Application of STPA to a Shift by Wire System

(GM-MIT Research Project)

GM Team
Joe D'Ambrosio
Rami Debouk
Dave Hartfelder
Padma Sundaram
Mark Vernacchia
Sigrid Wagner

MIT Team
John Thomas
Seth Placke

Table of Contents

- Introduction
- STPA Application
    - Step 0: Hazards/Accidents, Control Structure
    - Step 1: Identify Unsafe Control Actions, Safety Constraints
    - Step 2: Causal Factors, refine detailed safety requirements
- Summary
- Conclusion/Next Steps

Introduction

- Electronics and software content continue to increase in automotive systems
- Safety-critical systems require disciplined and comprehensive engineering effort to identify safety related risks and eliminate or control them
  - Need to address both random and systematic concerns
  - Internally developed robust processes have been put in place to verify the integrity of these systems since the launch of electronic throttle control (ETC) in 1997
    - System safety process was influenced by MIL STD 882 and has been updated to be consistent with ISO26262

Introduction

- As part of the continuous improvement of our system safety process, we are open to evaluating new techniques that may enhance effectiveness and efficiency
  - It is in this context that we did a preliminary experiment applying STPA to a simple engine control system last year
  - We found the technique to be valuable and wanted to explore further
- This year, we have started a research project with MIT to pursue the following joint goals:
  - Continue STPA benefit study with an automotive system
  - Evaluate how to incorporate it within the GM system safety process
  - MIT to explore improvement opportunities for STPA step 2 (Causal Factors)
  - Broaden MIT STPA team exposure to automotive systems
  - Broaden GM System Safety Team Exposure to STPA
  - Use automotive system example for possible STPA/STAMP enhancements

