Iterative Application of STPA for an Automotive System

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

MIT Team
John Thomas

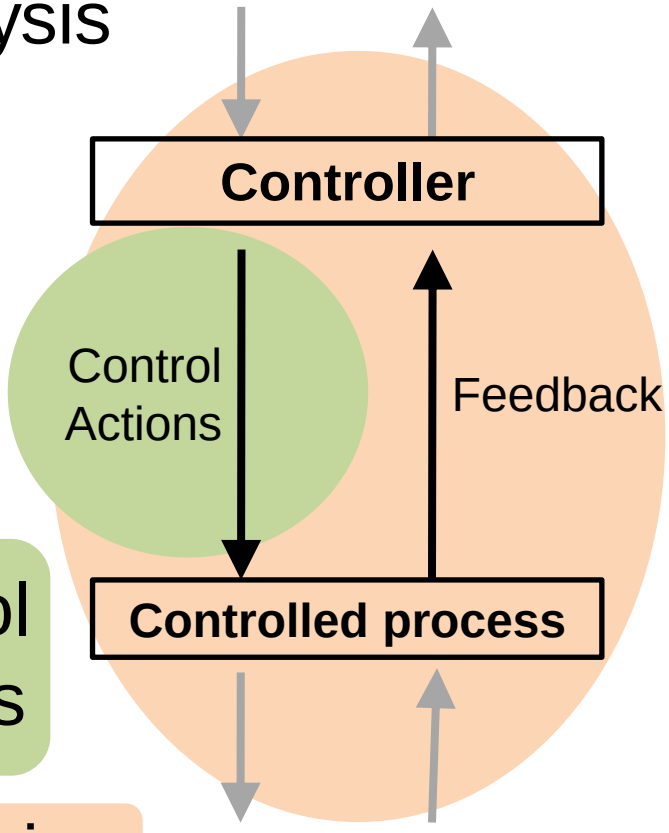
Table of Contents

- 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

- 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 in 2013
  - We found the technique to be valuable and wanted to explore further
- In 2014, we started a research project with MIT to continue to study the benefits of STPA
- Case study: 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

- Once initial STPA is done at a high level, how to iterate and add detail?
  - Provide guidance to efficiently get from one iteration to the next?
  - Can we perform the STPA analysis as design decisions are being made (without starting over)?
  - How to intelligently add detail only as necessary?

- Establish foundation for analysis
  - Define accidents
  - Define system hazards
  - Rewrite hazards as safety constraints
  - Draw safety control structure
- Step 1: Identify unsafe control actions and safety constraints
- Step 2: Identify causal scenarios



Accidents and Hazards

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

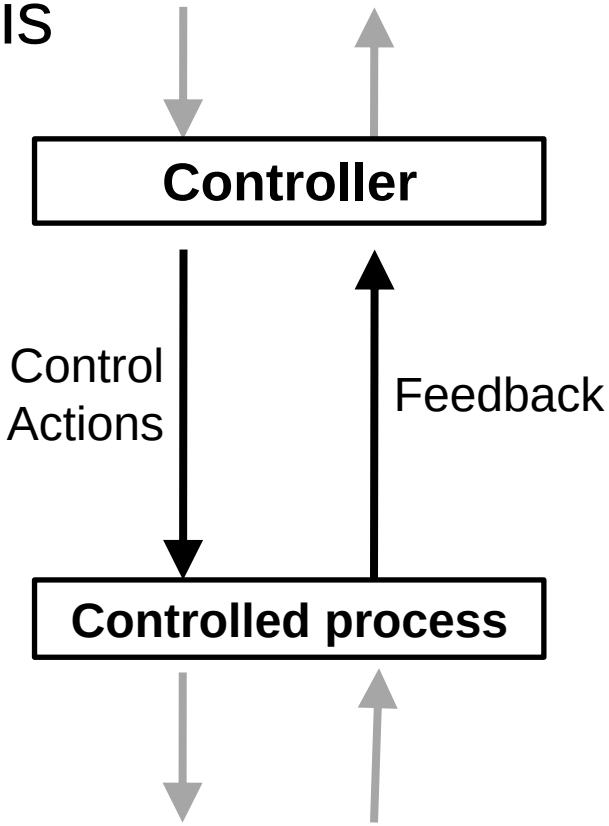
[1] ”Other obstacle” includes pedestrians, bikers, animals, etc.
[2] ”Terrain” includes fixed, permanent objects such as guard rails, trees, bridges, signage, pavement, etc.

