

DELPHI

Development Of A Simulation Model For System Safety Analysis

Padma Sundaram

Joseph D'Ambrosio

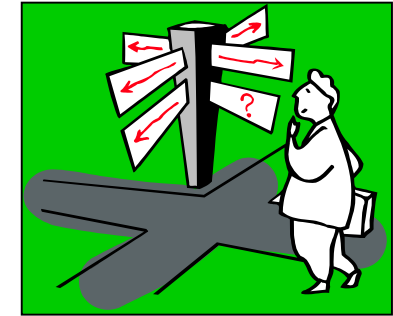
Song You

Siddharth D'Silva

IAC2005

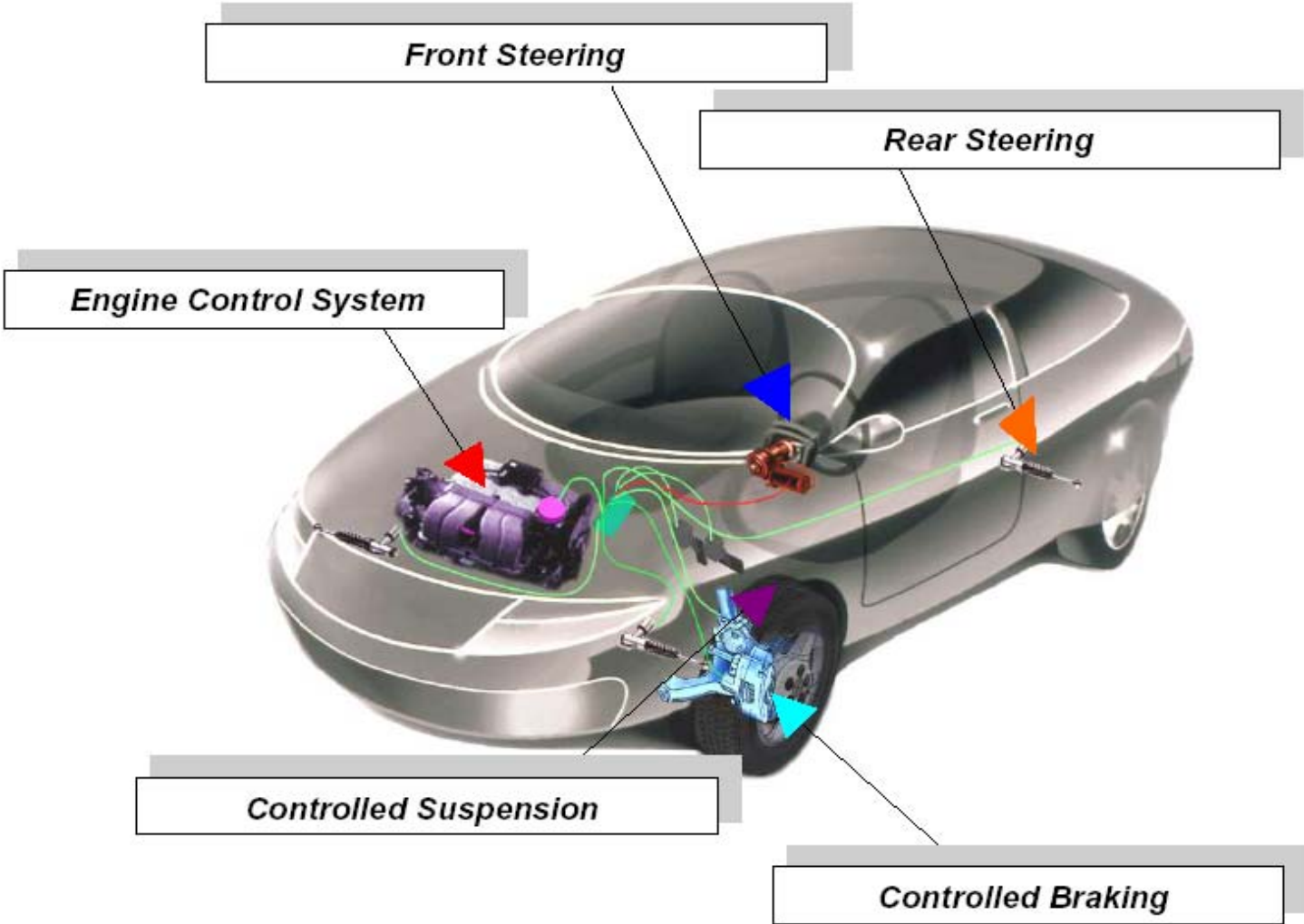


DELPHI



- Motivation
 - Safety Critical Systems
 - Modeling & Simulation
- Simulation Model Development
 - Tools- MATLAB®, Simulink®, CarSim®, AmeSim®
 - Vehicle Model, Subsystem Model, Actuator Model
- Simulation Model Validation
- Potential Hazard Analysis
 - Hazard Testing
- Summary