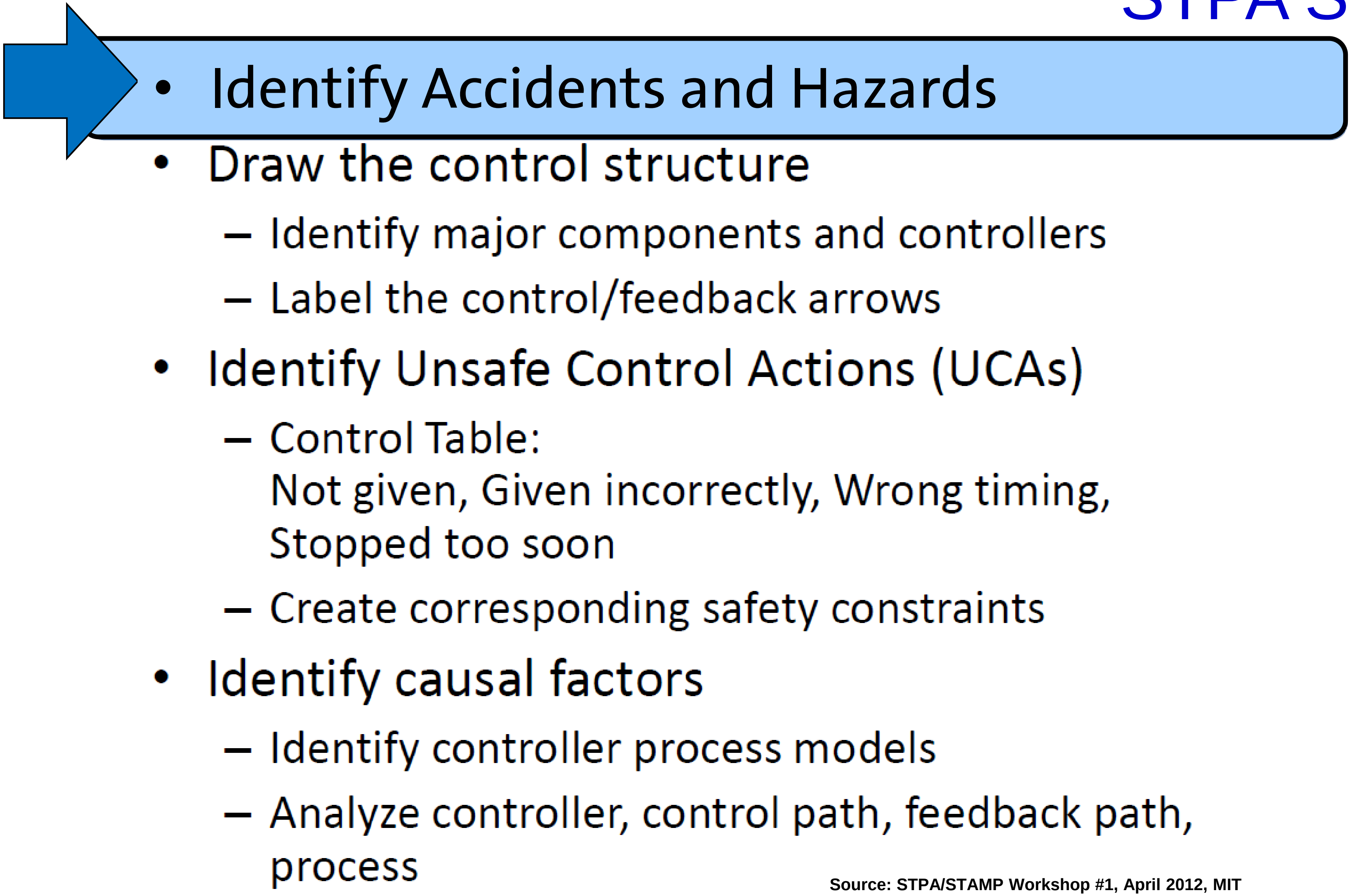
STPA Evaluation Study

- As part of the study we have started applying STPA to a generic automotive shift by wire system
  - Shift by Wire system is a electronic control system that enables electronic automotive transmission range selection
    - Park, Drive, Reverse, Neutral, positions achieved electronically
    - Mechanical linkage between shifter & transmission is eliminated

- Study is on-going; plan to complete by end of 2014

- In the following slides we share our interim results

STPA Steps



- Identify Accidents and Hazards
- Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions (UCAs)
  - Control Table:
    Not given, Given incorrectly, Wrong timing,
