Software Requirements Document
Active Safety Features

Team 10

[redacted]

Table of Contents

Table of Figures

Table of Table

1 Introduction

1.1 Purpose

The purpose of this document is to outline the functionality, interfaces, attributes and constraints of four active-safety features for automobiles. These features include blind spot detection (BSD), parking assist (PA), tire pressure monitoring (TPM) and pre/post collision protection (PCP). The models presented in section 3 of this document demonstrate how each system will typically be used, what other systems it interacts with, and the basic behaviour of the system. This information can be used to design a solution that fits the project's requirements.

The intended audience for this document is the stakeholders of the project. This includes but is not limited to the client, developers and regulatory bodies. This specification documents the client requirements of the four active-safety features under design. The clients can use this document to verify the systems under design meet the specified requirements. The developers and designers should use this document to ensure all specified functionality is correct and present in the system. This specification further specifies the systems these features are expected to interface with. Regulatory bodies can use this document to verify compliance with relevant rules and regulations.

The reader of this document is assumed to have basic knowledge of cars and how to operate cars. Knowledge of UML diagrams is also required.

1.2 Scope

The active-safety system proactively monitors a vehicle's environment and takes action to avoid collisions or mitigate damage if a collision is unavoidable. This system is made up of four subsystems, which include blind spot detection, parking assist, tire pressure monitoring, and pre/post collision protection. These features use software controllers that monitor sensor data, process the sensed data, detect hazards or errors, operate actuators, communicate with other systems and/or log events.

Blind spot detection uses sensors in the car's rear corners to determine if there is an object in the car's blind spot. If an object is detected then the user is alerted visually. If the user signals a lane change, and there is an object in their blind spot then they will be alerted audibly.

Parking assist uses sensors on the car's front and rear bumpers to alert the driver of near-by objects at low speeds. The system visually and audibly alerts the user of the proximity of objects.

Tire pressure monitoring notifies the user if one or more of their tires has a pressure that varies too greatly from a user desired value. The pressure of each tire in monitored by sensors that are part of the wheels.

Pre/post collision protection integrates with several systems including seatbelts, hazard lights, steering, windows, and emergency communication. The system collects data from several sensors to determine that a collision is imminent and activates other systems to reduce the damage of the impending collision. Following the collision, systems are activated to ensure the safety of the passengers and facilitate rescue operations. This system is not intended to detect all types of collisions.

These active-safety features are intended to provide environmental information to the driver so they are able to make better decisions to reduce the likelihood of an accident. These features are not intended to control the operation of the vehicle unless an accident is unavoidable. These features operate within the the vehicle's system and interact with its available subsystems.

1.3 Abbreviations, Acronyms, Definitions, Notational Conventions

PA - Parking assist

BSD - Blind spot detection

TPM - Tire pressure monitoring

PCP - Pre/post collision protection

Collision Warning System – refers to the optional system which can help predict imminent collisions

Brake Assist – refers to optional system which can help with engaging the brake pedal in certain imminent collision situations

1.4 References

The content of the document was developed based on the original product description available in Appendix A. The requirements for the active-safety system were elicited through four customer question sessions. The minutes from these sessions are available in Appendix B. The technical content in this specification was developed with help from the University of Waterloo's ECE 451/CS 445 lecture notes.

1.5 Document Overview

This section introduces the active-safety system and its four distinct subsystems.

Section 2 of this document contains a general description of the four active safety features including each system's boundaries, constraints and interfaces. Also outlined in this section are the general use cases as well as assumptions about the user and environment.

Section 3 identifies the specific requirements, including external interfaces, states the system will be in and transitions between those states, functional requirements, and behavioural requirements.

The document concludes with two appendices, which contain the original product description and the minutes from customer sessions, and do not constitute additional requirements of the software; all requirements arising from these minutes have been incorporated into the specific requirements in Section 3.

2 Overall Description

2.1 Product Perspective

The active-safety features operate within the boundary of the car and interact with the various subsystems available in the car.

2.1.1 Communication Interface

Each of the four active-safety features communicates with the required sensors and actuators via the car's main control system. The car's main control system is responsible for ensuring that requested data is served and requested setting are applied.

2.1.2 Software Interface

The software for each system will be written in a manner, which is consistent with the software, which controls the car's other subsystems because the software of each feature must interface with many of these other subsystems. These subsystems include the large display dashboard, the collision warning system and the emergency communication system.

