
A comparison of STPA and automotive FMECA

Rodrigo Sotomayor

System Design and Management



Introduction

Motivation

- Increasing pressure to add more and more functionality to automobiles, e.g., Electric Power Steering (EPS), Cruise Control, Lane Keeping Assistance .
- Interactions among systems is dramatically increasing.
- The complexity is becoming intellectually unmanageable with current methods.
- How can we analyze the safety of these complex systems?



Motivation

- As of October 12, 2014 NHTSA database shows open recalls involving Electric Power Steering for the following makers:

Manufacturer	Model
BMW	ACTIVEE
BMW	X3
CHEVROLET	HHR
CHEVROLET	IMPALA
CHEVROLET	COBALT
FORD	F-150
FORD	EXPLORER
FORD	ESCAPE
INFINITI	Q50
LEXUS	LS600HL
MAZDA	MAZDA5
MAZDA	TRIBUTE
NISSAN	ROGUE
PONTIAC	G5
TOYOTA	YARIS
VOLKSWAGEN	PASSAT

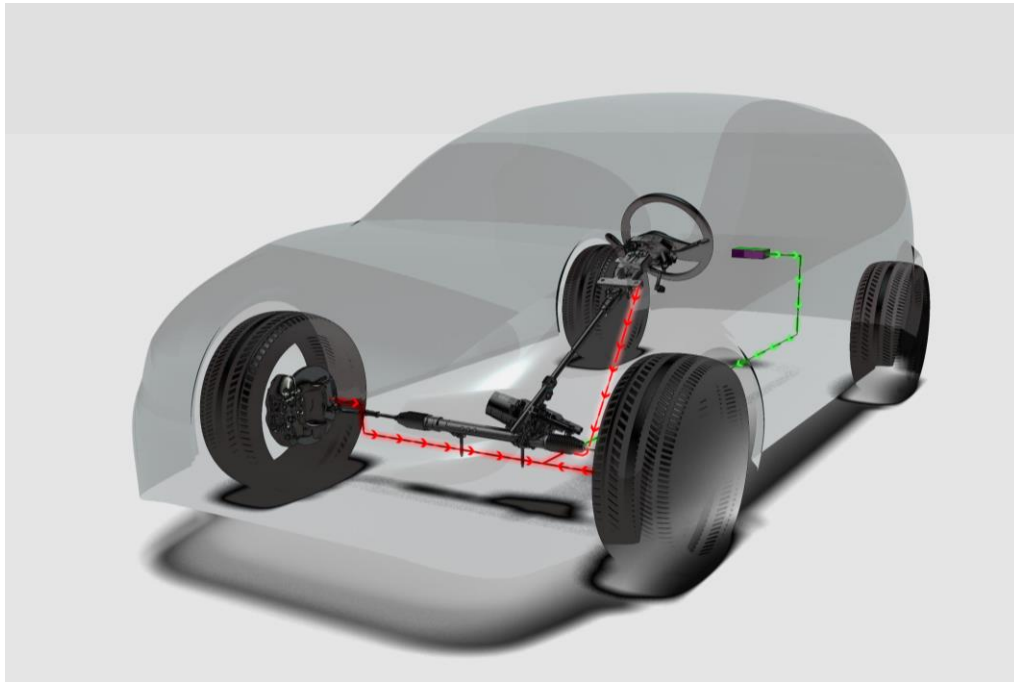
Introduction

Research questions

1. What are the limitations when using FMECA to develop complex automotive systems? Could it be complemented?
2. Can STPA provide more comprehensive results than FMECA, or vice versa?
3. What does it take in terms of resources to develop a robust FMECA compared to STPA?

System Description

Electric Power Steering



System Components and Interaction

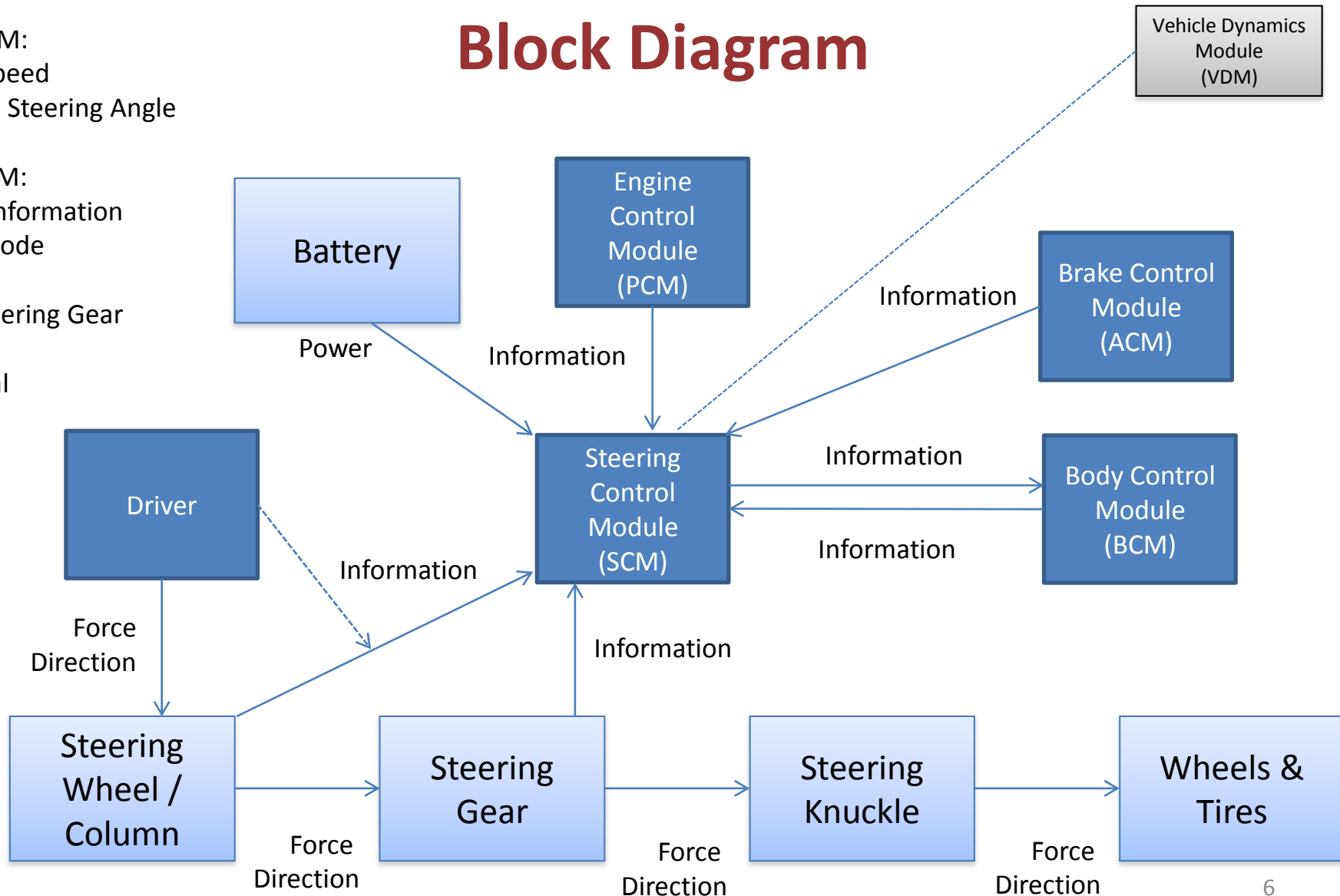
Information
From PCM:
Traction information
Engine Speed