    Stopped too soon
  - Create corresponding safety constraints
- Identify causal factors
  - Identify controller process models
  - Analyze controller, control path, feedback path, process

Source: STPA/STAMP Workshop #1, April 2012, MIT

STAMP Model: Accident Evaluation for Automotive Systems

Accident	Description
A-1	Two or more vehicles collide
A-2	Vehicle collides with non-fixed obstacle[1]
A-3	Vehicle crashes into terrain[2]
A-4	Vehicle occupants injured without vehicle collision

[1] ‘Other obstacle’ includes pedestrians, bikers, animals, etc.

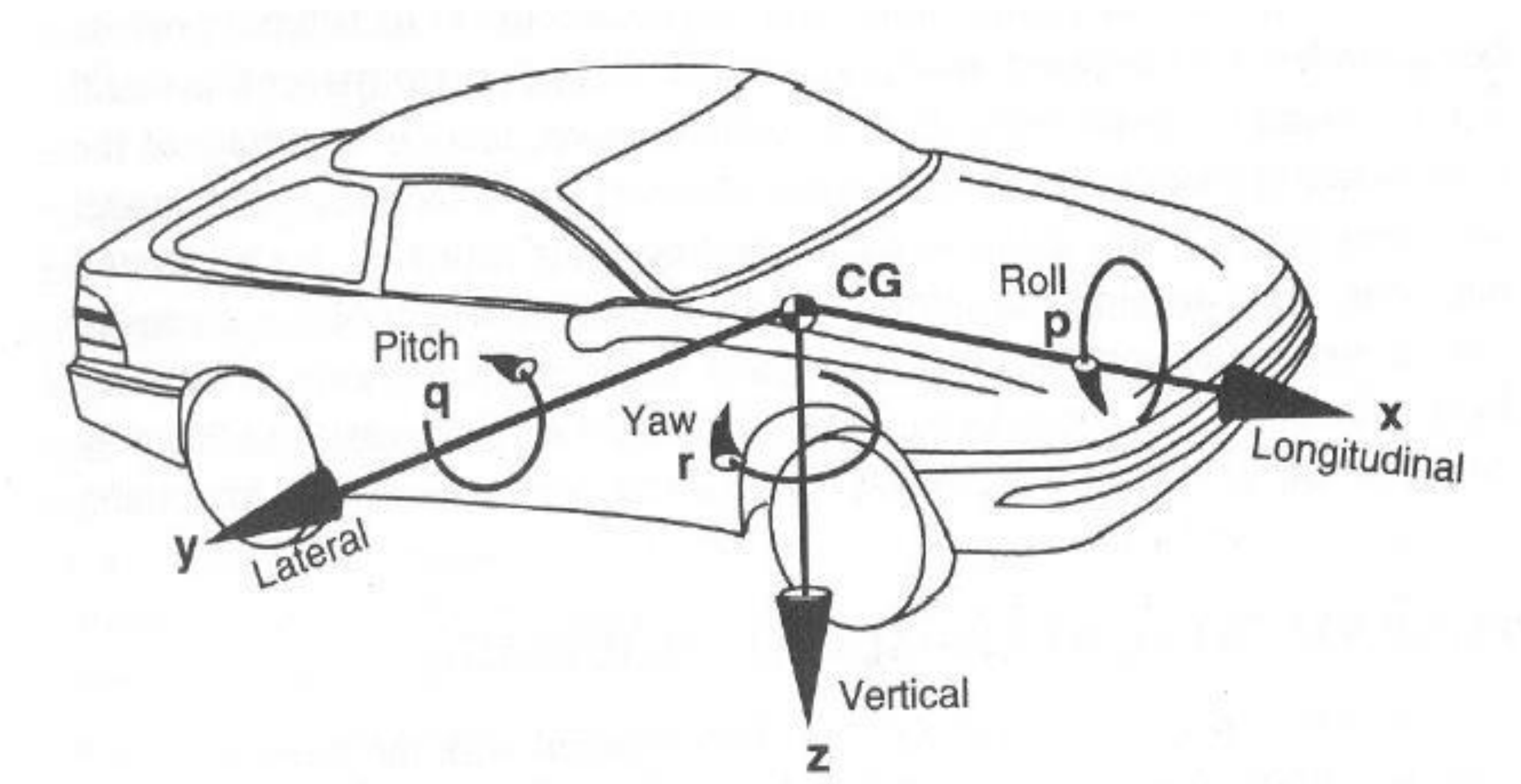
[2] ‘Terrain’ includes fixed, permanent objects such as guard rails, trees, bridges, signage, pavement, etc.

