DEVELOPMENT OF HUMAN INTERFACE REQUIREMENTS FOR SHIFT BY WIRE (SBW) DEVICES USING STPA

March 22, 2016

Mark A. Vernacchia – GM Technical Fellow, System Safety
Bill Arnold – GM Feature Owner, Shift by Wire Systems

2016 STAMP Workshop
March 22, 2016

GENERAL MOTORS

AGENDA

- INTRODUCTION
- SHIFT BY WIRE EXAMPLES
- PROJECT OVERVIEW
- PROJECT PLAN
- KEY POINTS
- SAFETY ANALYSIS TECHNIQUE COMMENT
- STPA ACTIVITIES
- TRADEOFF EVALUATION CRITERIA
- TRADEOFF MATRIX – EVOLUTION OF “HYBRID”
- SUMMARY

INTRODUCTION

The task was to develop requirements to eliminate or manage safety hazard risks associated with human interaction with “shift by wire” (SBW) devices

Evaluation was also to include vehicle behavior and driver feedback based on functional and design criteria that address regulatory, user interaction, and ease of use concerns

This presentation summarizes the safety evaluation process, design constraint development process, and the concept option evaluation and tradeoff effort that lead to a set of requirements

SHIFT BY WIRE DEVICE – "OLD SCHOOL" EXAMPLES

SHIFT BY WIRE DEVICE – "NEW SCHOOL" EXAMPLES

PROJECT OVERVIEW

Identify potentially hazardous conditions that could lead to mishaps (accidents)

Determine the system operating conditions

Identify potential driver interactions that could lead to any potentially hazardous condition [Unsafe Control Actions (UCA)]

Determine possible causes that could result in an UCA

Identify functional and design constraints (and requirements) that would eliminate or minimize the possible causes

Condense these functional and design constraints into requirements that can be used in a tradeoff matrix assessment to evaluate the proposed SBW implementations

PROJECT PLAN

- Identify participants — May
- Determine evaluation process — June
- Develop list of potential hazards and mishaps — June
- Determine possible unsafe driver actions — July
- Identify potential causes for these unsafe actions — July
- Define potential solutions to eliminate or minimize causes — Aug
- Convert potential solutions into high level requirements — Aug

KEY POINTS

Regulatory requirements are contained in:

FMVSS-101 - Controls and displays

FMVSS-102 - Transmission shift position sequence, starter interlock, and transmission braking effect

FMVSS-114 - Theft protection and rollaway prevention

Safety criteria were developed by conducting a detailed safety evaluation using Hazard Operability (HAZOP) techniques from the GM System Safety process augmented by system level causal factors analysis techniques (STPA). This safety criteria development effort focused on three specific areas:

- Eliminating or minimizing accidental/incidental activation
- Providing feedback in clear and understandable ways to maximize driver ability to interact with the SBW system
- Maximizing driver ability to activate device properly when required

Ease of use and user interaction were accommodated by the safety criteria development effort and by customer clinic data conducted on various SBW designs

SAFETY ANALYSIS TECHNIQUES

FTA

Possible causes

Start with the known Effects

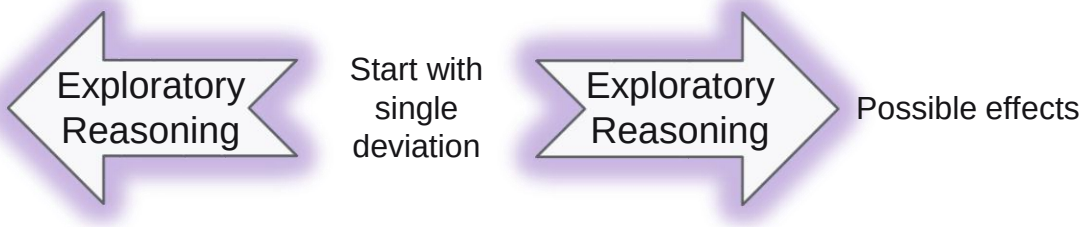
DFMEA

Start with the known causes

Possible effects

System Analysis

Possible causes



Possible effects

STPA ACTIVITIES

Identified potential accidents and potential hazardous conditions that could lead to these accidents and determined the intended system operating conditions (contexts)