From ACM:
Wheel speed
Absolute Steering Angle

From BCM:
Cluster information
Driver Mode


From Steering Gear:
Torque
SW signal
Angle

Block Diagram



FMECA

- Apply FMECA using current automotive standard in SAE J1739

 SURFACE VEHICLE STANDARD	SAE J1739 JAN2009
	Issued 1994-07 Revised 2009-01
	Superseding J1739 AUG2002
(R) Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA)	

FMECA SAE J1739

DESIGN FAILURE MODES AND EFFECTS ANALYSIS (DFMEA)

System / Subsystem / Component Name: _____
 Model Year / Program(s): _____
 DFMEA Owner (Design Resp.): _____
 Core Team / Facilitator: _____
 Support Team: _____

DFMEA Number: _____
 Revision Date: _____
 Key Date: _____
 Original Completion Date: _____

Item / Function / Requirement	Potential Failure Mode	Potential Effect(s) of Failure	S E V	Classification	Potential Cause(s) of Failure	O C C	Current Design Controls Prevention	Current Design Controls Detection	D E T	R P N	Recommended Action	Responsibility & Target Completion Date	Action Results					
													Actions Taken & Effective Date	S E V	O C C	D E T	R P N	

FMECA - Severity

Category (Product)	Criteria: Severity of Effect (Effect on Product) – DFMEA & PFMEA	Rank	Category (Process)	Criteria: Severity of Effect (Effect on Process) - PFMEA
Safety and/or Regulatory Compliance	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation without warning.	10	Safety and/or Regulatory Compliance	May endanger operator (machine or assembly) without warning.
	Potential failure mode affects safe vehicle operation and/or involves noncompliance with government regulation with warning.	9		May endanger operator (machine or assembly) with warning.
Primary Function	Loss of primary function (vehicle inoperable, does not affect safe vehicle operation)	8	Major Disruption	100% of product may have to be scrapped. Line shutdown or stop ship.
<i>Essential</i>	Degradation of primary function (vehicle operable, but at reduced level of performance)	7	Significant Disruption	A portion of the production run may have to be scrapped. Deviation from primary process; decreased line speed or added manpower.
Secondary Function	Loss of secondary function (vehicle operable, but comfort / convenience functions inoperable)	6	Rework out-of-station	100% of production run may have to be reworked off line and accepted.
<i>Convenient</i>	Degradation of secondary function (vehicle operable, but comfort / convenience functions at reduced level of performance)	5		A portion of the production run may have to be reworked off line and accepted.
Annoyance	Appearance or Audible Noise, vehicle operable, item does not conform. Defect noticed by most customers (> 75%)	4	Rework in-station	100% of production run may have to be reworked in station before it is processed.
	Appearance or Audible Noise, vehicle operable, item does not conform. Defect noticed by many customers (50%)	3		A portion of the production run may have to be reworked in-station before it is processed.
	Appearance or Audible Noise, vehicle operable, item does not conform. Defect noticed by discriminating customers (< 25%)	2	Minor Disruption	Slight inconvenience to process, operation, or operator
No effect	No discernible effect.	1	No effect	No discernible effect

FMECA - Occurrence

Likelihood of Failure	Criteria: Occurrence of Cause – DFMEA (Design life/reliability of item/vehicle)	Rank	Criteria: Occurrence of Cause – PFMEA (Incidents per 1000 items/vehicles)
Very High	New technology/new design with no history.	10	≥ 100 per thousand pieces >= 1 in 10
High	Failure is inevitable with new design, new application, or change in duty cycle/operating conditions.	9	50 per thousand pieces 1 in 20
	Failure is likely with new design, new application, or change in duty cycle/operating conditions.	8	20 per thousand pieces 1 in 50
	Failure is uncertain with new design, new application, or change in duty cycle/operating conditions.	7	10 per thousand pieces 1 in 100
Moderate	Frequent failures associated with similar designs or in design simulation and testing.	6	2 per thousand pieces 1 in 500
	Occasional failures associated with similar designs or in design simulation and testing.	5	.5 per thousand pieces 1 in 2,000
	Isolated failures associated with similar design or in design simulation and testing.	4	.1 per thousand pieces 1 in 10,000
Low	Only isolated failures associated with almost identical design or in design simulation and testing.	3	.01 per thousand pieces 1 in 100,000
	No observed failures associated with almost identical design or in design simulation and testing.	2	≤.001 per thousand pieces 1 in 1,000,000
Very Low	Failure is eliminated through preventative control.	1	Failure is eliminated through preventative control.

FMECA - Detection

Category (Product)	DFMEA Criteria: Likelihood of Detection by Design Control	Rank	Category (Process)	PFMEA Criteria: Likelihood of Detection by Process Control
Absolute Uncertainty	No current design control; Cannot detect or is not analyzed	10	Absolute Uncertainty	No current process control; Cannot detect or is not analyzed
Difficult to Detect	Design analysis/detection controls have a weak detection capability; Virtual Analysis (e.g. CAE, FEA, etc.) is <u>not correlated</u> to expected actual operating conditions.	9	Difficult to Detect	Defect (Failure Mode) and/or Error (Cause) is not easily detected (e.g. Random audits)
Post Design Freeze and Prior to Launch	Product verification/validation after design freeze and prior to launch with <u>pass/fail</u> testing (Sub-system or system testing with acceptance criteria e.g. Ride & handling, shipping evaluation, etc.)	8	Defect Detection Post Processing	Defect (Failure Mode) detection post-processing by operator through visual/tactile/audible means.
	Product verification/validation after design freeze and prior to launch with <u>test to failure</u> testing (Sub-system or system testing until failure occurs, testing of system interactions, etc.)	7	Defect Detection at Source	Defect (Failure Mode) detection in-station by operator through visual/tactile/audible means or post-processing through use of attribute gauging (go/no-go, manual torque check/clicker wrench, etc.)
	Product verification/validation after design freeze and prior to launch with <u>degradation</u> testing (Sub-system or system testing after durability test e.g. Function check)	6	Defect Detection Post Processing	Defect (Failure Mode) detection post-processing by operator through use of variable gauging or in-station by operator through use of attribute gauging (go/no-go, manual torque check/clicker wrench, etc.)
Prior to Design Freeze	Product validation (reliability testing, development or validation tests) prior to design freeze using <u>pass/fail</u> testing (e.g. acceptance criteria for performance, function checks, etc.)	5	Defect Detection at Source	Defect (Failure Mode) or Error (Cause) detection in-station by operator through use of variable gauging or by automated controls in-station that will detect discrepant part and notify operator (light, buzzer, etc.). Gauging performed on setup and first-piece check (for set-up causes only)
	Product validation (reliability testing, development or validation tests) prior to design freeze using <u>test to failure</u> (e.g. until leaks, yields, cracks, etc.)	4	Defect Detection Post Processing	Defect (Failure Mode) detection post-processing by automated controls that will detect discrepant part and lock part to prevent further processing.
	Product validation (reliability testing, development or validation tests) prior to design freeze using <u>degradation</u> testing (e.g. data trends, before/after values, etc.)	3	Defect Detection at Source	Defect (Failure Mode) detection in-station by automated controls that will detect discrepant part and automatically lock part in station to prevent further processing.
Virtual Analysis - Correlated	Design analysis/detection controls have a strong detection capability. Virtual Analysis (e.g. CAE, FEA, etc.) is <u>highly correlated</u> with actual and/or expected operating conditions prior to design freeze.	2	Error Detection and/or Defect Prevention	Error (Cause) detection in-station by automated controls that will detect error and prevent discrepant part from being made
Detection not applicable; Failure Prevention	Failure cause or failure mode can not occur because it is fully prevented through design solutions (e.g. Proven design standard/best practice or common material, etc.)	1	Detection not applicable; Error Prevention	Error (Cause) prevention as a result of fixture design, machine design or part design.