- Advanced systems provide improvements in vehicle safety, stability, fuel economy, comfort, handling etc
 - Electric power assisted steering, Active Steering and Brake control systems
 - Some of these systems activate independent of the driver input
 - Example- [Simulation of an advanced system](#)

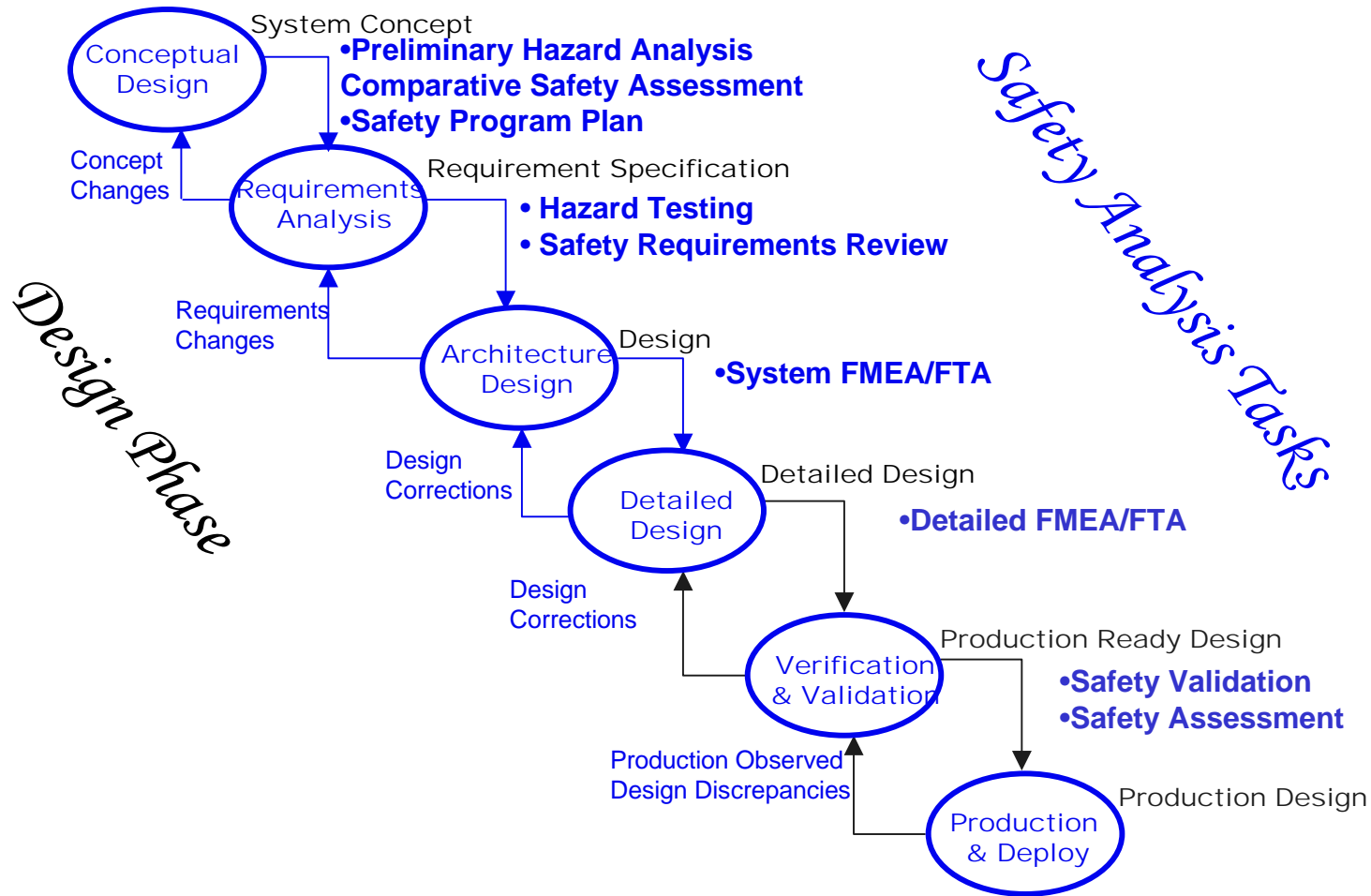


- Some of these systems control critical vehicle functions
 - Increased electronics, increased intelligence
 - Software making key decisions
- When these systems deviate from their intended behavior, the overall consequence can be a safety concern under some conditions
 - Example – Simulation of a system deviating intended behavior
- **System Safety:** A systematic, comprehensive engineering effort to optimize safety
 - Goal is to identify safety related risks and eliminate/control them