ACCIDENTS		
A1	Two or more Vehicles Collide	
A2	Vehicle Collides with Pedestrian(s)	
A3	Vehicle Occupant Injury	
HAZARDS		
H1	Unintended Park Disengagement	A1, A2, A3
H2	Vehicle Roll Away from Not Engaging Park	A1, A2, A3
H3	Unintended Change of Direction	A1, A2
H4	Unintended Propulsion	A1, A2
CONTEXTS		
C1	Vehicle Moving	
C2	Vehicle Stationary on Level Ground	
C3	Vehicle Stationary on Incline	

STPA ACTIVITIES

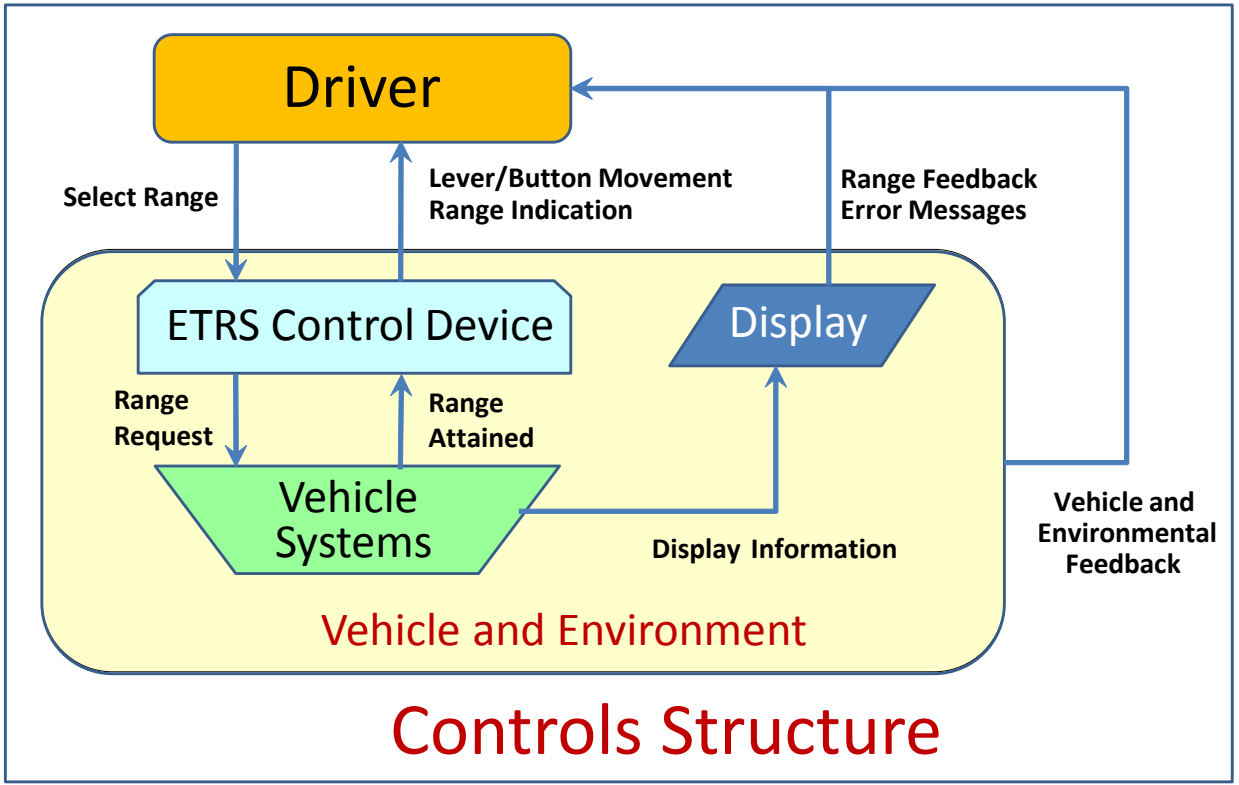
Identified potential driver interactions that could lead to any hazardous condition (Unsafe Controls Actions (UCA))