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 occupants exposed to harmful effects and/or health hazards	A-4

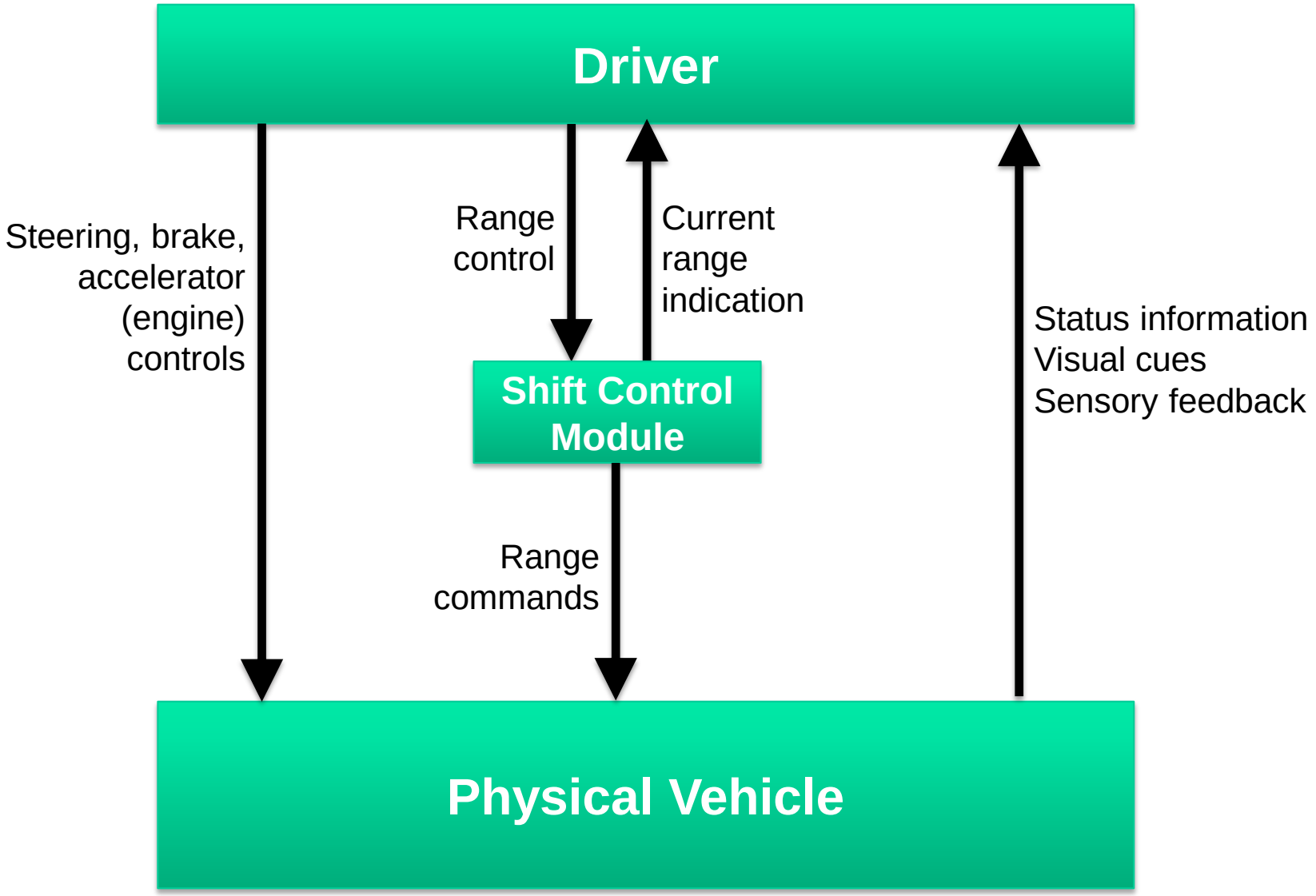
System-level safety constraints

- SC-1: Vehicle must maintain safe distance from nearby vehicles
- SC-2: Vehicle must maintain safe distance from terrain and other obstacles
- SC-3: Vehicle must not expose occupants to harmful effects and/or health hazards