DELPHI

Typical System Safety Process

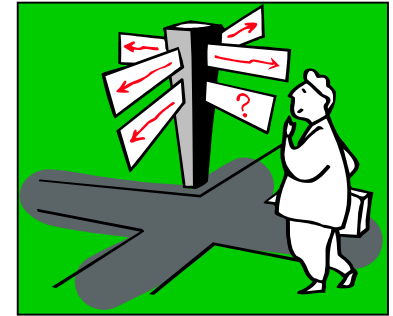


- Advanced automotive technologies are typically comprised of an integrated set of software and hardware components
 - Controllers, communication systems, hydraulic modules, and motors.
 - Such systems can exhibit dynamic behavior under real time conditions
 - Engineering analysis process can be challenging if relying on static techniques alone
- Modeling and simulation techniques can be applied to address a variety of system development issues including design robustness, safety and reliability



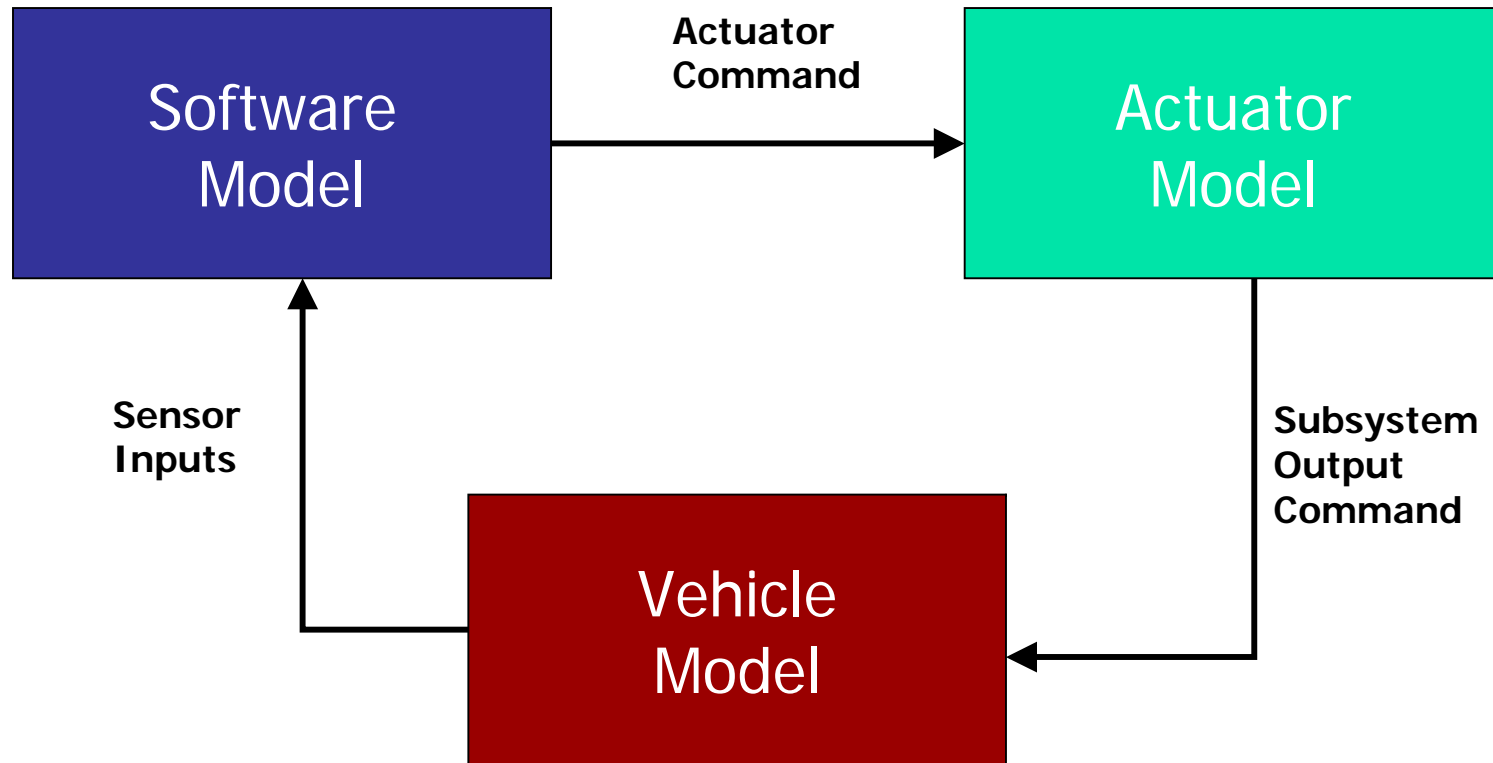
DELPHI

- Introduction
 - Simulation Modeling
 - System Safety Analysis
- **Simulation Model Development**
 - Vehicle Model, Subsystem Model, Actuator Model
 - Tools- MATLAB®, Simulink®, CarSim®, AmeSim®
- Simulation Model Validation
- Potential Hazard Analysis
 - Hazard Testing
- Summary