Driver "responsibilities" within the system were defined:

	Driver Control Responsibilities For Shifting
1	Decide when to shift
2	Select and move appropriate activation device
3	Assess resulting state
4	Acts accordingly

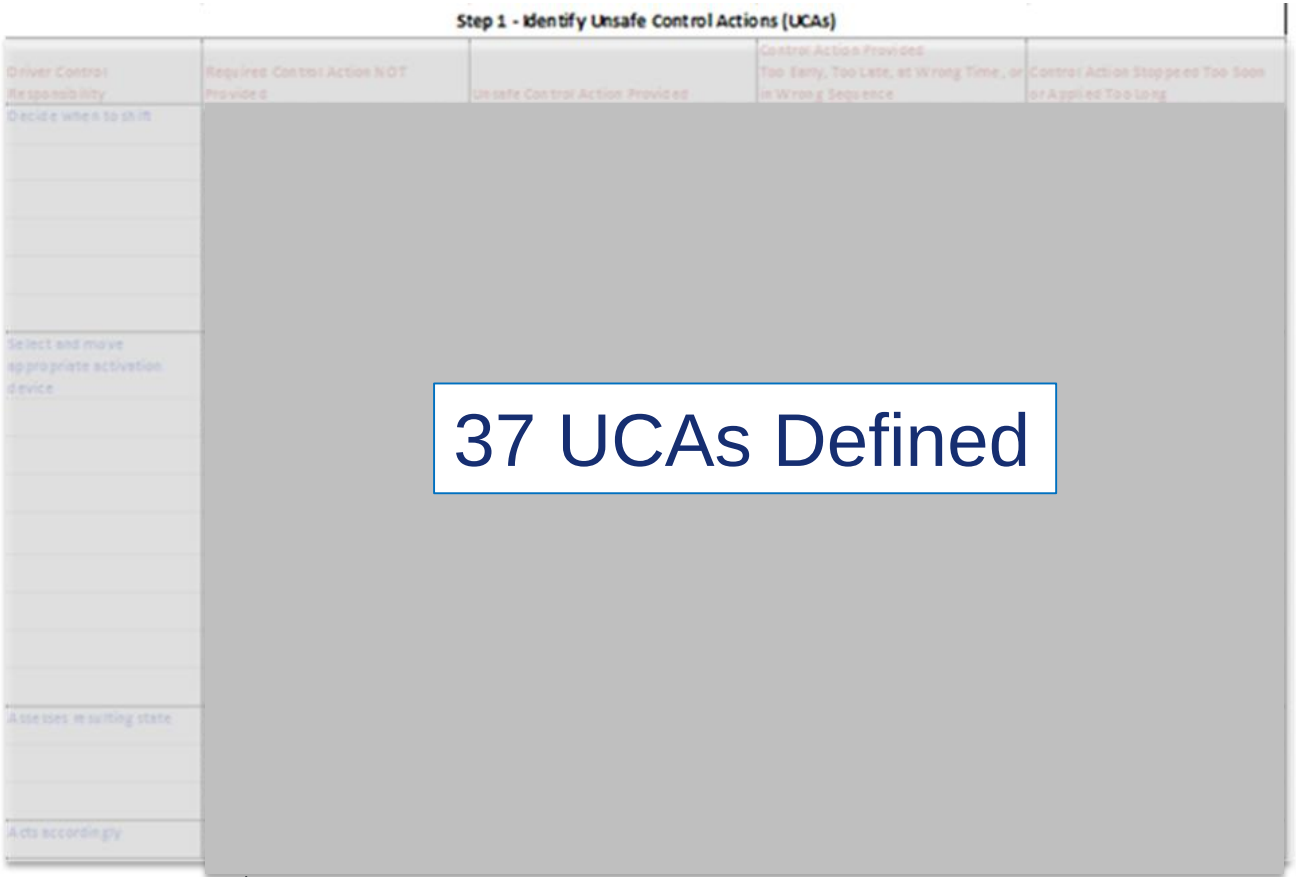
STPA ACTIVITIES

Define system content (control structure) and the interactions between the driver and the system