2.1.3 Hardware Interfaces

All four of the active-safety features rely on several sensors and actuators.

The BSD system relies on proximity sensors on the corners of the rear bumpers to detect objects in the blind spot. The system alerts the user of blind spot objects with lights on the side mirrors and through the sound system with audible alerts. This system also has a button to enable and disable the system.

Parking assist relies on several proximity sensors on the front and rear bumpers. This system communicates the proximity of objects to users audibly through the car's sound system, which allows sounds of varying frequencies. The system communicates the object proximity visually to the user through either a series of dash lights (red, yellow, green) or through use of a large interactive dashboard display. This system also has a button to enable and disable the system.

The TPM system relies on sensors that are part of the wheels to communicate changes in tire pressure. The tire pressure information is displayed to the user through a series of coloured dash lights (red, green) or through a large interactive dashboard display.

PCP relies on a variety of sensors including the steering wheel sensor, brake pedal sensor, pressure impact sensors and may include a high speed radio sensor. PCP will activate the collision warning system and brake assist if these systems are available.

All systems have a dashboard light, which will illuminate in the case that the system has malfunctioned.

2.1.4 User Interfaces

The most important feature of the user interface for all four features is that they do not distract the driver unless absolutely necessary. The placement and style of the visual displays is important because the driver needs to be able to understand the message being communicated without taking their eyes off the road for too long. The audio alerts should convey the appropriate intensity without startling the driver. The driver can enable and disable this feature by pressing a button.

The notification light for the blind spot detection system is located on the side mirror, and only has two states: on and off. This way the user is only notified when they need the information and the notification is intuitive to understand. A sound is played and the steering wheel vibrates when the user signals a movement in the direction of an object. This increased alert level should attract the user's attention. The driver can enable and disable this feature by pressing a button.

Both the audio and visual alerts in the parking assist system are more prominent because it is assumed that the user is traveling at a slower speed so taking more of their attention does not risk their safety. The audio and visual alerts increase in intensity as the driver nears an object while in a parking situation. This allows the driver to park closer to objects without hitting them.

The visual alert for the tire pressure monitoring system is discreetly placed on the dash so it does not distract the driver. It can be one of three colours: green, red or grey. These colours intuitively tell the user the status of the system at a glance. For cars with advanced displays more information can be requested such as showing the exact pressure of each tire.

The pre/post collision protection system has fewer notifications because in the event of an imminent crash the user should be focused on minimizing damage, and distracting them with lights and sounds could cause more problems.

2.1.5 Use Case Diagrams

The following four figures are the use case diagrams for the four active safety features.