SUBSYSTEM



➤ System safety analysis requires a high fidelity simulation model

➤ Simulation model needs to be validated against real vehicle test data

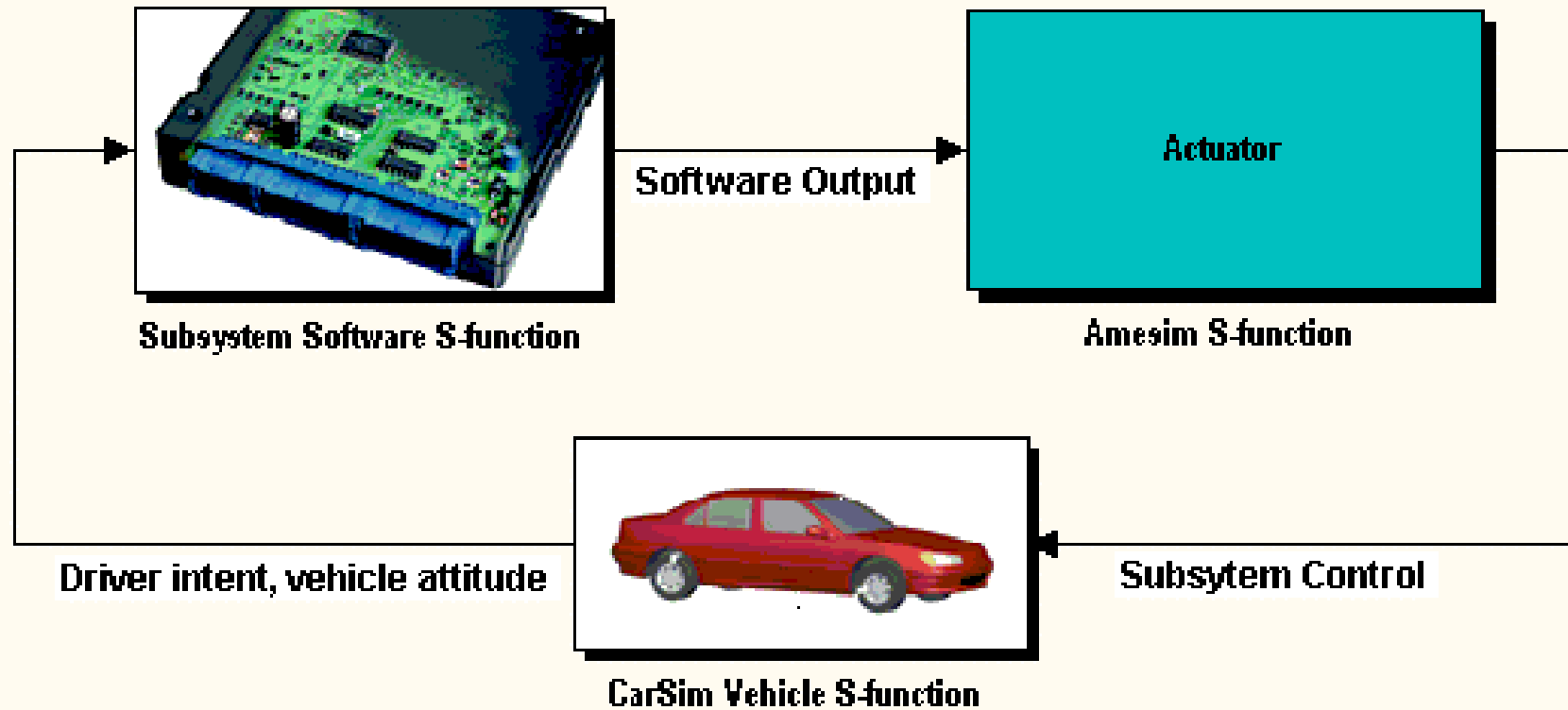


- MATLAB®/Simulink® was chosen as a common shell for simulation development
 - MATLAB® provides templates and tools to create S-functions
 - Capable for working with DLL from other simulation tools
 - Developers comfortable working with MathWorks tools
- CarSim® provides vehicle DLLs for different axle configurations
 - Provides convenient interface to work with Simulink®
 - Capable of simulation vehicle dynamics
- Amesim® compiles a DLL when the actuator model is built
 - DLL can be used as a S-function in Simulink®
 - Capable for simulating actuator dynamics



