implements complex features.
 - **Bad:** Growing complexity and interactions among distributed systems leads to increased risk of unexpected/unintended behaviors.
- Software is deceptively easy to change
 - **Good:** Rapid response to failure mode identification.
 - **Bad:** Additional failure modes created by lack of attention to verification and validation.



Example: Volvo XC-90

- Total SW content 10 MB - 50 MB (Base – Full Option)
 - Body network 2 MB - 10 MB
 - P/T network 5 MB – 10 MB
 - Infotainment network 3 MB – 30 MB
- All modules are reprogrammable via OBD connector in factory or workshop

Full option includes:

- Forward collision warning
- Blind spot detection
- Navigation
- Rear view camera
- Telephone/Telematics
- and more



Proposed Fault Tolerant Roadmap

- Research needs:
 - Fault Classification
 - Taxonomy of faults, errors, and failures to be addressed
 - Models of faults and fault interactions
 - Fault Detection
 - Methods for formal specification of conditions to be monitored
 - Methods for run-time detection of faults, errors, and failures
 - Model-based generators for run-time monitors
 - Fault Isolation
 - Methods of run-time identification of the cause of faults for the purpose of fault mitigation
 - Fault Mitigation
 - Methods and architectures for mitigation, recovery, and/or reconfiguration
- Research roadmap:
 - Establish automotive challenge problems in at least three domains:
 - USDOT Vehicle Infrastructure Initiative framework (critical vehicle-to-vehicle or vehicle-to-infrastructure communication, for example)
 - Anticipated active safety/vehicle stability control
 - Hybrid electric vehicle powertrain control.
 - Integration of all of the above problems to create an automotive grand challenge.
 - Develop fault injection methodologies, and an open experimental platform for implementation of detection, isolation and mitigation solutions.