- Establish foundation for analysis
  - Define accidents
  - Define system hazards
  - Rewrite hazards as safety constraints
  - Draw safety control structure
- Step 1: Identify unsafe control actions and safety constraints
- Step 2: Identify causal scenarios



Control structure for vehicle



*Similar for both mechanical/electrical implementations

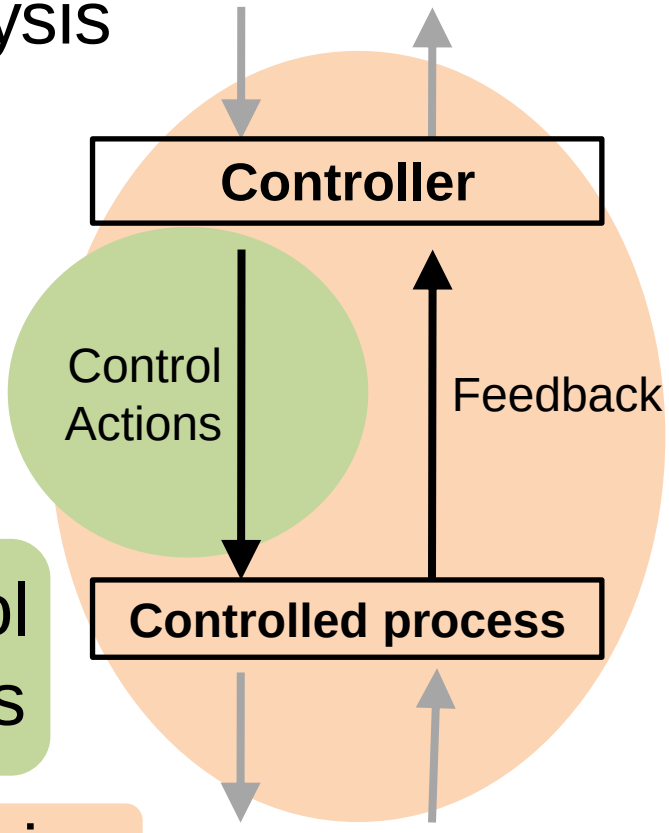
Unsafe control actions for shifter control module

Control Action	Not Providing	Providing	Too early/too late/wrong order	Stopped too soon /Applied too long
Range command	UCA-1: Shifter Control Module does not provide range command when driver selects new range [H-1, H-2, H-3] UCA-2: Shifter Control Module does not provide new range command once current range becomes unavailable [H-1, H-2, H-3]	UCA-3: Shifter Control Module provides range command without driver new range selection [H-1, H-2, H-3] UCA-4: Shift Control Module provides range command for an unavailable range [H-1, H-2] UCA-5: Shift Control Module provides inconsistent range command [H-1, H-2, H-3]	UCA-6: Shifter Control Module provides range command too late after driver range selection [H-1, H-2, H-3] UCA-7: Shift Control Module provides range commands consistent with driver selection but in different order [H-1, H-2, H-3]	N/A