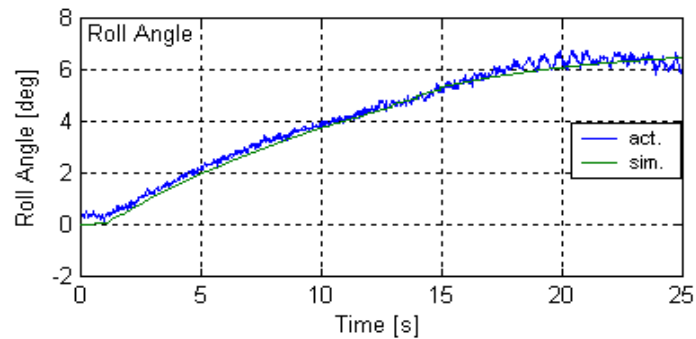
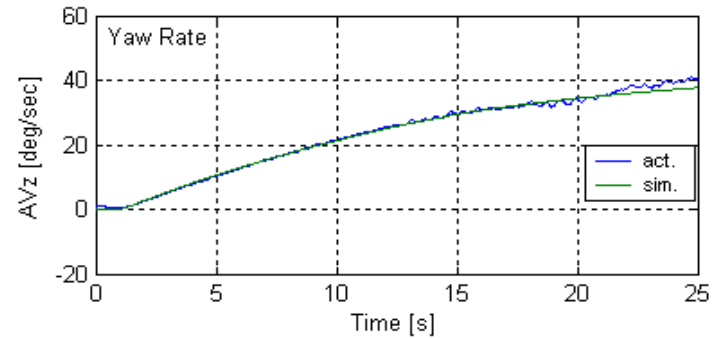
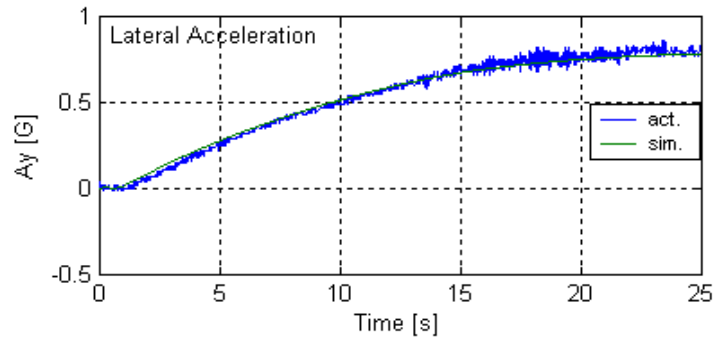
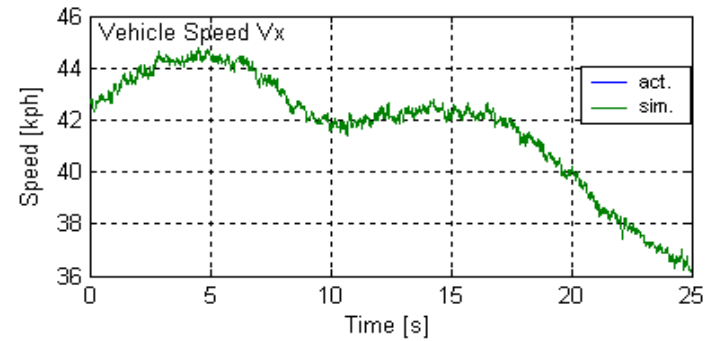
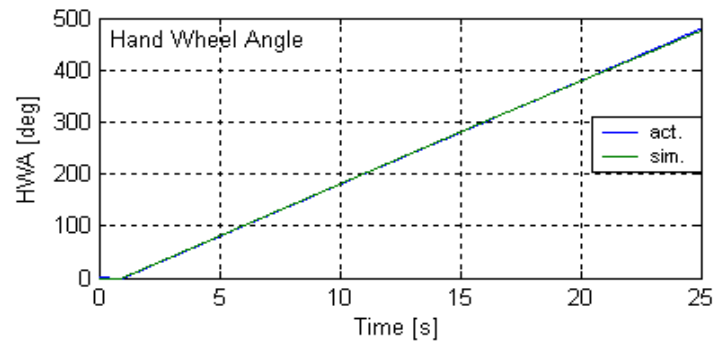
DELPHI