FMECA SAE J1739

- FMECA use in Automotive Industry:
 - Used to document design actions and initial understanding of the design team.
 - Outputs of Design FMECA are used as inputs for PFMECA (SAE J1739)
 - Error proofing for critical and significant design characteristics are cascaded to manufacturing groups and supplier base.
 - Cascade to Control Plan (written descriptions of the system used for controlling parts and processes).
 - Input for target settings in Testing phase.
 - Widely used in industry.
-

EPS FMECA



FMECA- Hardware excerpt

Function	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Class	Potential Cause(s) of Failure	OCC	Prevention Controls	Detection Controls	DET	RPN
(4) Provide assistance to reduce driver's steering efforts to levels that match the functional requirements of the vehicle	(4.1) No assistance - Full loss of power assist	(4.1.1) Increased steering efforts due to complete loss of power assist	8		(4.1.1) Belt assembly does not transmit torque between Electric Motor and rack	5	- Belt assembly FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	6	240
		(4.1.2) Increased brake effort due to complete loss of power assist to the boost system	8		(4.1.2) Electric motor does not provide torque to belt assembly	5	- Electric motor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out - Electrical hardware testing review	6	240
		(4.1.3) Customer dissatisfaction	8		(4.1.3) Torque sensor does not provide torque measurement to Electric motor ECU	5	- Torque sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather	6	240
			8		(4.1.4) Torque sensor cover assembly does not protect outboard housing assembly	5	- Torque sensor cover FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather	6	240
			8		(4.1.5) Power supply harness does not supply required	5	- Power Supply Harness FMEA	- Development test at vehicle level - Durability test at	6	240
			8		(4.1.6) Damage / wear of gear system	5	- Fatigue test at system level	- Development test at vehicle level	6	240

FMECA – Software excerpt

Function	Potential Failure Mode	Potential Effects of Failure	SEV	Class	Potential Cause	OCC	Prevention Controls	Detection Controls	DET	RPN
(2) Provide assistance to reduce driver's steering efforts to levels that match the functional requirements of the vehicle	(2.1) No assistance provided by software - Full loss of power assist	(2.1.1) Increased steering efforts due to complete loss of power assist	8		(2.1.1) Incorrect thresholds values set for assistance curve	3	- Calibration testing at system level - Calibration testing at vehicle level	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	3	72
		(2.1.2) Increased brake effort due to complete loss of power assist to the boost system	8		(2.1.2) Torque sensor does not provide torque measurement to Electric motor SCM	3	- Torque sensor FMEA	- Development test at vehicle level - Durability test at vehicle level - Duty cycle testing - Hot/cold weather prove out	3	72
		(2.1.3) Customer dissatisfaction	8		(2.1.3) Steering Wheel angle sensor does not provide angle change to SCM	3	- Steering Wheel Angle sensor FMEA	- Hot/cold weather prove out	3	72

FMECA summary

- 29 pages long*
- 13 Functions analyzed
- 72 Failure modes
- 95 Causes
- 53 Prevention actions

STPA



STPA - Accidents

- A1: Vehicle occupants are injured during operation
 - A1.1: Two or more vehicles collide
 - A1.2: Vehicle collides with a moving body
 - A1.3: Vehicle collides with a non-moving body
 - A2: Vehicle is damaged (economic loss)
 - A3: Loss of customer preference/ brand loyalty
-

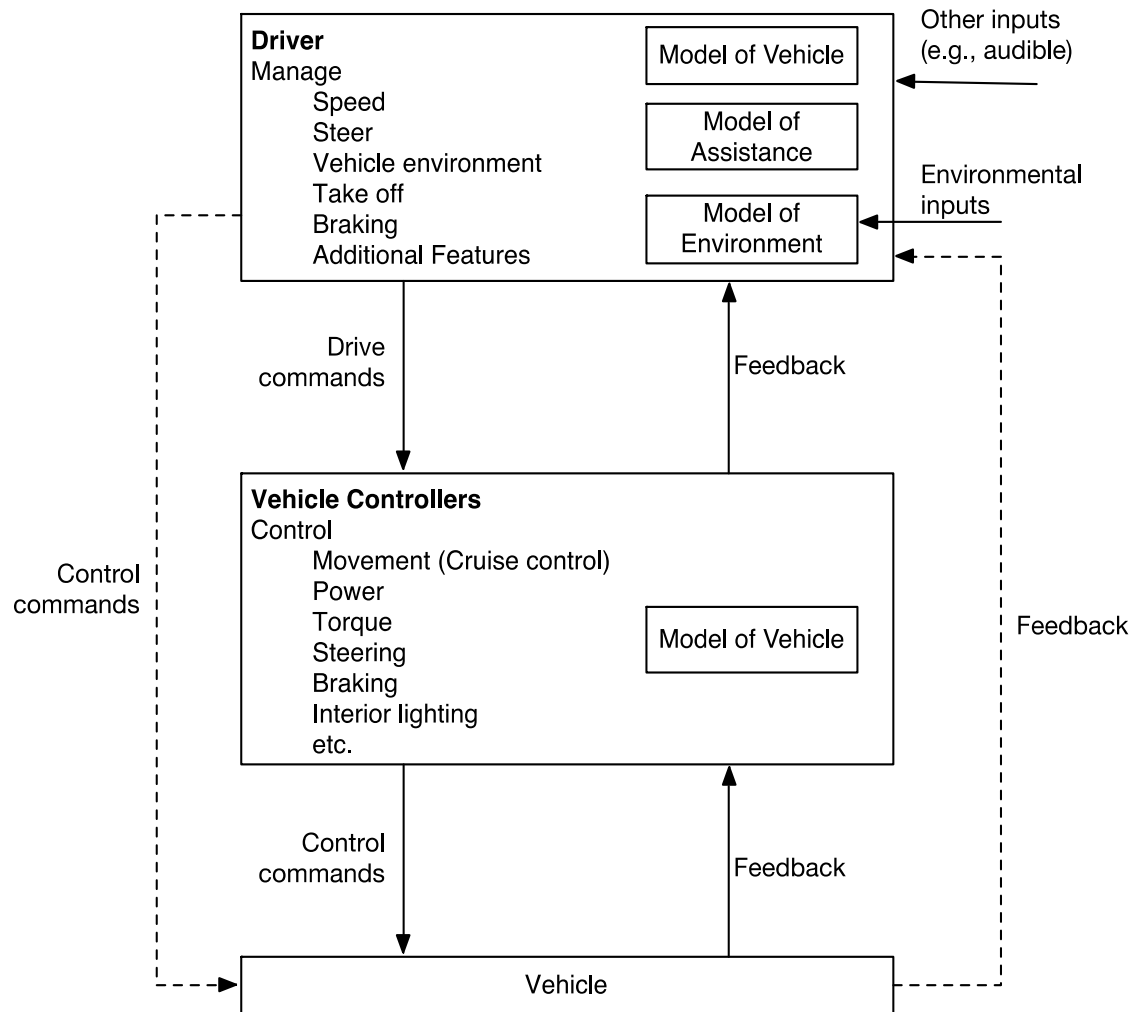
STPA – Hazards and Accident relationship