System Level Hazards

Hazard	Description	Accident
H-1	Vehicle does not maintain safe distance from nearby vehicles	A-1
H-2	Vehicle does not maintain safe distance from terrain and other obstacles	A-2, A-3
H-3	Vehicle enters uncontrollable or unrecoverable state	A-1, A-2, A-3, A-4
H-4	Vehicle occupants exposed to harmful effects and/or health hazards	A-4

Motion Control Vehicle Level Hazards (Example)

Comparing the hazards derived based on vehicle motion



Source: SAE Vehicle Axes

Note: In this presentation, only motion control vehicle hazards are being considered

Vehicle Level Hazards For Shift By Wire

- Based on the 3 primary degrees of freedom of vehicle, the Table on the right shows the generic vehicle level motion control hazards that are possible
- Hazards are based on motion control properties that can be potentially affected by malfunctioning electrical/electronic control systems
- Applicable motion hazards are highlighted and are mapped to STAMP System Level Hazards

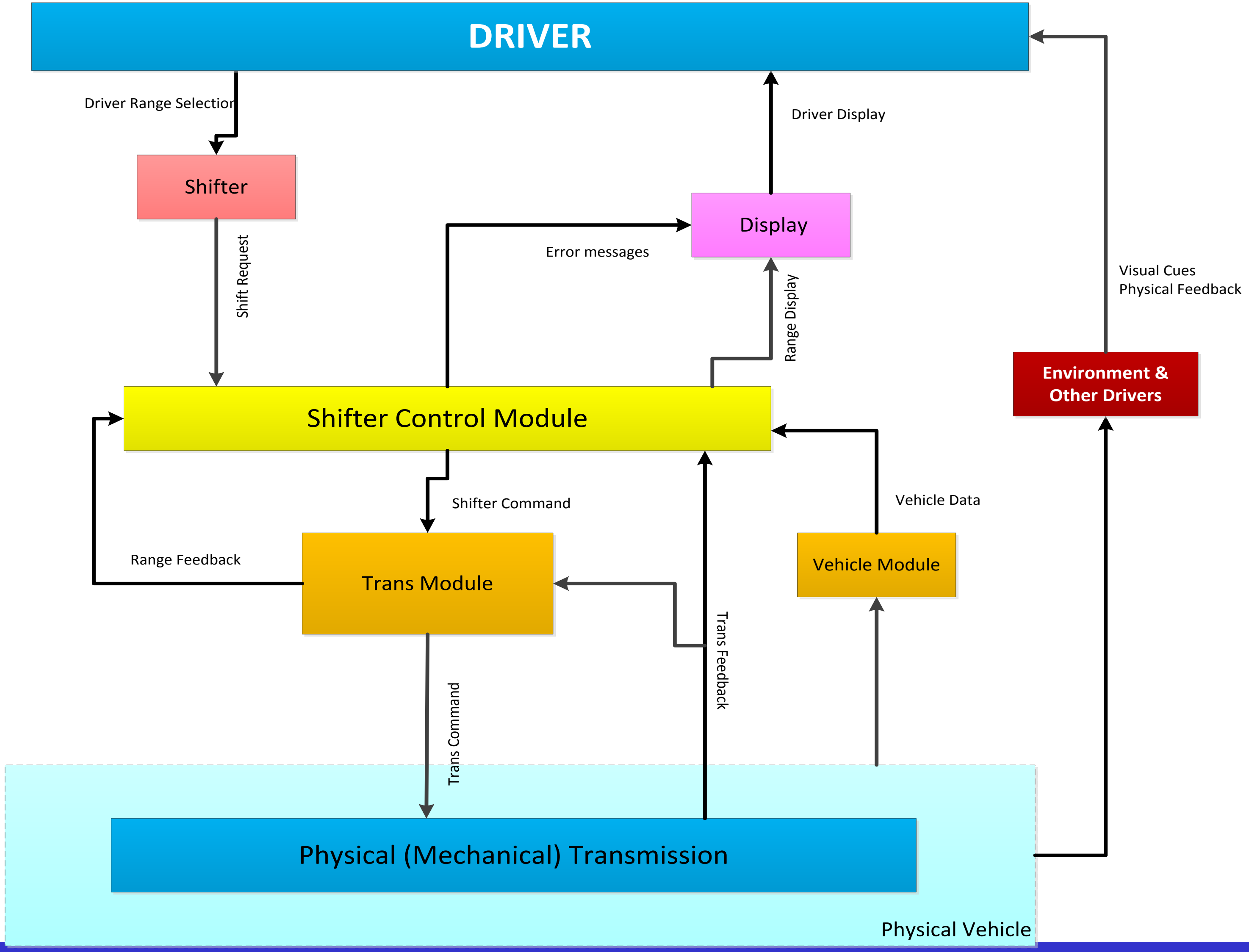
Potential Vehicle Level Motion Hazards
Unintended Longitudinal Vehicle Acceleration
Loss/Reduced Longitudinal Vehicle Acceleration
Unintended Vehicle Motion (Wrong Direction) H1, H2
Unintended Propulsion Engage (or Power flow) H1, H2
Loss of Propulsion (or Power flow) H1, H2, H3
Unintended Vehicle Motion (Rollaway) H1, H2, H3
Loss of Longitudinal Vehicle Motion H1, H2, H3
Unintended Vehicle Deceleration
Loss/Reduced Vehicle Deceleration
Unintended Lateral Vehicle Motion
Loss of Lateral Vehicle Motion
Unintended Vehicle Yaw
Unintended Vehicle Vertical Motion/Roll

STPA Steps

- Identify Accidents and Hazards
- Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions (UCAs)
  - Control Table:
    Not given, Given incorrectly, Wrong timing,
    Stopped too soon
  - Create corresponding safety constraints
- Identify causal factors
  - Identify controller process models
  - Analyze controller, control path, feedback path, process

Source: STPA/STAMP Workshop #1, April 2012, MIT

Generic Shift By Wire Control Structure



STPA Steps

- Identify Hazards
- Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions (UCAs)
  - Control Table:
    Not given, Given incorrectly, Wrong timing, Stopped too soon
  - Create corresponding safety constraints
- Identify causal factors
  - Identify controller process models
  - Analyze controller, control path, feedback path, process

Source: STPA/STAMP Workshop #1, April 2012, MIT

STPA Step 1

- Shift Control Module Responsibilities:
  - Engage the transmission range (PRND) selected by the driver <u>unless unavailable or inconsistent</u>
  - Do not allow ranges that are unavailable or inconsistent
  - Notify driver of any problems that arise

- Definitions:
  - <u>Range Unavailable</u>: A physical fault has been detected that would prevent the range from being properly achieved
  - <u>Range Inconsistent</u>: Based on current sensor information (wheel speed, etc.), the new range would not be achievable, could cause physical damage, or would cause unsafe change in motion