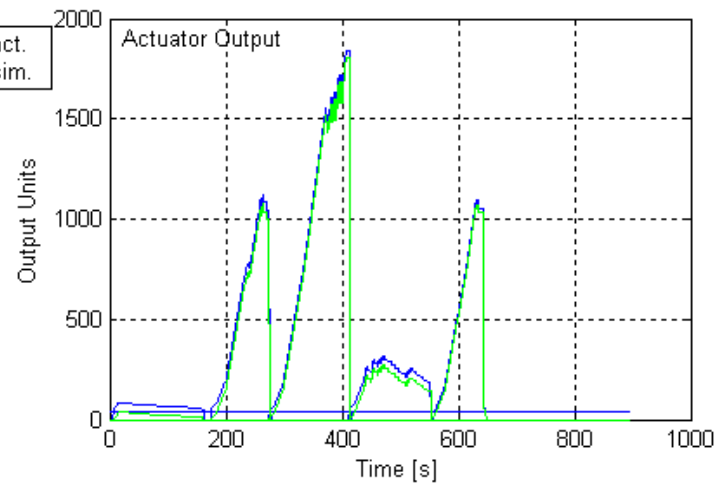
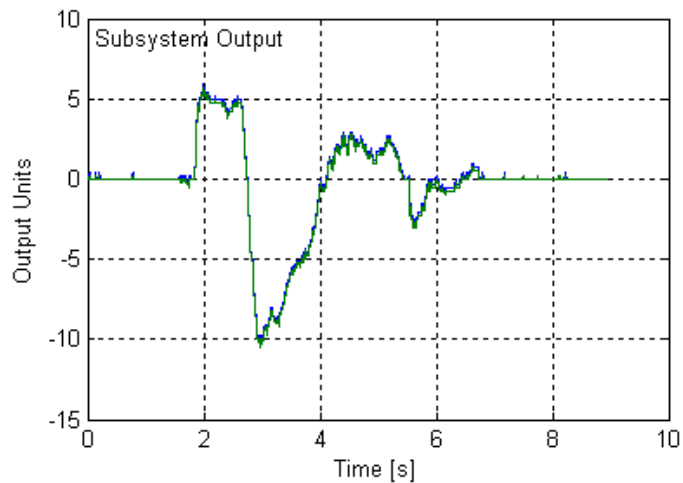
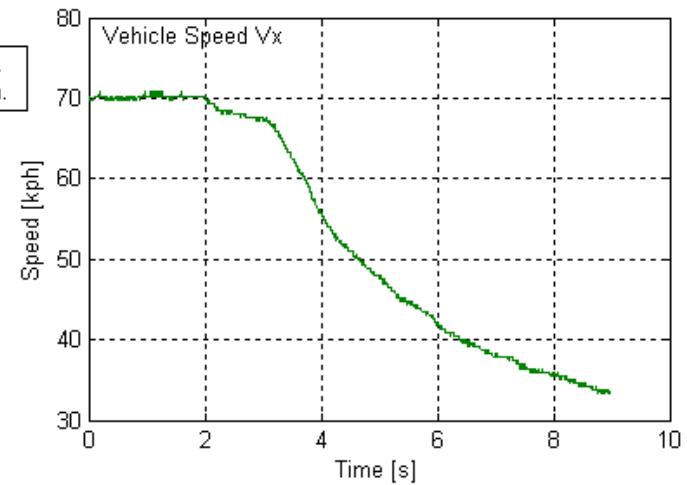
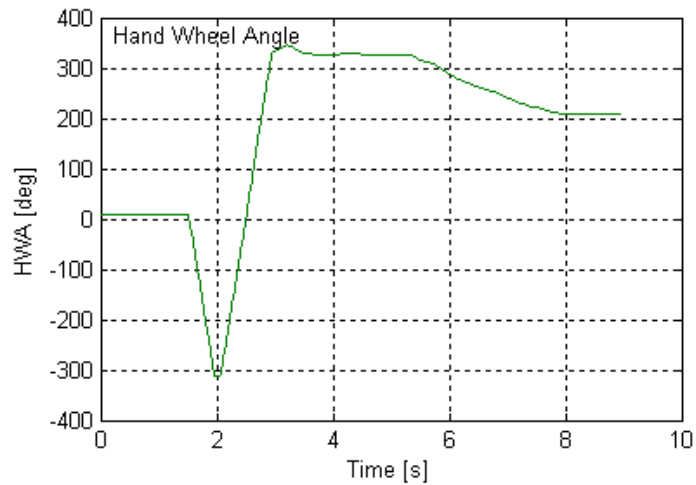
Co-Simulation Environment in Simulink



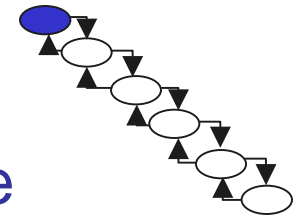
- CarSim® Vehicle Model was validated against actual vehicle test data
 - Steady state and transient maneuvers on different surfaces
 - Driver Model was validated against actual driver test results for approximate driver response time
- Co-Simulation model was validated against real test data
 - Outputs of software component and actuator component were compared against data in the vehicle for a given maneuver