STPA ACTIVITIES

Define the potential Unsafe Control Actions (UCAs)



STPA ACTIVITIES

Determine possible causes that could result in any UCA

UCA	Potential Causes
UCA1: Driver does not put car in Park on hill	Driver is distracted, or in a panic mode, or is rushing to decide to get into park
UCA1: Driver does not put car in Park on hill	Driver already thinks the car is in Park because of a previous action
UCA1: Driver does not put car in Park on hill	Driver thinks it is already in Park because belief the vehicle will do it automatically
UCA1: Driver does not put car in Park on hill	Driver cannot find Park
UCA1: Driver does not put car in Park on hill	Driver performs prior habitual actions leads to not selecting Park in this vehicle (Prior Learned Behavior)
UCA1: Driver does not put car in Park on hill	System feedback is confusing to driver
UCA1: Driver does not put car in Park on hill	Display(s) not in driver's view

100 Potential Causes Defined

STPA ACTIVITIES

Identify constraints to eliminate or minimize possible causes

Unsafe System Action	Potential Causes	DC#	Design Requirements (Preventive Controls)	Occurances	Priority
UCA0.3: Driver does not put car in park prior to exiting vehicle	Driver is distracted, or in a panic mode, or is rushing to decide to get in to park	1			
UCA13: Driver does not move any button during shift attempt	Driver was not looking at button (just missed)	2.3			
UCA9: Driver selects Reverse at speed	Control bumped unintentionally by driver	1.4			
UCA9: Driver selects Reverse at speed	Control bumped unintentionally by driver	1.9			
UCA9: Driver selects Reverse at speed	Driver reaching for a different control/device (e.g. radio)	2.6			
UCA9: Driver selects Reverse at speed	Control bumped unintentionally by driver	1.6			
UCA9: Driver selects Reverse at speed	Control bumped unintentionally by driver	1.2			
UCA9: Driver selects Reverse at speed	Control bumped unintentionally by driver	1.1			
UCA9: Driver selects R					
UCA9: Driver selects R					
UCA9: Driver selects R					
UCA3: Driver does not select Reverse to go backward	Forward Range control actuates with much lower input than driver expects	9			
UCA2: Driver does not select Drive to go forward	Driver performs prior habitual actions leads to not selecting Reverse in this vehicle (Prior	6			
UCA9: Driver selects Reverse at speed	Driver performs prior habitual actions leads to not selec	5			
UCA0.3: Driver does not put car in park prior to exiting vehicle	System f				
UCA0.3: Driver does not put car in park prior to exiting vehicle	System feedback is confusing to driver	3.9			
UCA0.3: Driver does not put car in park prior to exiting vehicle	Display(s) not in driver's view	3.6			
UCA9: Driver selects Reverse at speed	Driver Experimenting to test System	9.3			

48 Design Constraints Defined

What to Work On First??

Over 750 Combinations (Line Items)