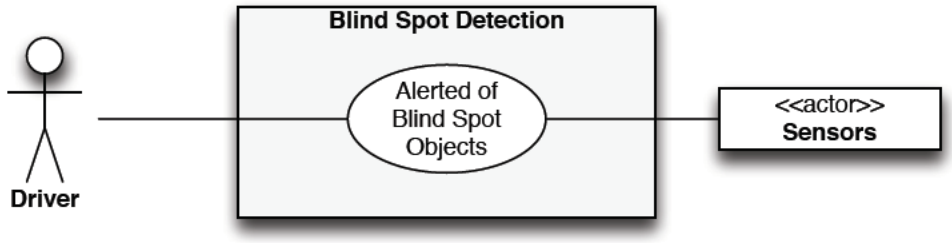

Figure 1 Use case diagram for the blind spot detection system

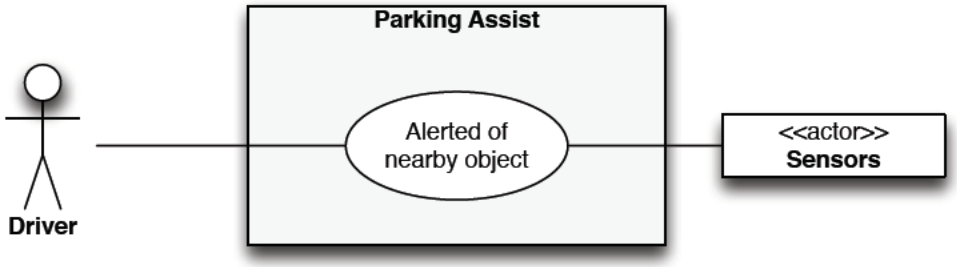

Figure 2 Use case diagram for the parking assist system

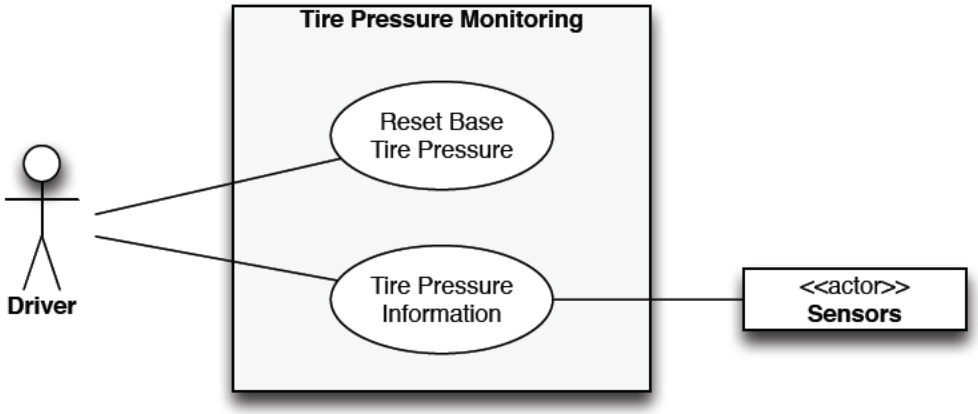

Figure 3 Use case diagram for the tire pressure monitoring system

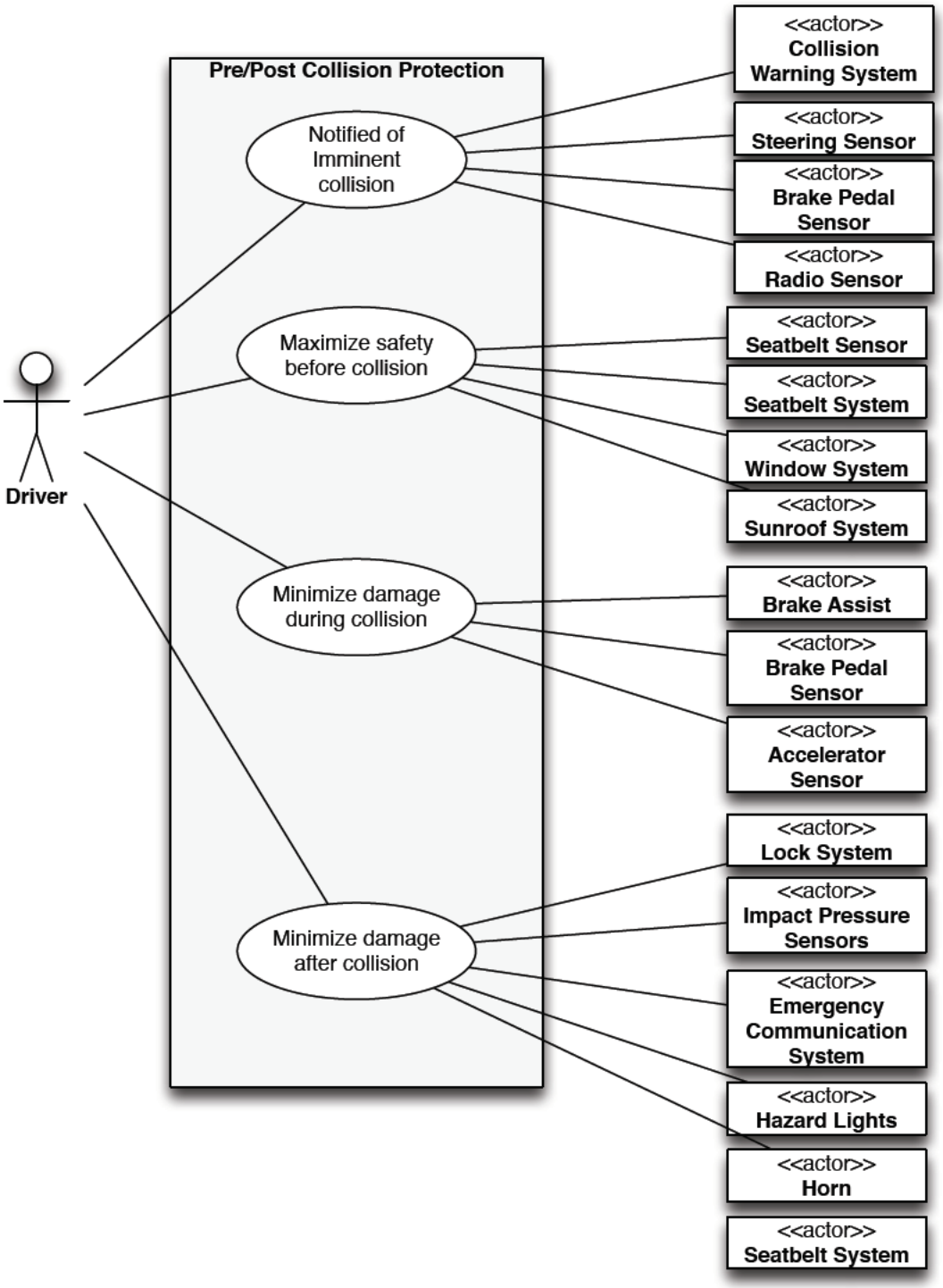

Figure 4 Use case diagram for the pre/post collision protection system

2.2 Product Functions

Blind Spot Detection (BSD)

Alerted of Blind Spot

When the BSD system is enabled the driver is notified when there is an object in their blind spot(s) by illuminating the corresponding side mirror light. If there is an object detected in their blind spot and the driver enables the turn signal for that same side then the system will issue an audible alert. The user can disable or re-enable the feature.

Parking Assist (PA)

Alerted of nearby objects

User is alerted of objects in front or behind the car that are in rage of the parking assist sensors. User is alerted by use of display and sounds with increasing intensity as the car continues to get closer to the object(s). The user can disable or re-enable the feature.

Tire Pressure Monitoring (TPM)

Reset Base Tire Pressure

After user changes tire pressure, user presses a button to reset baseline tire pressure. Baseline tire pressure is used for detecting bad tire pressure.

Tire Pressure Information

User will be notified of a tire pressure change of +/- 25% of the base pressure by an illuminated dash light.

Pre/Post Collision Protection (PCP)

Notified of imminent collision

Driver is notified of imminent collision.

Maximize safety before collision

System tightens seat belts, brake assist is engaged if driver initiates braking, open windows are mostly closed leaving a slight opening, if sunroof is present and open it is closed.

Minimize damage during collision

Brake assist continues even if driver disengages brakes during collision.

Minimize damage after collision

Hazard lights are switched on, doors are unlocked and horn is sounded. If available, emergency services are contacted with vehicle position.