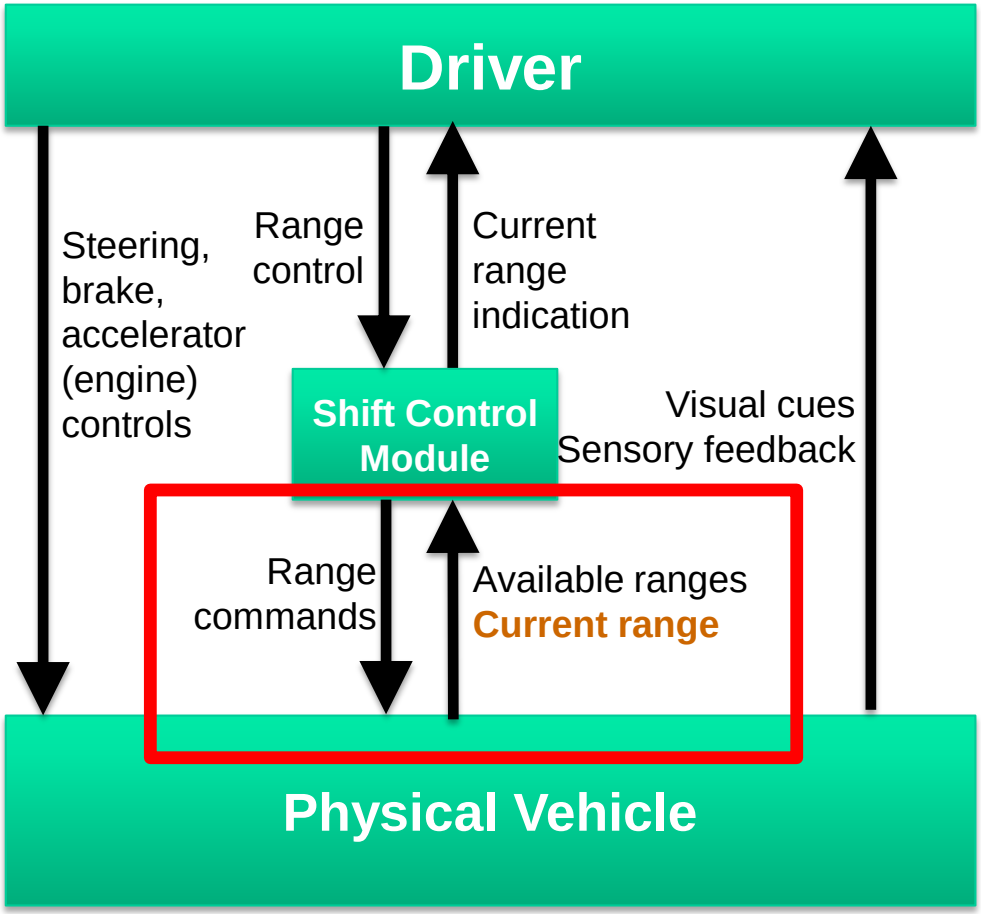
Inconsistent: The requested range would cause physical damage, an unsafe change in motion, or violate motor vehicle regulations.
Unavailable: A physical fault occurs that would prevent the vehicle from shifting to the selected range.

- **SC-1**: Shifter Control Module must provide range command when driver selects new range
- **SC-2:** Shifter Control Module must provide new range command once current range becomes unavailable
- **SC-3:** Shifter Control Module must not provide range command without driver new range selection
- **SC-4:** Shifter Control Module must not provide range command when that range is unavailable
- **SC-5:** Shifter Control Module must not provides range commands that are inconsistent

- Establish foundation for analysis
  - Define accidents
  - Define system hazards
  - Rewrite hazards as safety constraints
  - Draw safety control structure
- Step 1: Identify unsafe control actions and safety constraints
- Step 2: Identify causal scenarios



UCA-1: Shifter Control Module does not provide range command when driver selects new range



Scenarios:

- Shifter Control Module does not provide range command because it *incorrectly believes no new range was selected*
- Shift Control Module does not provide range command because it ***incorrectly believes the range was already achieved***
  - *Missing feedback about the current range!*
  - *If previous command wasn't successful, would never be detected*
- Etc.