STPA ACTIVITIES

"First Filter"- Use operational contexts to prioritize UCA impact

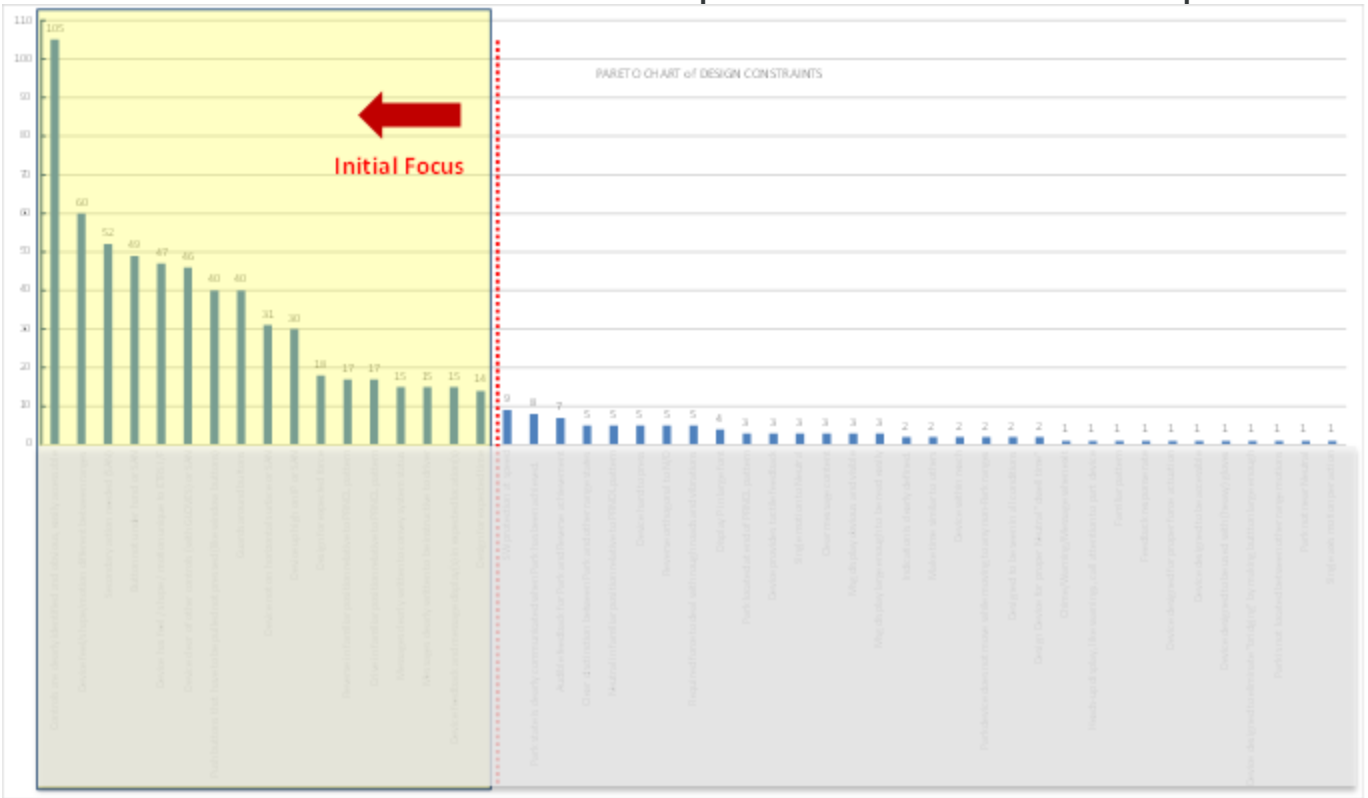
CONTEXTS

- C1 Vehicle Moving
- C2 Vehicle Stationary on Level Ground
- C3 Vehicle Stationary on Incline

UCA	IMMEDIATELY HAZARDOUS OR NOT			
	Vehicle Moving	Vehicle Stationary on Level Ground	Vehicle Stationary on Incline	
UCA0.5: Driver does not put car in park prior to exiting vehicle	YES	YES	YES	1st
UCA0.7: Driver does not put car in park remaining in vehicle	NO	NO	YES	Next
UCA1: Driver does not put car in Park on hill (What about not on a hill?)	NO	NO	YES	Next
UCA2: Driver does not select Drive to go forward	NO	NO	NO	na
UCA3: Driver does not select Reverse to go backward	NO	NO	NO	na
UCA5: Driver puts car in a Non-Park range when intending to go to Park	NO	YES	YES	Next
UCA6: Driver decides to select Drive when Reverse is needed	YES	YES	YES	1st
UCA7: Driver decides to select Reverse when Drive is needed	YES	YES	YES	1st
UCA8: Driver decides to select Reverse or Drive when Neutral is needed	YES	YES	YES	1st