Hazards

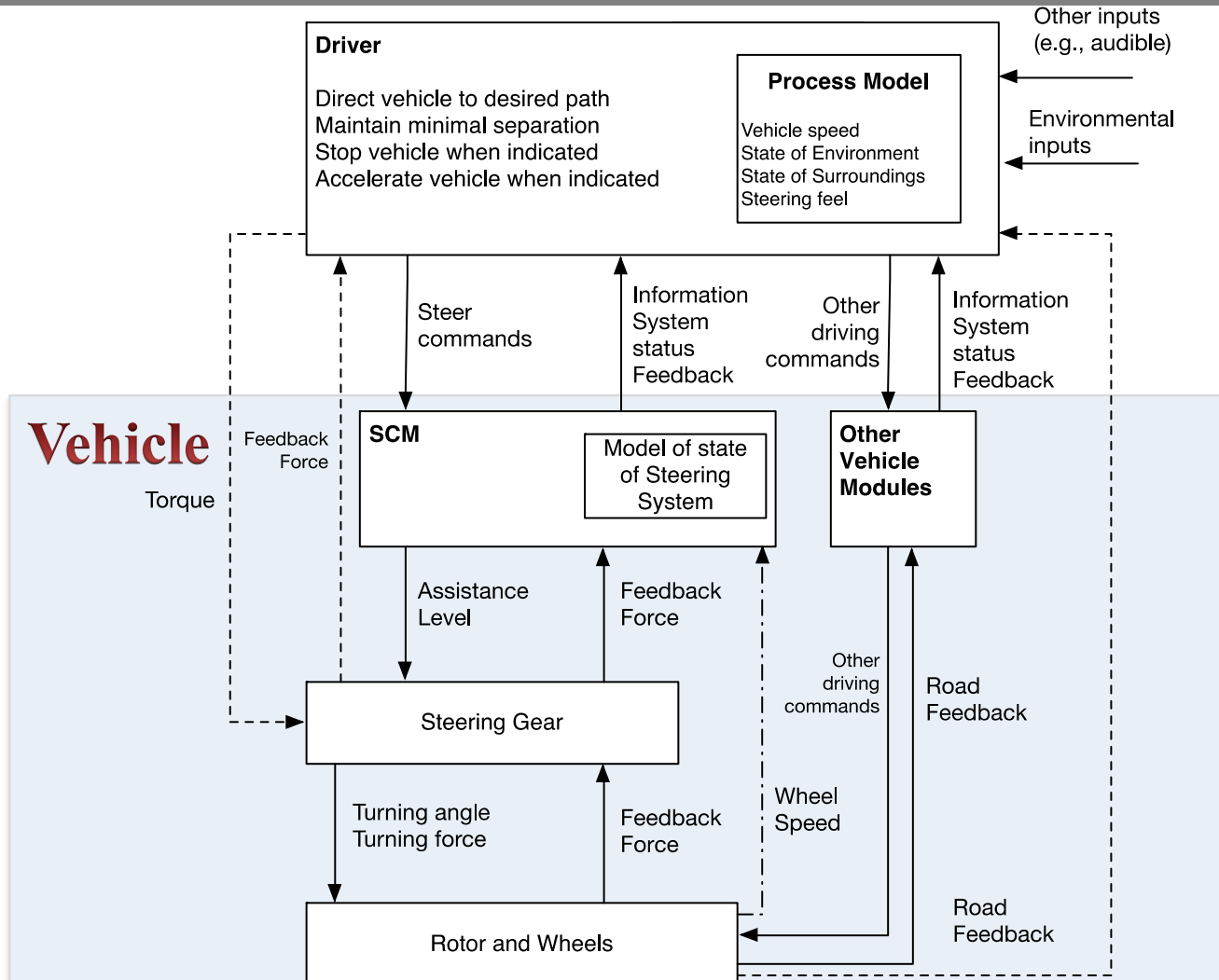
- H1: Vehicle occupants experience harmful conditions during vehicle operation.
- H2: Vehicle does not maintain minimum separation against other moving bodies.
- H3: Vehicle does not maintain minimum separation against static bodies.
- H4: Vehicle is difficult to operate.
- H5: Vehicle equipment operated beyond limits (experience excessive wear and tear)

Hazard	Description	Accident
H1	Vehicle occupants experience harmful conditions during vehicle operation	A1,2,3
H2	Vehicle does not maintain minimum separation against other moving bodies	A1,2,3
H3	Vehicle does not maintain minimum separation against static bodies	A1,2,3
H4	Vehicle is difficult to operate	A1,2,3
H5	Vehicle equipment is operated beyond limits (experience excessive wear and tear)	A2,3

STPA – High-Level Control Structure



STPA – System Control Structure



STEP 1 - SCM

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order	Stopped Too Soon/ Applied Too Long
SCM provides assistance level command to the motor	UCA1: SCM does not provide assistance level command when driver executes a steering maneuver (H-1,2,3,4)	UCA2: SCM provides high assistance level while traveling at high speeds (H-1,2,3,4,5)	UCA3: SCM provides assistance command too late when driver executes a steering maneuver (H-1,2,3,4,5)	UCA4: SCM stops providing assistance command while driver executes a steering maneuver (H-1,2,3,4)
		UCA5: SCM provides low assistance level while traveling at low speeds (H-1,2,3,4)	UCA6: SCM provides assistance command intermittently when driver executes a steering maneuver (H-1,2,3,4,5)	UCA7: SCM continues providing assistance command when safe angle has been reached (H-1,2,3,4,5)
		UCA8: SCM provides too much assistance provided when driver is steering (over assist) (H-1,2,3,4,5)		
		UCA9: SCM provides assistance level in a direction not commanded by the driver (H-1,2,3,4,5)		
		UCA10: SCM provides assistance in a manner that discomforts the driver (H4, 5)		