Each Iteration has Different Goals

Iteration #1

- Very quick
- Produced immediate results for the design

Iteration #2

- More careful analysis
  - Make sure nothing was missed
- Add design detail
- Address any control flaws that could not be eliminated in #1

Formalize step 1
Check for missing UCAs, conflicts, formal requirements

More detailed step 2
Add sensors & actuators, identify detailed scenarios, mitigations

Apply rigorous/formal STPA Step 1

Controller	Control Action	Current range available	Not Providing Causes Hazards	Providing Causes Hazards
SCM	Range command	No	Yes	

UCA-2:

Shifter Control Module does not provide new range command when current range becomes unavailable

Rigorous/formal STPA Step 1

Control Action	Driver Selected Range	SCM Selected Range Available	SCM Selected Range Consistent	Current range available	Not Providing Causes Hazards	Providing Causes Hazards
Transmission Range command	None	*	*	*		Yes
	*	*	*	No	Yes	
	Doesn't match SCM cmd	*	*	*		Yes
	Matches SCM cmd	*	*	*	Yes	
	Matches SCM cmd	No	*	*		Yes
	Matches SCM cmd	*	No	*		Yes

Rigorous/formal STPA Step 1

Control Action	Driver Selected Range	SCM Selected Range Available	SCM Selected Range Consistent	Current range available	Not Providing Causes Hazards	Providing Causes Hazards	
Transmission Range command	None	*	*	*		Yes	UCA-3
	*	*	*	No	Yes		UCA-2
	Doesn't match SCM cmd	*	*	*		Yes	
	Matches SCM cmd	*	*	*	Yes		UCA-1
	Matches SCM cmd	No	*	*		Yes	UCA-4
	Matches SCM cmd	*	No	*		Yes	UCA-5

Rigorous/formal STPA Step 1

Control Action	Driver Selected Range	SCM Selected Range Available	SCM Selected Range Consistent	Current range available	Not Providing Causes Hazards	Providing Causes Hazards	
Transmission Range command	None	*	*	*		Yes	UCA-3
	*	*	*	No	Yes		UCA-2
	Doesn't match SCM cmd	*	*	*		Yes	
	Matches SCM cmd	*	*	*	Yes		UCA-1
	Matches SCM cmd	No	*	*		Yes	UCA-4
	Matches SCM cmd	*	No	*		Yes	UCA-5

Identified new UCA

*Dajiang Suo

Unsafe control actions for shifter control module

Control Action	Not Providing	Providing	Too early/too late/wrong order	Stopped too soon /Applied too long
Range command	UCA-1: Shifter Control Module does not provide range command when driver selects new range [H-1, H-2, H-3] UCA-2: Shifter Control Module does not provide new range command once current range becomes unavailable [H-1, H-2, H-3]	UCA-3: Shifter Control Module provides range command without driver new range selection [H-1, H-2, H-3] **UCA-8: Shift Control Module provides range command that does not match the new range selection provided by the driver [H-1, H-2, H-3]** UCA-4: Shift Control Module provides range command when that range is unavailable [H-1, H-2] UCA-5: Shift Control Module provides inconsistent range command [H-1, H-2, H-3]	UCA-6: Shifter Control Module provides range command too late after driver range selection [H-1, H-2, H-3] UCA-7: Shift Control Module provides range commands consistent with driver selection but in different order [H-1, H-2, H-3]	N/A

Inconsistent: The requested range would cause physical damage, an unsafe change in motion, or violate motor vehicle regulations.
Unavailable: A physical fault occurs that would prevent the vehicle from shifting to the selected range.

Each Iteration has Different Goals

- Iteration #1
  - Very quick
  - Produced immediate results for the design

- Iteration #2
  - More careful analysis
    - Make sure nothing was missed
  - Add design detail
  - Address any control flaws that could not be eliminated in #1

