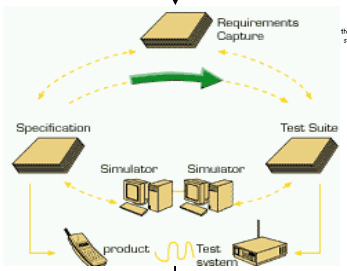
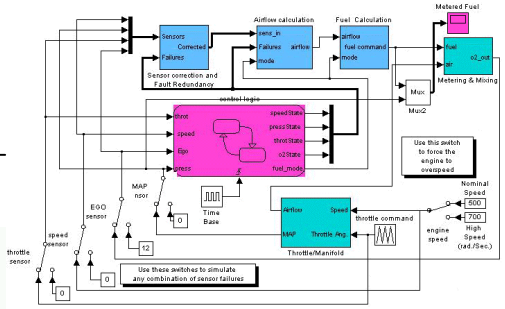
Formal Composition Technology for Time-Triggered Systems

From models





To time-triggered implementations

Through designs

TTP
As Predictable as Time

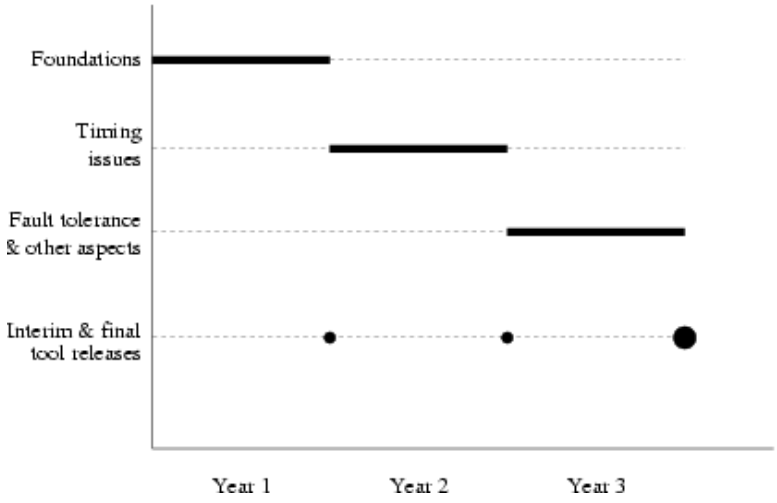
New Ideas

- Formal treatment of the multiple modeling and implementation frameworks used in development of an embedded system and formally-based transformations between them
- Formal assurance methods for the industrially important frameworks provided by Matlab/Simulink/Stateflow and the Time-Triggered Architecture
- Compositional development and analysis for embedded systems based on formal integration of modeling and implementation frameworks

Impact

- Formal assurance of selected critical properties for complete time-triggered implementation of an embedded system
- Order of magnitude reduction in effort required to transform the abstract design for an embedded control system (e.g., in Matlab/Simulink/Stateflow) into one for a fault-tolerant,time-triggered implementation
- Formal assurance of selected critical properties for complete Matlab/Simulink/Stateflow models

Schedule



John Rushby, Computer Science Laboratory, SRI International