- This paper discusses the Preliminary Hazard Analysis and the Hazard Test activity
- Preliminary Hazard Analysis
 - Identifies potential high-level system hazards and assesses the risk
 - Determines system safety design constraints
- For the subsystem discussed PHA identified the following potential hazards
 - Unwanted Activation
 - Incorrect Activation
 - Inadequate Activation
 - Excessive Activation

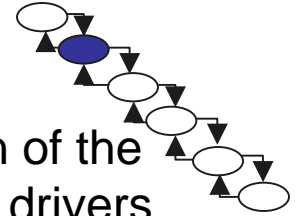


- Intent of hazard testing and analysis is to
 - Understand the vehicle behavior during unwanted activation of the subsystem actuator during normal maneuvers with average drivers
 - Determine the worst case fault response time

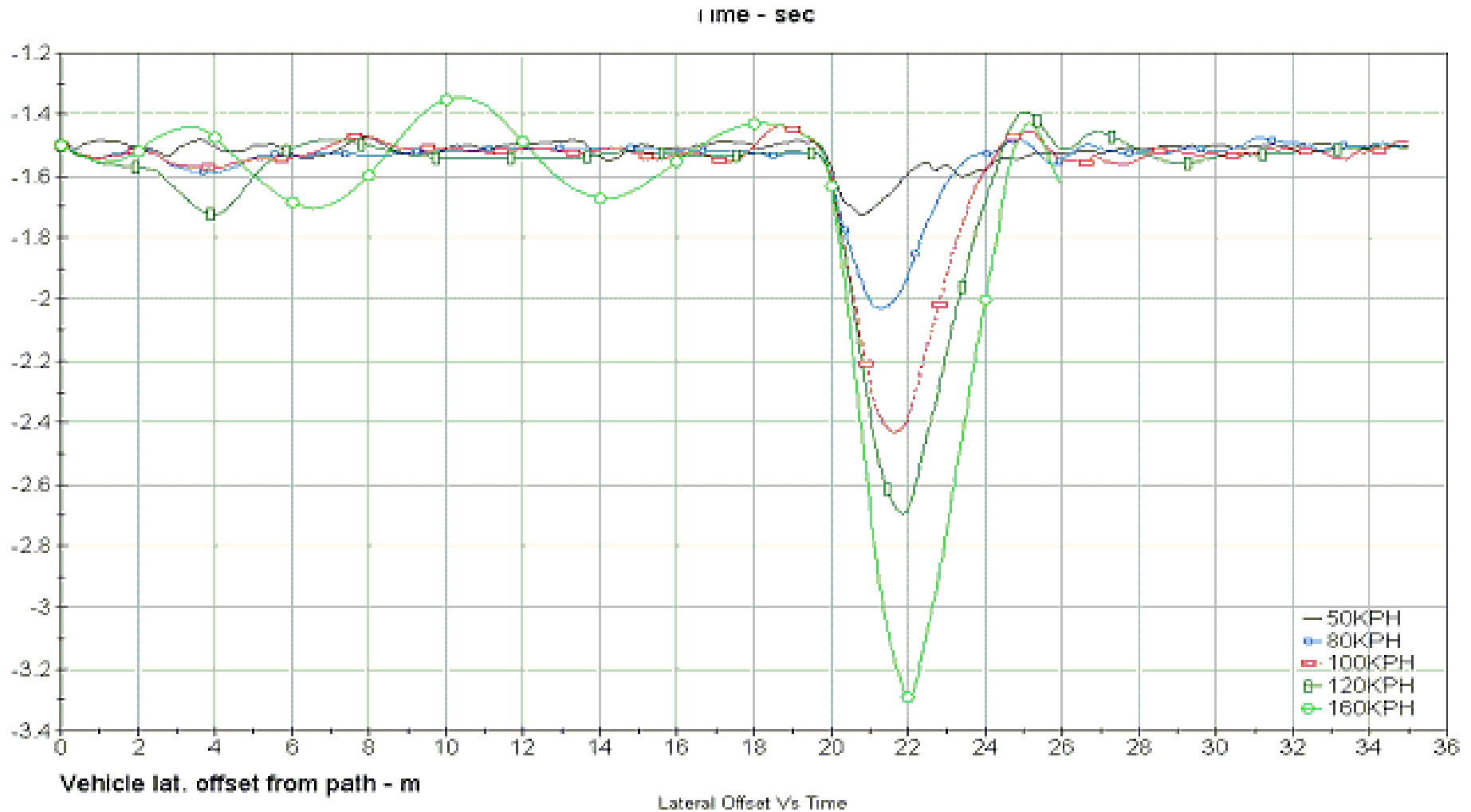
- Hazard Testing was conducted using the co-simulation model to determine the safe fault response time (FRT) for the subsystem
 - Path Deviation safety requirement used in determination of FRT