Formalize step 1
Check for missing UCAs, conflicts, formal requirements

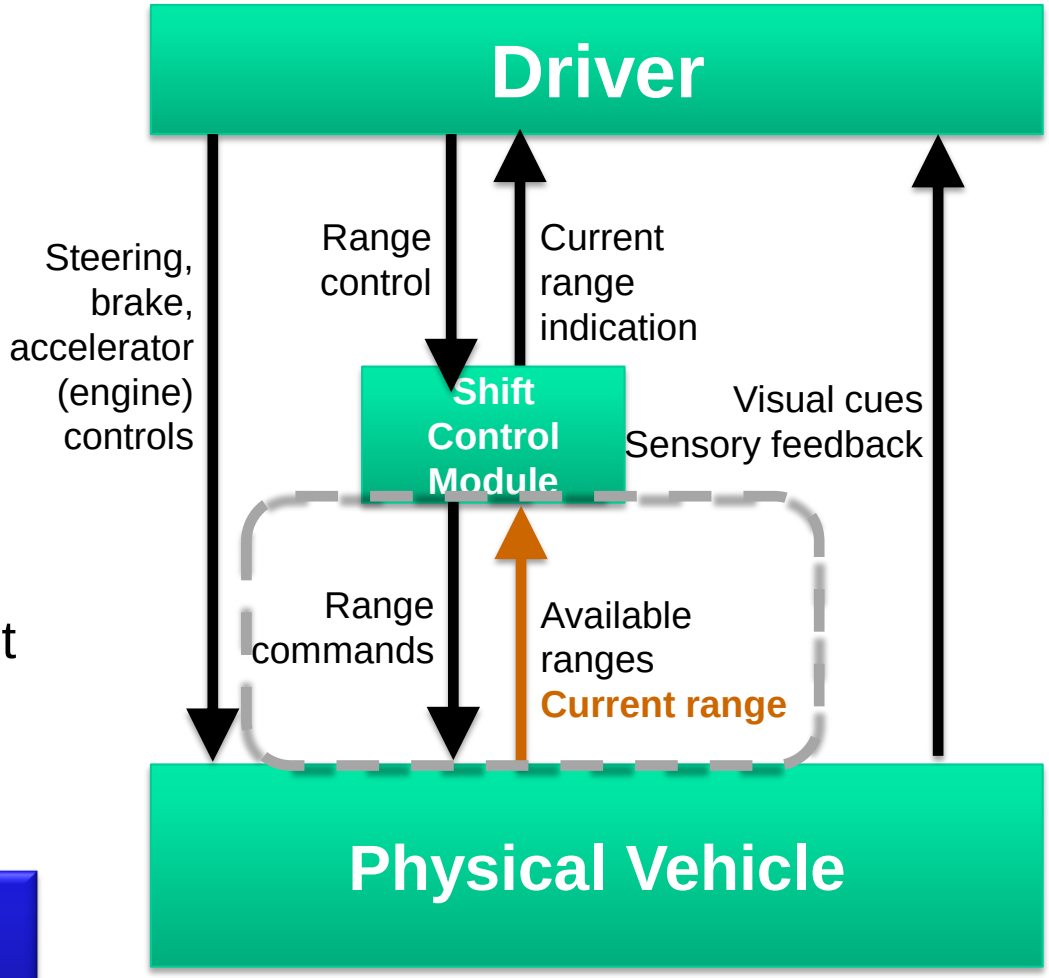
More detailed step 2
Add sensors & actuators, identify detailed scenarios, mitigations

From Iteration #1:

- **Scenario:** Shifter Control Module does not provide range command because it **receives incorrect feedback that the range is already selected**

- Safety constraint: Current range feedback must be correct
  - Not helpful by itself
  - Now what? Enforce this how?