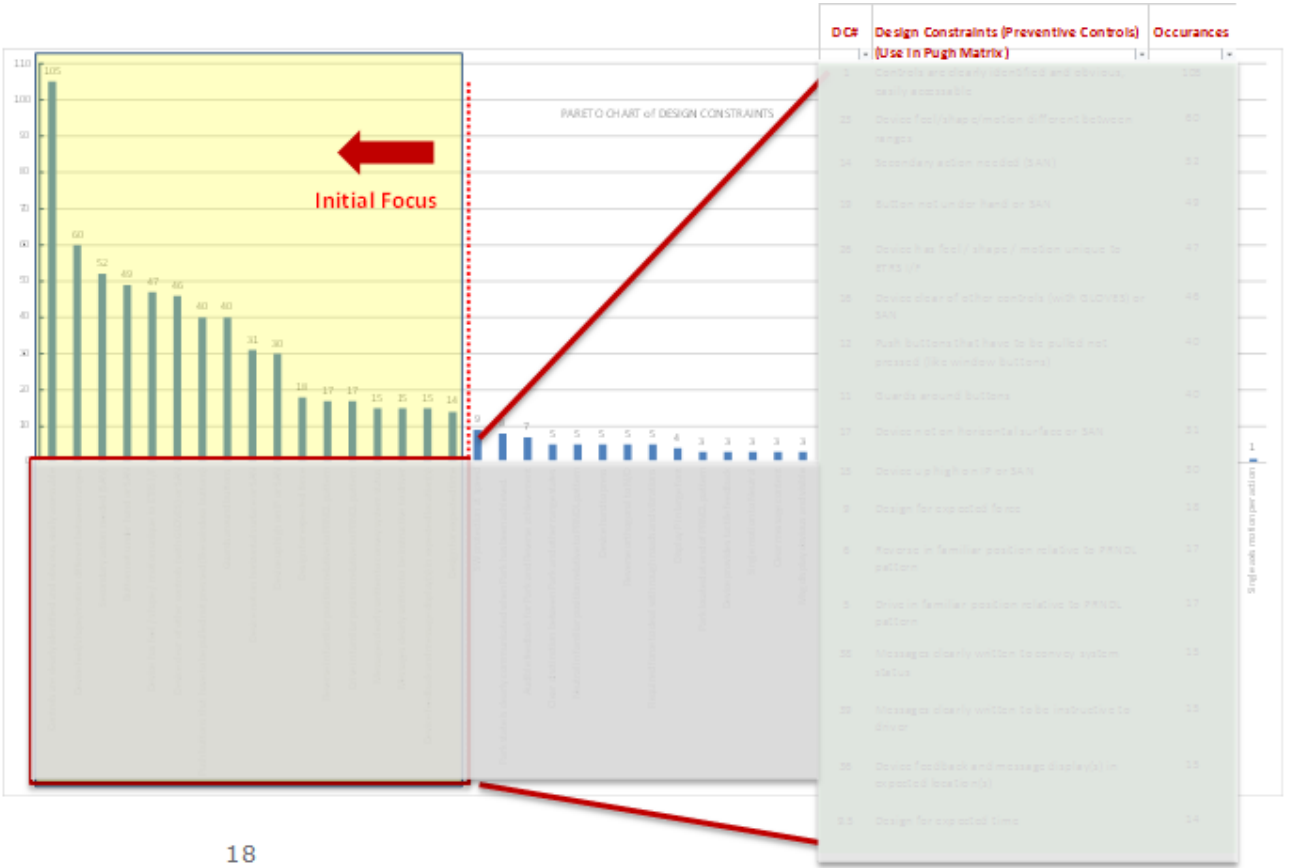
STPA ACTIVITIES

"Second Filter" Use PARETO to prioritize constraint impact



STPA ACTIVITIES

Determine which constraints appear most often for the UCAs



STPA ACTIVITIES

Condense functional and design constraints into requirements to be used in Tradeoff matrix assessment