STPA Step 1: Unsafe Control Actions -Shift Control Module- Example

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopped Too Soon or Applied Too Long
Transmission Range Command	UCA-1: Shift Control Module does not provide range command when driver selects available and consistent range	UCA-3: Shift Control Module provides range command without driver new range selection and without current range becoming unavailable/inconsistent	UCA-7: Shift Control Module provides range command too late after driver range selection	N/A
	UCA-2: Shift Control Module does not provide new range command once current range becomes unavailable	UCA-4: Shift Control Module provides range command that does not match a new range selection provided by driver	UCA-8: Shift Control Module provides range commands consistent with driver selection but in different order	
		UCA-5: Shift Control Module provides range command when that range is unavailable		
		UCA-6: Shift Control Module provides range command inconsistent with vehicle motion		

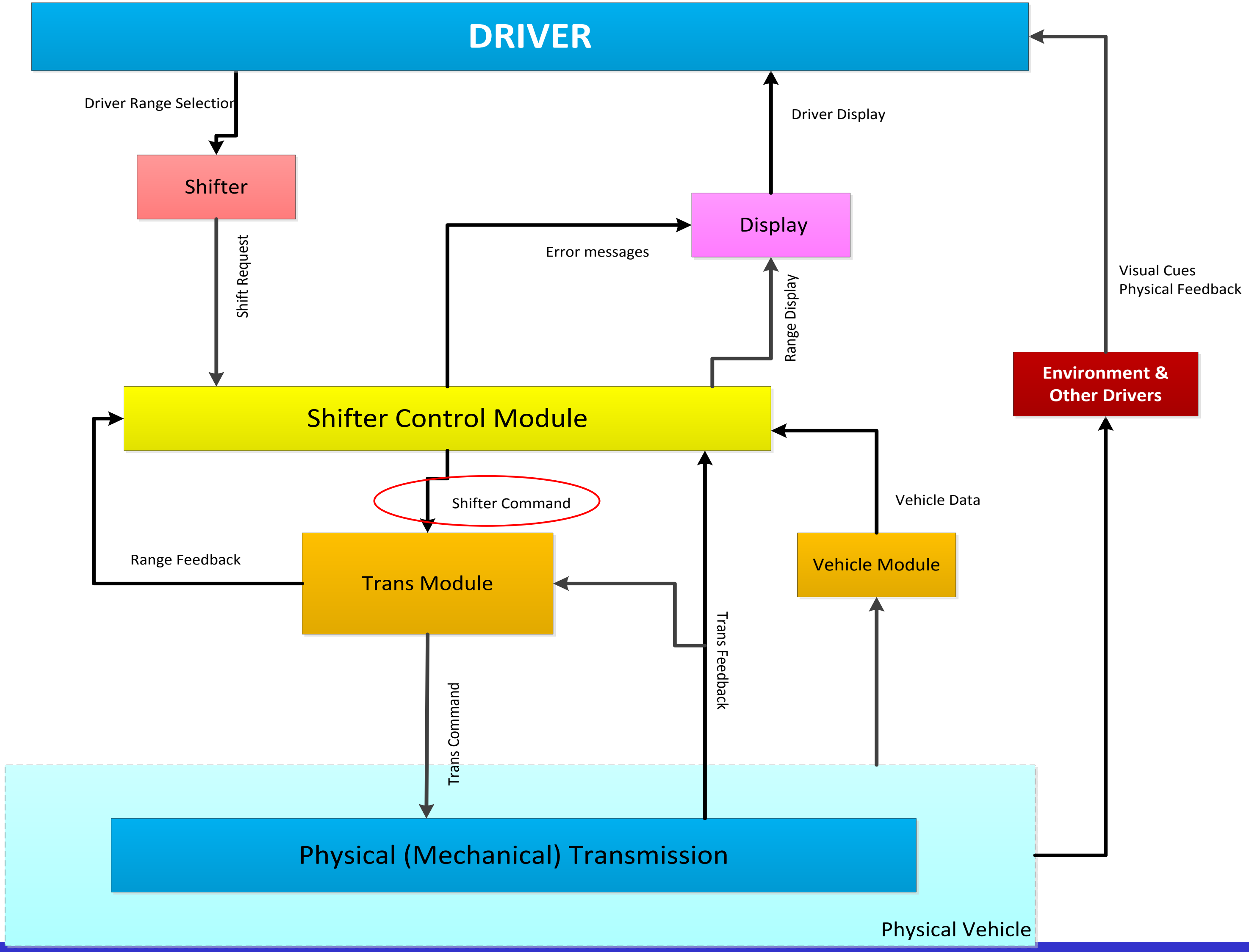
System Safety requirements derived from UCAs