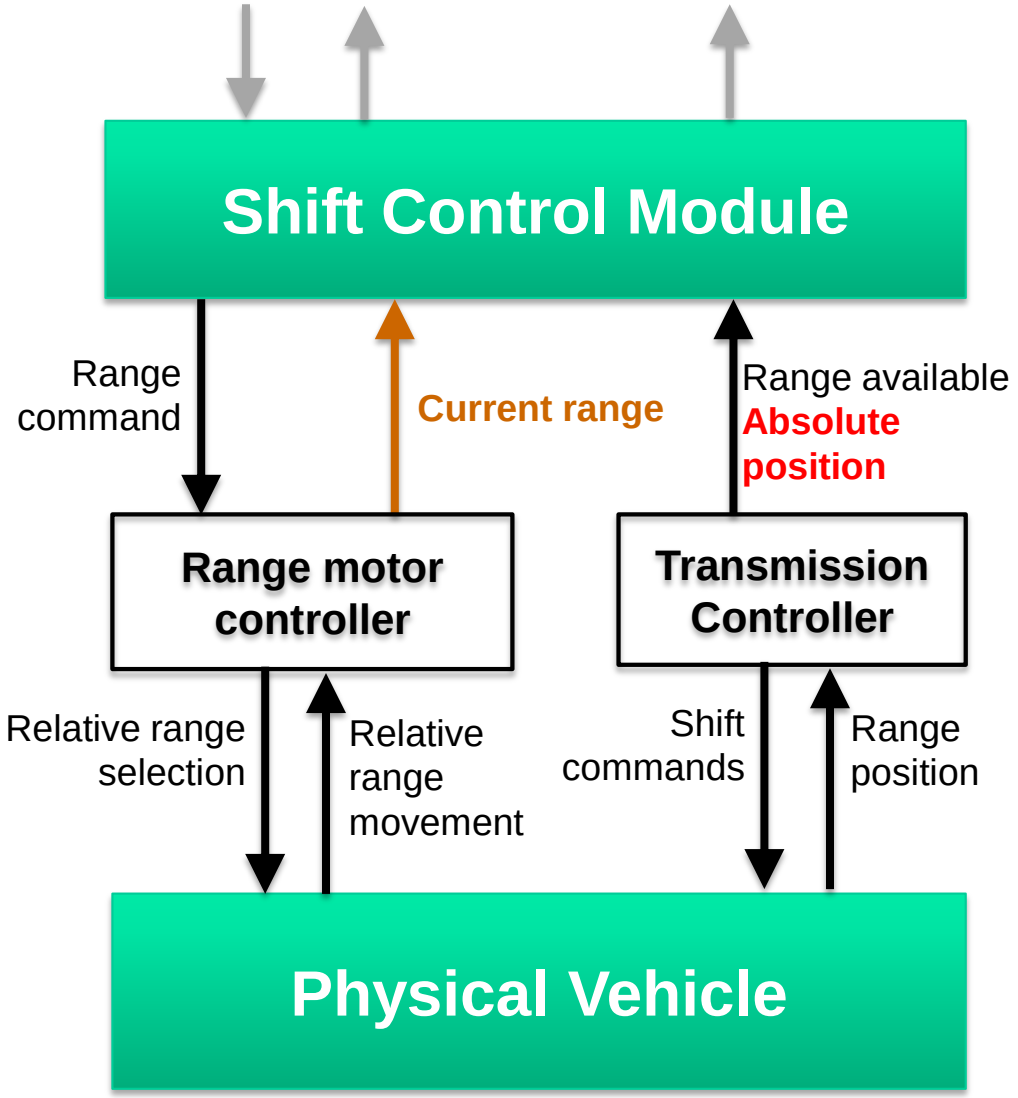
Need more detailed safety requirement



Need to “zoom in”, add detail

STPA Step 2

- **Potential solution:**
  Require transmission controller to report **absolute range position**
- Revise control structure accordingly
- Analyze potential new scenarios introduced by the revision



Iteration #1

STPA	Design

Initial control structure

STPA Step 1

Revise control structure based on safety constraints

STPA Step 2

Eliminate/mitigate causal factors if possible

Iteration #2

STPA	Design

Formal STPA Step 1

Resolve any new UCAs, conflicts

Detailed STPA Step 2
(for unaddressed scenarios only)

Add controls for new causal factors identified

Method Summary

GM

STAMP / STPA Integration with ISO 26262

- ISO 26262 is a Functional Safety Standard broadly used within the automotive industry
- ISO 26262 specifies requirements on the entire functional safety lifecycle
  - E.g., safety management, supplier / OEM interface agreement, safety hazard and risk analysis, safety requirements, requirements traceability, change & configuration management, verification / validation, vehicle production, …
- With respect hazard analysis, STAMP / STPA can be integrated in to an ISO 26262 functional safety lifecycle as a means to implement hazard analysis
  - Potential STAMP / STPA benefits – (1) focus on preventing system accidents, (2) effective incorporation of human factors aspects, (3) iterative development well suited for advanced development activities

Summary

- 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
  - Detailed safety requirements added as design process evolved abstract level
- Initial Step 2 scenarios done very quickly with minimal effort while not requiring a lot of detail
- Scenarios not immediately fixed were addressed in second iteration

Thank You