STEP 1 - Driver

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order	Stopped Too Soon/ Applied Too Long
Driver provides steering commands (force and direction) to steering wheel	UCA11: Driver does not provide steering command when there are people or objects in his/her path (H-1,2,3,4,5)	UCA12: Driver provides steering command towards a static or moving object (H-1,2,3,4)	UCA15: Driver performs a steering maneuver before or after the vehicle follows a safe path (H-1,2,3,4,5)*	UCA13: Driver leaves safe path before steering maneuver is being completed (H-1,2,3,4,5)
		UCA14: Driver provides abrupt steering command while traveling at degraded road conditions(H-1,2,3,4,5)		

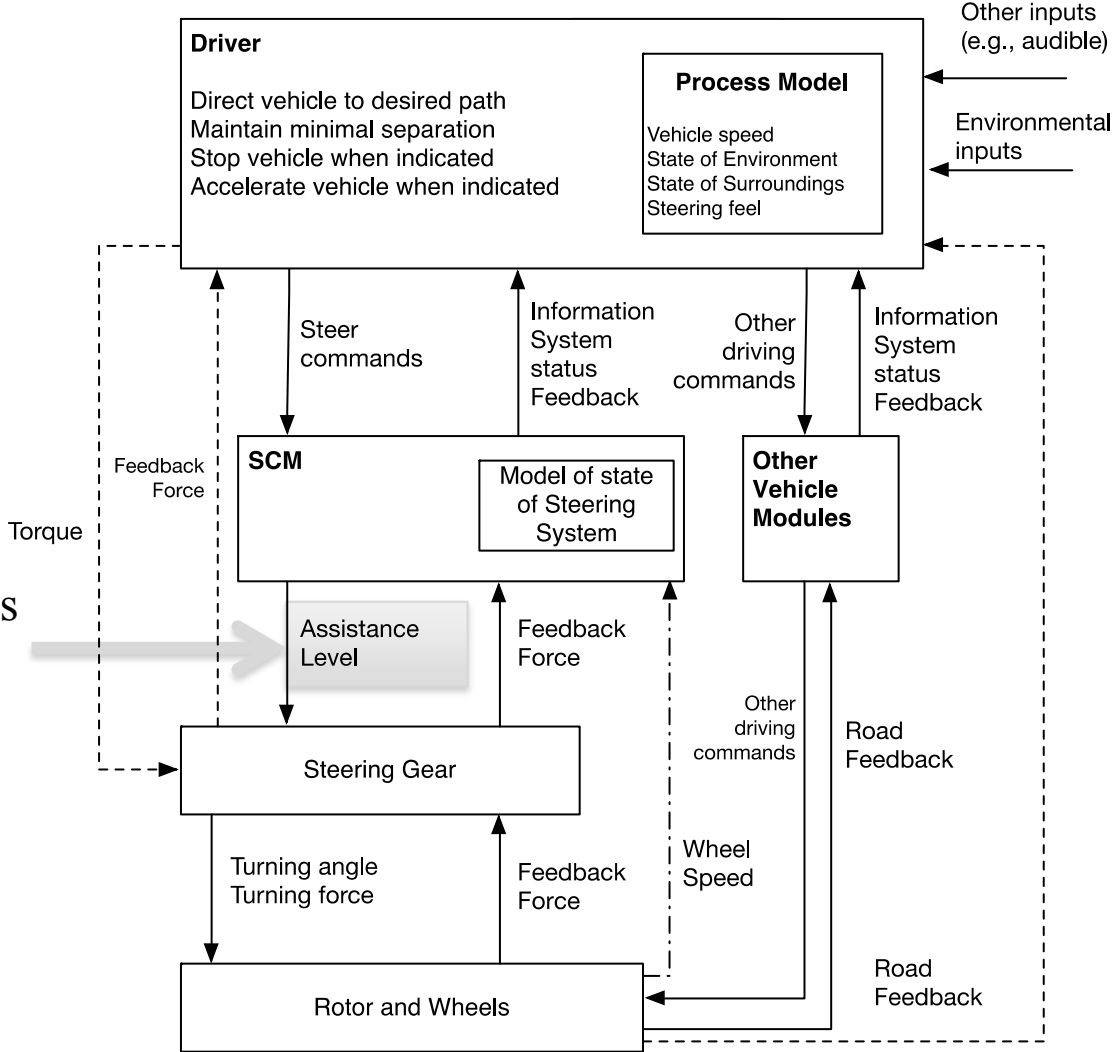


Safety Constraints -SCM

- SC-R1 : Minimum assistance (TBD) Nm shall always be ensured when driver executes a steering maneuver(UCA1)
 - SC-R2: High assistance shall not be provided when vehicle speed is high (UCA2).
 - SC-R3: Assistance shall be provided within TBD ms of steering command is received. (UCA 3)
 - SC-R4: Assistance shall not be interrupted while steering command is being received. (UCA4)
 - SC-R5: Minimum Assistance TBD [Nm] shall be ensured when vehicle speed is below TBD [kph] (UCA1, 5)
 - SC-R6: Assistance shall change accordingly with the range of vehicle speed and efforts defined for the vehicle architecture (UCA6)
 - SC-R7: Assistance shall stop within TBD [ms] after steering command stops being requested by the driver. (UCA7)
 - SC-R8: Assistance shall be provided according to vehicle speed and assistance curves within TBD [ms] of driver initiating a steering command (UCA3)
-



STPA Step 2: Identify causes of UCA



UCA1: Assistance is not provided when driver executes a steering maneuver (H-1,2,3,4)

UCA and Scenarios analysis

UCA1: Assistance is not provided when driver executes a steering maneuver (H-1,2,3,4)

- Scenario1: SCM does not provide assistance because SCM incorrectly believes that assistance is not needed (incorrect process model). SCM does not know assistance is needed because
 - SCM electronic failure (circuit internal failure)
 - Vehicle turning angle feedback is greater than actual turning angle
 - Steering wheel/Torque sensor failure
 - Etc.

Step 2A

Command given but not followed.

- Scenario2: SCM provides assistance command but it is not effective because the current to power the motor is low. The current is too low because:
 - System voltage is too low
 - Electrical system does not account for voltage drain during high assistance situations
 - Etc.
- Scenario3: SCM provides assistance command but it is insufficient to steer the vehicle due to steering lock condition. The system is locked because:
 - High friction in the system due to improper geometry selected
 - Corrosion
 - Steering components installed incorrectly

Step 2B

Examples from Requirements table

- UCA1-S1-R1: Provide additional feedback for determining vehicle speed and steering angle.
- UCA1-S1-R2: System level validation shall ensure that electric sensors, actuators and modules does not irradiate electromagnetic noise that could cause improper behavior of modules, actuators and sensors of the system and the vehicle.
- UCA1-S1-R5: System shall not operate above TBD [C] that would detriment the safe operation of the system. Additional temperature sensor required.
- UCA1-S2-R3: Current requested by the module shall drop within TBD s after rack's end of travel has been reached.