STPA Steps

- Identify Accidents and Hazards
- Draw the control structure
  - Identify major components and controllers
  - Label the control/feedback arrows
- Identify Unsafe Control Actions (UCAs)
  - Control Table:
    Not given, Given incorrectly, Wrong timing, Stopped too soon
  - Create corresponding safety constraints
- Identify causal factors
  - Identify controller process models
  - Analyze controller, control path, feedback path, process

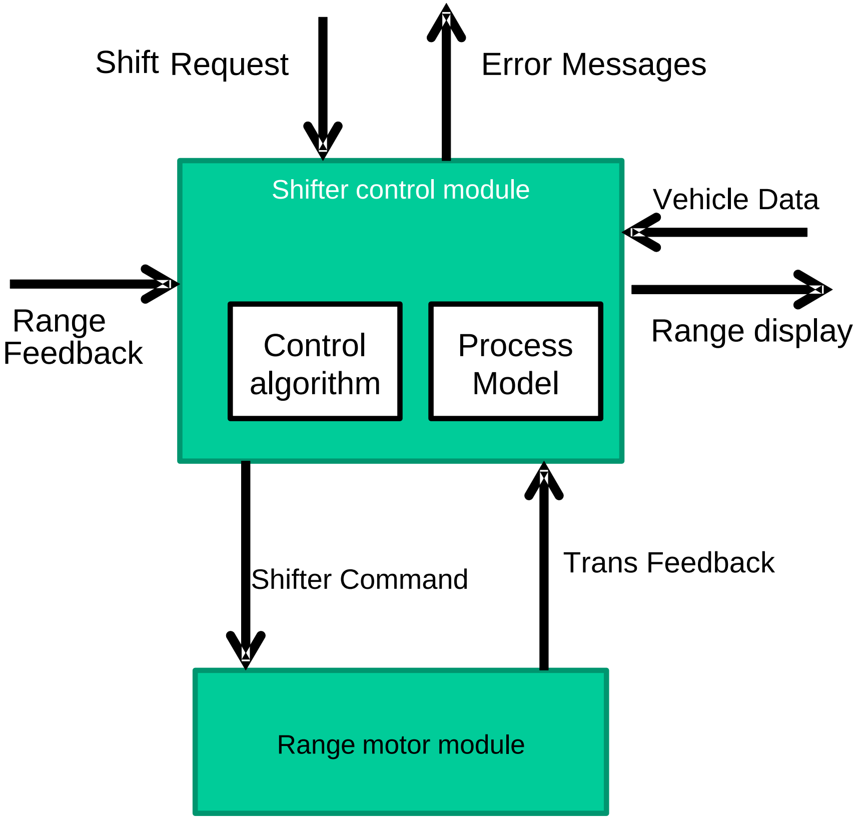
Source: STPA/STAMP Workshop #1, April 2012, MIT

Generic Shift By Wire Control Structure



STPA Step 2: Causal Factors Analysis Example

UCA-3: Shift Control Module provides range command without driver new range selection and without current range becoming unavailable/inconsistent



Safety requirements derived from the analysis

- Control algorithm flaws
  - …
- Process model flaws
  - SCM incorrectly believes driver requested a new range
  - …
- Inadequate Information for Range Selection Command Computation
  - Shift lever sequence is incorrect/missing/delayed
  - Range incorrectly reported as unavailable/inconsistent
  - …
- SCM does not provide range command, but it is executed
  - Shared data bus problem?
  - Another controller provides range command?
  - …

Summary

- Excellent hands on learning opportunity for GM Safety Engineers
- Effort demonstrates that STPA is iterative
    - Example: Control structure evolves as we apply STPA and learn more about the system
    - Iterative process works well as effort moves from concept level to more detailed design level
- Additional guidance needed for the Causal Factors step to produce consistent results
    - Experience suggests that MIT STPA Causal Factors (step 2) could be made more systematic
- Explore additional opportunities for STPA process enhancement

Conclusions/Next Steps

- GM continues to believe that STPA technique is valuable and different from other techniques

- GM safety team will continue working with MIT on this project

- Opportunities will be explored for incorporating STPA to enhance the efficiency of GM’s system safety engineering process where appropriate

- Joint team (GM and MIT) will continue to use the project results to expand and enhance MIT STPA Technique as appropriate

Thank You