- The following slides show some of the simulation model results

- FRT used in conjunction with the PHA results to develop system safety requirements



Unwanted activation of the subsystem at varying vehicle speeds



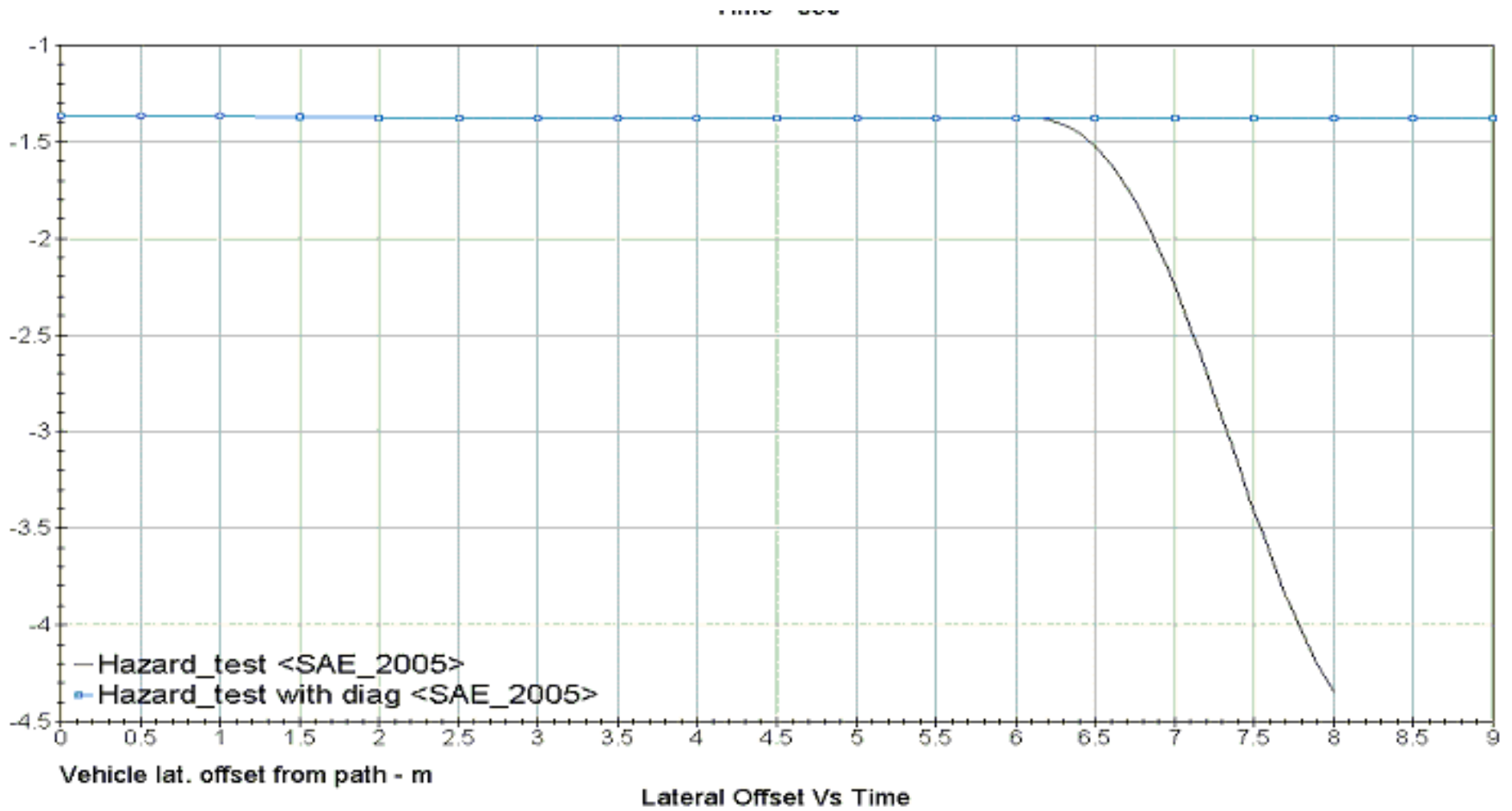
DELPHI

Hazard Test Simulation Results



Animation





DELPHI

Summary/Conclusions

- Setting up accurate simulation environment takes significant effort, time investment
- Benefits of such an investment
 - The simulation model can be used confidently for several purposes
 - **Robustness study**
 - **Safety Analysis**
 - **New algorithm development**
 - **Design validation**
- Simulation model can be successfully used in safety analysis tasks to support static analysis activities
 - Next steps – Simulation model for algorithm/software FMEA