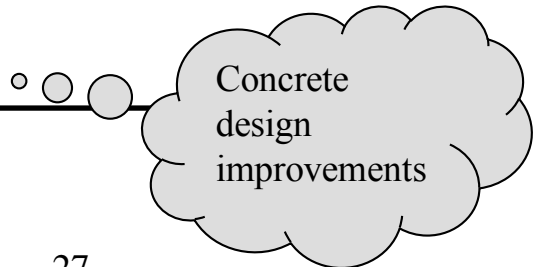
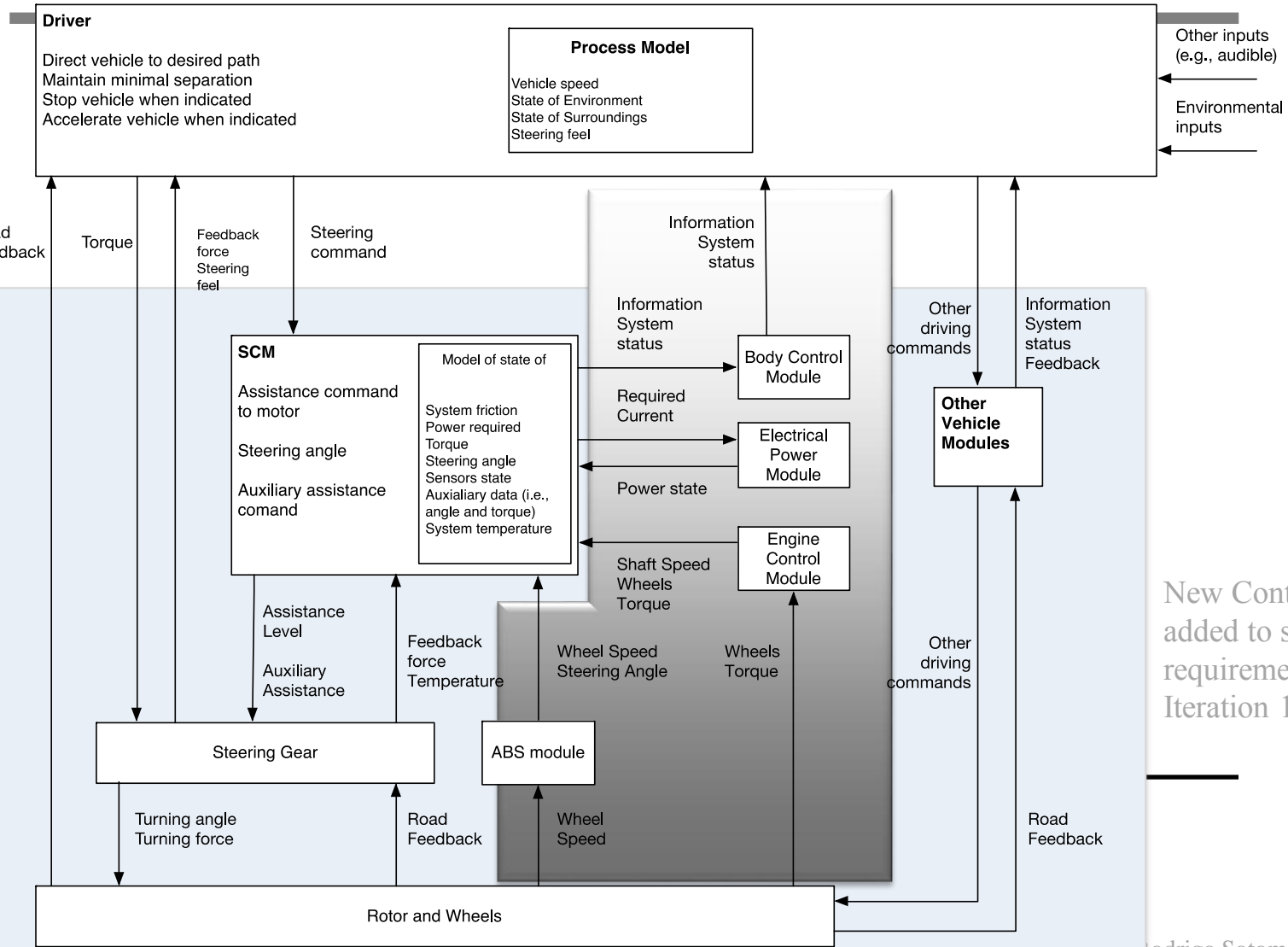


Table of requirements as reference for UCA1

Requirement ID	Description
UCA1-S1-R1	Provide additional feedback for determining vehicle speed and steering angle.
UCA1-S1-R2	System level validation shall ensure that electric sensors, actuators and modules do not irradiate electromagnetic noise that could cause improper behavior of modules, actuators and sensors of the system and the vehicle.
UCA1-S1-R3	System level validation shall ensure that electric sensors, actuators and modules signal to noise ratio remains functional during vehicle operation and through common (environmental) electro-magnetic noises.
UCA1-S1-R4	Algorithm shall include logic to detect if signals from sensors are not being sent with the periodic timing the system requires
UCA1-S1-R5	System shall not operate above TBD [C] that would detriment the safe operation of the system. Additional temperature sensor required.
UCA1-S2-R1	Ensure that enough power is available to provide assistance to the speed of the vehicle. Prioritization shall be enforced to ensure that vehicle control actuators receive the required power to operate the vehicle under safe conditions.
UCA1-S2-R2	Additional feedback might be required to report demanded current by the motor.
UCA1-S2-R3	Current requested by the module shall drop within TBD [s] after rack's end of travel has been reached
UCA1-S2-R4	The system shall not reinitiate while the vehicle is in operation or is below TBD speed [kph].
UCA1-S2-R5	Auxiliary power in vehicle shall be capable to maintain road lights and minimum of TBD [V] to provide assistance in the event of engine stall and vehicle speed is higher than TBD [kph].
UCA1-S3-R1	Torque sensor shall be calibrated to measure TBD [Nm] minimum required torque to steer the vehicle including geometrical characteristics of the vehicle

STPA: Iteration 2 – Control Structure



New Control Actions added to satisfy requirements from Iteration 1

STPA: Iteration 2 – Step 1

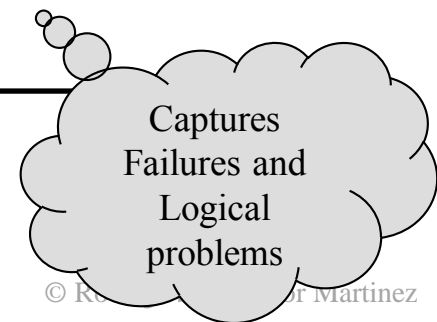
Perform Step 1 for the new control action:

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order	Stopped Too Soon/ Applied Too Long
Command auxiliary assistance mode when fault is detected or high temperature is detected	UCA18: SCM does not command limited assistance when fault is detected or there is a high temperature event (H-4,5)	UCA19: SCM sends auxiliary assistance command when there is no fault or high temperature event (H-4)	UCA20: SCM intermittently commands auxiliary assistance (H-1,2,3,4,5)	UCA21: Stops providing auxiliary assistance command while there is a fault (H-1,2,3,4,5)

STPA: Iteration 2 – Step 2

UCA1: UCA1: Assistance is not provided when driver executes a steering maneuver (H-1,2,3,4)

- Scenario 4: SCM does not provide assistance command because SCM incorrectly believes that it is not safe to provide assistance. SCM believes it is unsafe because:
 - There is no correlation between angle signal and ABS signal
 - Temperature sensor failure
 - Incorrect process model (friction, temperature, torque)
 - Etc



Deriving detailed requirements

- Additional requirements that apply:
- UCA1-S1-R5: The system requires a minimum assistance TBD Nm that is to be to help driver to maneuver the vehicle and bring it to safe state. Such assistance shall be available when algorithm detects that system is in error state, or other modules are sending information that does not match with the model of SCM.
- UCA3-S1-R3: If discrepancy is constant among correlated signals, the algorithm shall include logic to display MIL and laudable chimes to the driver so he can be made aware that the vehicle requires inspection. When discrepancy occurs, the system shall provide minimum TBD [Nm] auxiliary assistance to ensure the driver can take the vehicle for inspection.

STPA and FMECA Comparison Example



Comparison

STPA

FMECA

UCA1: Assistance is not provided when driver executes a steering maneuver(H1, 2, 3, 4)

Failure Mode:
(1.1) EPS does not convert angular displacement/torque to linear displacement/force
(4.1) No assistance - Full loss of power assist

Scenario 1: SCM does not provide assistance because SCM incorrectly believes that assistance is not needed (incorrect process model)



???

Scenario 2: SCM provides assistance command but it is not effective because the current to power the motor is low

Effects:
(4.1.1) Increased steering efforts due to complete loss of power assist

Scenario 3: SCM provides assistance command but it is insufficient to steer the vehicle due to steering lock condition

(1.1.3) Driver input is not enough to turn EPS input shaft
(1.1.1) Unable to control direction of vehicle

Scenario 4: SCM does not provide assistance command because SCM incorrectly believes that it is not safe to provide assistance



???

A3: Loss of customer preference/ brand loyalty

(1.1.2) Customer dissatisfaction

Causes in both STPA and FMECA

STPA	FMECA	
Mechanical failure with electric motor.	(2.1.1) Electric motor does not provide torque to belt assembly	(1.1.1.11) Motor fails to allow rotation of input shaft under driver input
Assembly connections improperly made or don't retain torque/ torqued out of specification or aligned.	(1.1.1.8) Improper connections made at system interface: I-shaft to gear, gear to frame, tie rod to knuckle	(1.1.1.12) Rack and ball nut assembly does not permit axial movement of the rack
Foreign components lodge in steering system.	(1.1.1.5) External objects stuck in the system or contiguous components	
Incorrect geometry selected for the type of suspension of the vehicle.	(1.1.1.1) Incompatibility between gears assembly	
Steering rack travel limiters set incorrectly.	(1.1.1.7) Adjustment travel limiters failure/improper set up	
Corrosion is formed within steering gear components that prevent assistance from motor to move the front knuckle.	(1.1.1.4) Corrosion	
High friction in the system due to improper geometry selected.	(1.1.1.6) Steering gear lock up	
SCM electronic failure (circuit internal failure)	(1.1.1.2) Internal components failure (ICF)	
Sensors degrade over time (incorrect assembly, corrosion)	(2.1.2) Torque sensor does not provide torque measurement to Electric motor ECU	
Faults related to material and geometry for steering components.	(4.1.1) Belt assembly does not transmit torque between Electric Motor and rack	


Causes in both STPA and FMECA

STPA	FMECA
Material and geometry selected does not stand duty cycle designed for the vehicle.	(1.1.1.9) Gear/linkage system not adequately designed to handle wear, impact & fatigue
High friction due to out of alignment components or premature ware.	(1.1.1.9) Gear/linkage system not adequately designed to handle wear, impact & fatigue
Low voltage available due to battery drain or other systems require more power to provide function.	(4.1.5) Power supply harness does not supply required current to Electric motor
Engine stalls while driving (unrelated to EPS) and power is insufficient to command the vehicle.	(4.1.7) Stalled engine
Steering angle/Torque/Wheel speed sensor does not provide signal to the SCM or has measurement error	(2.1.2) Torque sensor does not provide torque measurement to Electric motor ECU
Shorted harness from sensors	(4.4.5) Power supply harness does not supply required current to Electric motor
Premature ware of components due to improper alignment.	Would be captured in other FMECA function

Causes in STPA and FMECA

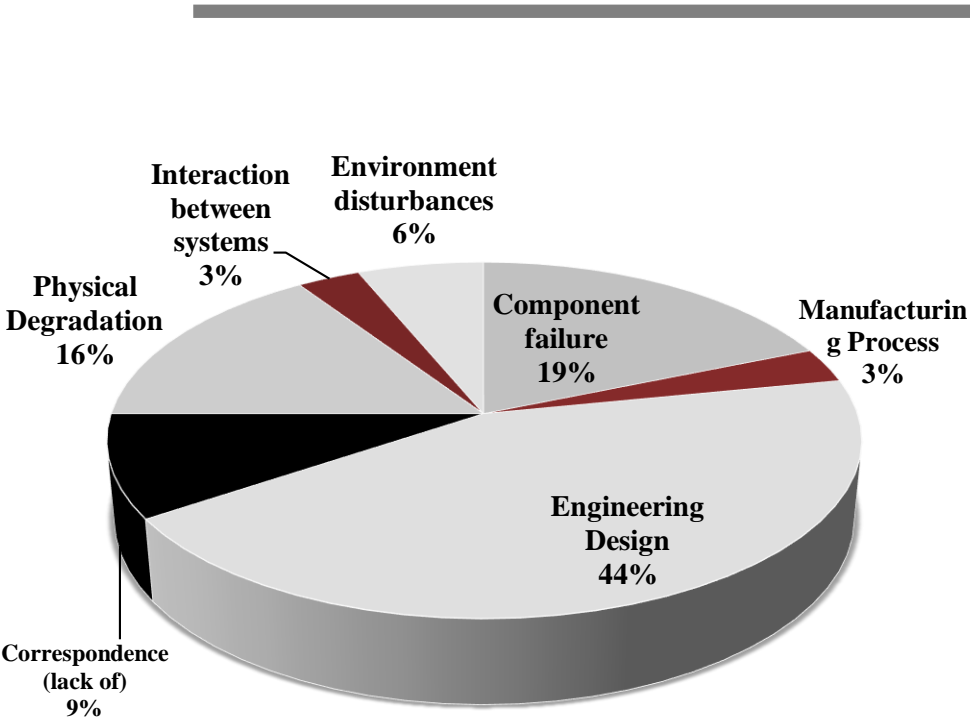
STPA	FMECA
Premature wear of components due to improper alignment.	Would be captured in another FMECA function
Electromagnetic disturbance interferes with signal from wheel speed sensors (high signal to noise ratio)	Would be captured in another FMECA function
Tolerances for friction components out of specification.	Would be captured in another FMECA function
Internal components overheat causing degradation of the system and false readings.	Would be captured in another FMECA function
In Lock-to-lock events the motor keeps providing high assistance once the rack has reached the travel	Would be captured in another FMECA function
Quick acceleration in uneven surface could make the system to acquire different wheel speed sensor information and cause conflict.	Would be captured in another FMECA function
Incorrect calibration for vehicle architecture and geometry.	Would be captured in another FMECA function
Electrical system does not account for high current demand during high assistance situations.	Would be captured in another FMECA function