2.3 User Characteristics

The user is expected to be a fully licensed driver and obey all rules and regulations for operating a car in their current environment. In addition to this they are expected to have read the user manual, which outlines the purpose and operation of these four features.

2.4 General Constraints

All of these active-safety features must obey all laws, standards and regulations. These vary from country to country so the local laws, standards and regulations should be reviewed before designing a solution.

2.5 Assumptions and Dependencies

These systems assume that all cars and driver will be following the rules of the road and driving in a safe manner. It is also assumed that the sensors know when they are malfunctioning by knowing validity ranges for data and don't produce erroneous data. It is assumed that all other malfunctions will be known absolutely to the system.

It is assumed that the operating environmental conditions such as weather would not interfere with the system and sensor operation. It is assumed the systems will function at any temperature. It is expected that all sensors will function for the lifetime of the car.

These four features depend largely on the proper operation and function of the vehicle. It is assumed that external systems to these features would not fail or would handle their failure to manage their interface with other subsystems.

For sensors in the blind spot detection system it is expected that it will only detect large car-like objects.

For the tire pressure monitoring system it is expected that the accuracy of the readings be within 1% of the actual tire pressure.

For the parking assist feature the accuracy of the sensors is expected to be within 2 to 4 inches.

3 Specific Requirements

3.1 External Interfaces

The domain model for the blind spot detection system can be seen in Figure 5. It outlines all of the actors, interfaces and domain elements of the system as well as the relationships between each element. The relevant attributes of each element are also shown.