Meets FMVSS Requirements 101, 102, and 114
Buttons, Knobs, Levers Must Be "Mono-Stable" (momentary activation)
Brake, plus two motions, necessary to exit Park; P => N (Safe)
One motion from D => N (Easy)
Two Motions to get to Reverse from any "Drive" gear (D,L,M)
Controls are clearly identified and obvious, easily accessible
Park button easy to find

TRADEOFF EVALUATION CRITERIA BASED ON HIGH-LEVEL REQUIREMENTS

Tradeoff Evaluation Considered Safe Operation and Customer Usage Criteria

Evaluation Criteria
Meets GM Safety GSSLT Requirements
Meets Regulatory Requirements
Provides Feedback for Errors or Driver Assistance *
Prevents Inadvertent Activation *
Aids New User Operation **
Allows Park Function Activation *
Easy to Use **

* Direct safety impact
** Ancillary safety impact

RESULTING CRITERIA TO USE IN TRADEOFF STUDY FOR CONCEPT EVALUATIONS

Concepts / Requirements and Constraints	Requiement Type	Safety Requirement	Regulatory	Minimizes Inadvertant	Feedback for errors or driver assistance	Allows activation	New User Operation	Easy to Use
Meets FMVSS Requirements 101, 102, and 114	Reg		x					
Buttons, Knobs, Levers Must Be "Mono-Stable" (momentary activation)	Motion	x						
Brake plus two motions necessary to exit Park; P => N (Safe)	Motion	x						
One motion from D => N (Easy)	Motion	x						
Two Motions to get to Reverse from any "Drive" gear (D,L,M)	Motion	x						
Controls are clearly identified and obvious, easily accessable	Funct			x		x	x	x
Park Button easy to find	Funct			x		x	x	x
Park Button display large enough to be read easily.	Funct			x			x	x
Park Button in familiar position relative to PRNDL pattern	Funct			x			x	x

TRADEOFF MATRIX – EVOLUTION OF "HYBRID"

Concepts / Requirements and Constraints	Requiement Type	Current Design	Option 1	Option 2	Option 3	Hybrid Version
		0	1	2	3	
Meets FMVSS Requirements 101, 102, and 114	Reg	DATUM	S	S	S	S
Buttons, Knobs, Levers Must Be "Mono-Stable" (momentary activation)	Motion		S	S	S	S
Brake plus two motions necessary to exit Park; P => N (Safe)	Motion		+	S	S	+
One motion from D => N (Easy)	Motion		S	S	S	+
Two Motions to get to Reverse from any "Drive" gear (D,L,M)	Motion		S	S	S	+
Controls are clearly identified and obvious, easily accessable	Funct		S	S	S	S
Park Button easy to find	Funct		+	-	S	+
Park Button display large enough to be read easily.	Funct		S	-	S	S
Park Button in familiar position relative to PRNDL pattern	Funct		+	-	S	+
		Σ+	9	6	0	13
		Σ–	4	6	0	0
		ΣS	9	10	23	9

SUMMARY

- Thirty seven (37) Unsafe Control Actions Identified
- One Hundred (100) Potential Causes Defined
- Forty Eight (48) Constraints Determined
- Seven Hundred Fifty (750) Unique UCA-Cause-Constraint Combinations Evaluated
- Twenty Five (25) resultant Requirements are Being Used in SBW Designs
- Some Key Safety Related Requirements:
  - Buttons, Knobs, Levers Shall Be "Mono-Stable" (momentary activation)
  - Brake pedal, plus two motions, shall be necessary to exit Park; P => N
  - Only one motion shall be necessary to shift from D => N
  - Two motions shall be necessary to get to Reverse from any "Drive" range (Drive, Low, Manual)