Causes in STPA for UCA 1/ FM1

STPA	FMECA
The system enters into a reboot or protection mode that impedes normal functionality.	
Algorithm minimum or maximum threshold for torque is incorrect and assistance is not provided	
The method for determining vehicle speed could be incorrect. Relying in one method of measurement (in this case wheel speed) might be hazardous if sensor fails.	
ABS and shaft speed does not match the calculated vehicle speed.	
SCM can't estimate the power required to provide assistance required	
Measurement delays for sensors, or there is a communication error in the BUS	
One of the other modules goes to error state.	
The SCM is not able to combine data from different input and does not detect that steering is needed.	

Types of accident causes

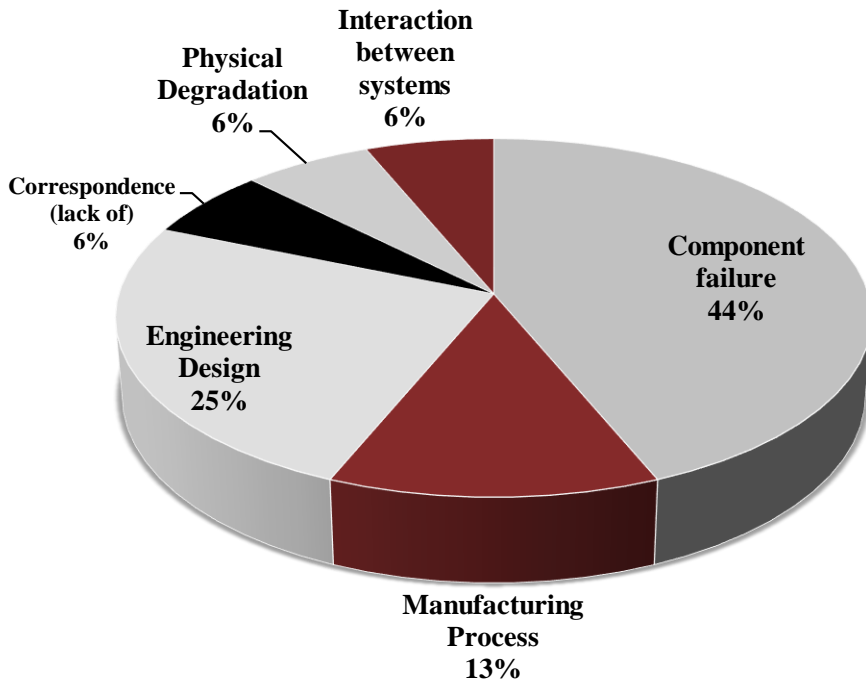
found by STPA



STPA causes for UCA1

Types of accident causes

found by FMECA



FMECA causes for FM1

Types of accident causes found by FMECA

STPA Example	Type of Cause	FMECA Example
Assembly connections improperly made or designed incorrectly	Engineering Design	(1.1.1.1) Incompatibility between gears assembly
Mechanical failure with electric motor	Component failure	(1.1.1.11) Motor fails to allow rotation of input shaft under driver input
Assembly connections improperly made or don't retain torque/ torqued out of specification or aligned	Manufacturing Process	(1.1.1.8) Improper connections made at system interface: I-shaft to gear, gear to frame, tie rod to knuckle
Corrosion is formed within steering gear components that prevent assistance from motor to move the front knuckle.	Correspondence (lack of)	(1.1.1.4) Corrosion
Vehicle speed signal corrupt or missing	Interaction between systems	(2.3.1) Incorrect or no signal provided of vehicle speed

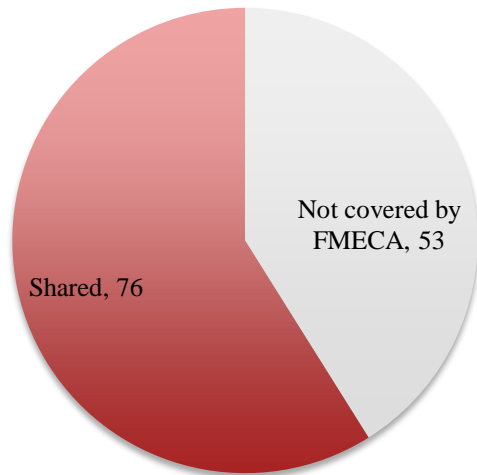
Full comparison



Causes captured by STPA and not by FMECA

Examples of causes not captured by FMECA

STPA Causes



The method for determining vehicle speed could be incorrect. Relying in one method of measurement (in this case wheel speed) might hazardous if sensor fails.

Assistance would not be provided because there is a conflict between steering angle and speed signals.

There is no prioritization for critical operation components if there is low voltage available.

Delayed signal information provided by sensor, or there is a communication error in the BUS

Another controller limits speed when auxiliary assistance is provided (Cruise control).

High friction event is detected at low speed.

Chime is not loud enough or displayed in a way it is easily noticeable by the driver.

137 vs. 95 total causes found (but there are overlaps)

STPA vs FMECA

STPA	FMECA
↓ Analyzes 22 UCA's	↓ Analyzes 13 System Functions
↓ 49 Scenarios	↓ 72 Failure modes
↓ 137 Causes	↓ 95 Causes
47 high-level requirements and 10 System Safety Constraints	53 Prevention Actions

Philosophical Comparison

- FMECA
 - Forward search base on underlying chain of events.
 - Emphasizes standard ranking criteria's and focuses on mitigation of previously known potential failure modes.
 - Assumes successful functioning based on reliability methods.



Philosophical Comparison

- STPA
 - Top-down approach using System Theory to prevent Accidents.
 - Avoids system hazards by deriving high-level requirements aimed to mitigate both individual and related hazard causes.
 - Include system controllers and interaction as well as human controllers (operators) and mental process.
 - Consequently, Safety is an emergence property of the system.



Q & A



Massachusetts Institute of Technology