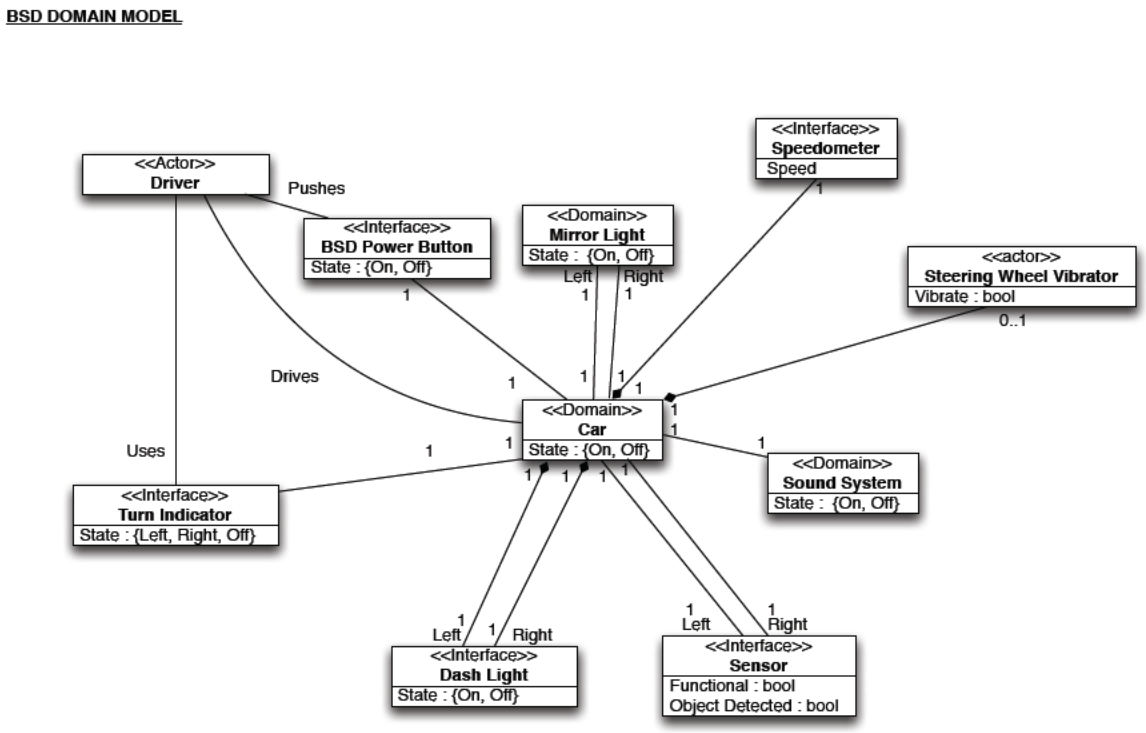

Figure 5 Domain model for the blind spot detection system

The following describes the input and output events for the BSD system.

Input Events

- object(s) - Object is sensed by blind spot sensor on side s, car.s.sensor.objected detected = true
- signal(s) - Driver turns on indicator to signal to side s, car.turn indicator.state = s (s = {right, left})
- signalOff - Driver turns off indicator, car.turn indicator.state = off
- power - driver presses BSD power button, driver.presses.car.BSD power button

Output Events

- soundOn - System plays sound, car.sound system = on

- soundOff - System ends sound, car.sound system = off
- vibrateOn - System vibrates steering wheel, car.steering wheel vibrate.vibrator = true
- vibrateOff - System ends vibration, car.steering wheel vibrate.vibrator = false
- lightOn(s) - System turns on mirror light on side s, car.s.mirror light.state = on
- lightOff(s) - System turns off mirror light on side s, car.s.mirror light.state = off

The domain model for the parking assist system can be seen in Figure 6. It outlines all of the actors, interfaces and domain elements of the system as well as the relationships between each element. The relevant attributes of each element are also shown.

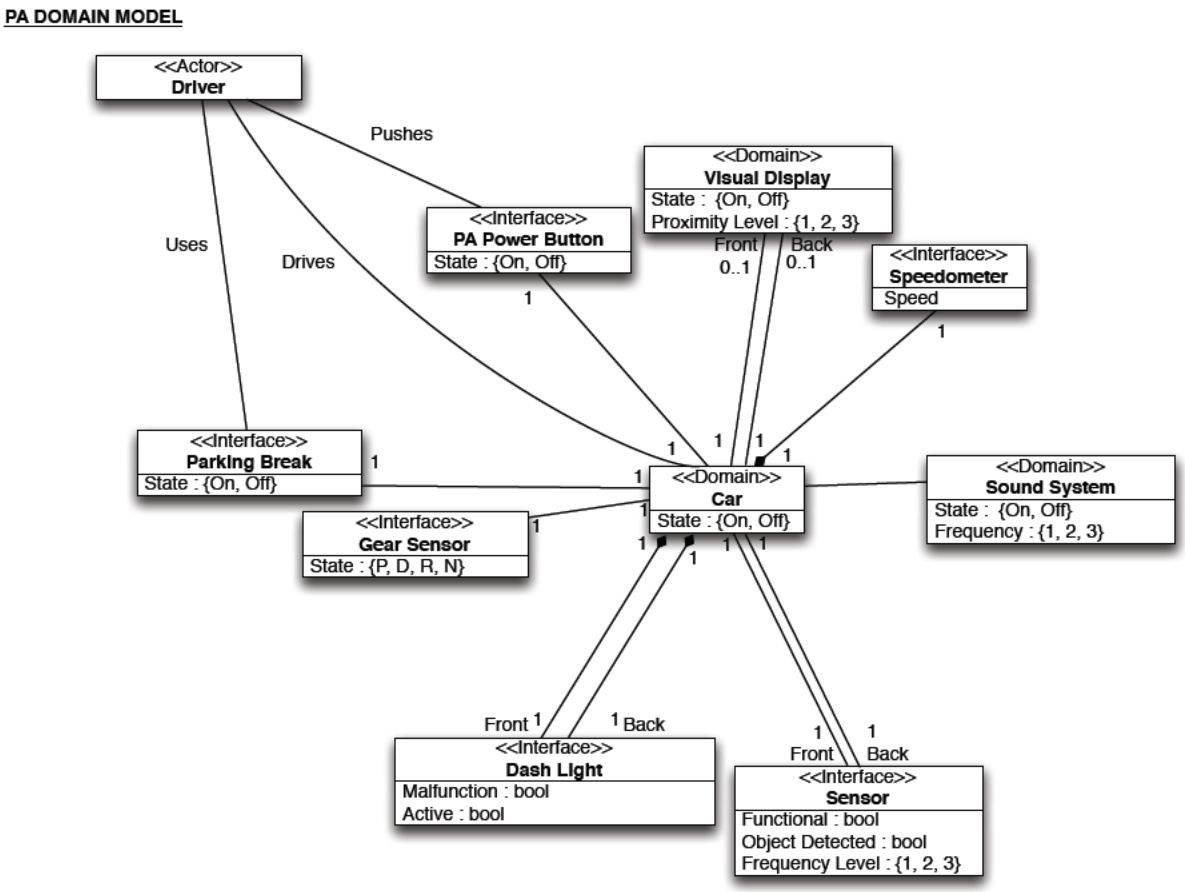

Figure 6 Domain model for the parking assist system

The following describes the input and output events for the PA system.

Input Events

- object(s) - Object is sensed by sensor on side s, car.s.sensor.objected detected = true

- power - driver presses PA power button, driver.presses.car.PA power button = true

Output Events

- displayOn(s) - visualDisplay for PA is turned on for side s, car.s.visual display.state = on
- displayOff(s) - visualDisplay for PA is turned off for side s, car.s.visual display.state = off
- soundOn - Sound system turns on, car.sound system = on
- soundOff - Sound system turns off, car.sound system = off

The domain model for the tire pressure monitoring system can be seen in Figure 7. It outlines all of the actors, interfaces and domain elements of the system as well as the relationships between each element. The relevant attributes of each element are also shown.

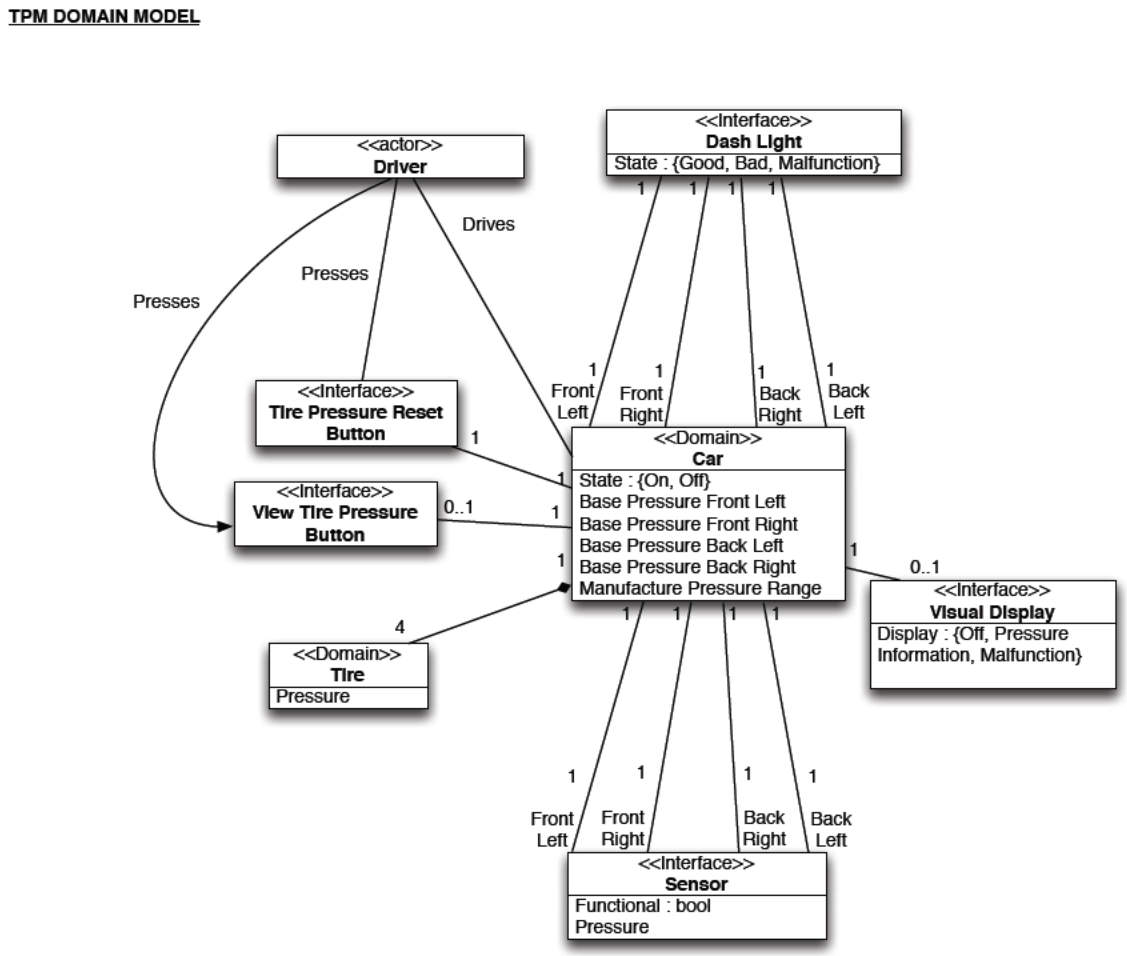

Figure 7 Domain model for the tire pressure monitoring system

The following describes the input and output events for the TPM system.

Input Events

- highExceeded(t) - pressure is above threshold for tire t, car.t.sensor.pressure <= 0.75*car.base pressure t
- lowExceeded(t) - pressure is below threshold for tire t, car.t.sensor.pressure >= 1.25*c.base pressure t
- reset - driver presses tire pressure reset button, driver.presses.car.tire pressure reset button

Output Events

- bad(t) - illuminates "pressure out of range" (red) light for tire t, car.t.dash light.state = bad
- malfunction(t) - illuminates "malfunctioning sensor" (grey) light for tire t, car.t.dash light.state = malfunction
- good(t) - illuminates "pressure within range" (green) light for tire t, car.t.dash light.state = good
- display tire info - displays tire pressure on fancy display, car.visual display.display = tire pressure

The domain model for the pre/post collision protection system can be seen in Figure 8. It outlines all of the actors, interfaces and domain elements of the system as well as the relationships between each element. The relevant attributes of each element are also shown.

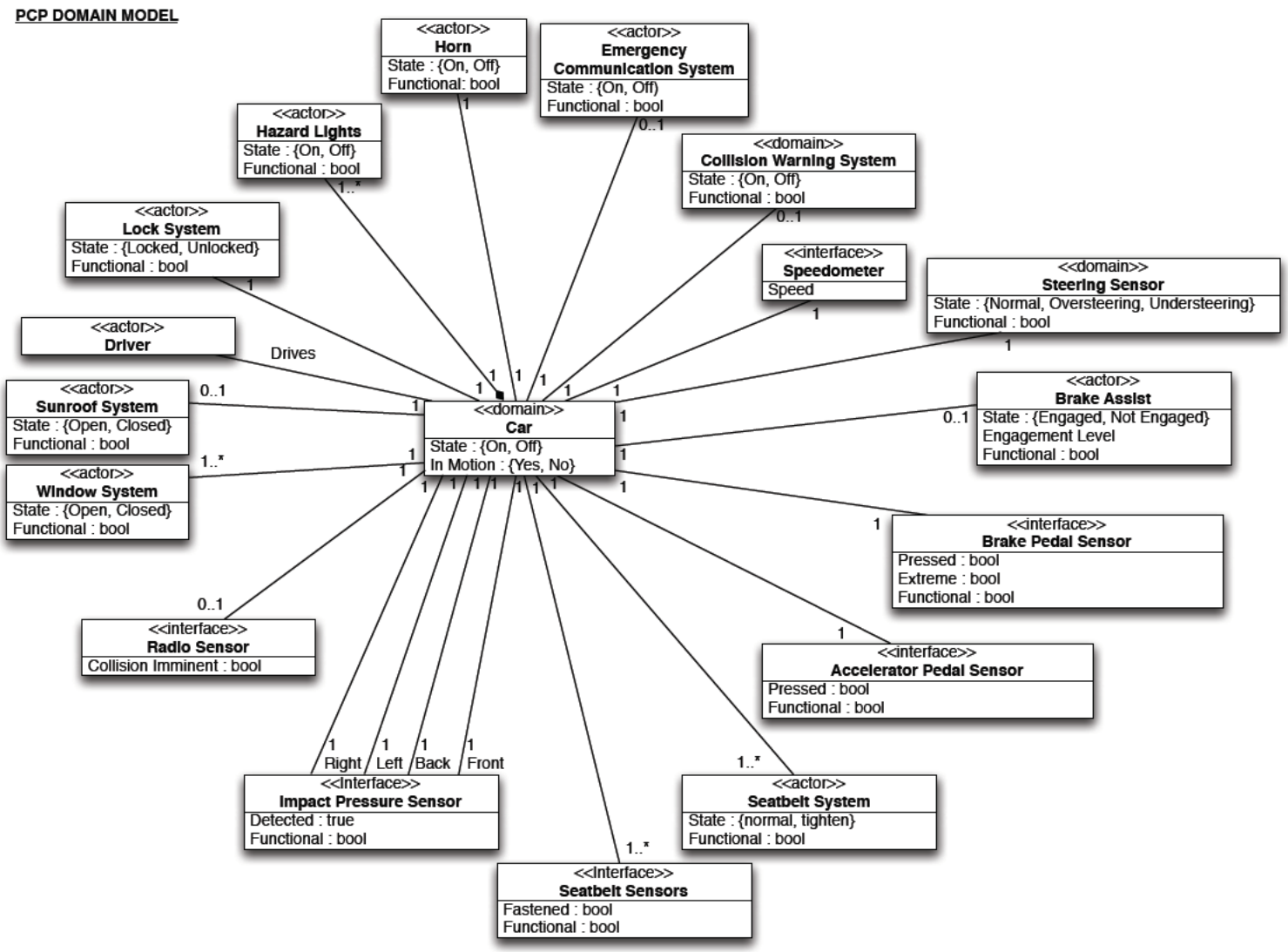

Figure 8 Domain model for the pre/post collision protection system

The following describes the input events for the PCP system.

Input Events

- oversteering - event when oversteering is detected, car.steering sensor = oversteering
- understeering - event when understeering is sensed, car.steering sensor = understeering
- extremeBraking - event when extreme braking is detected, car.brake pedal sensor.extreme = true
- braking - event when when brake pedal is engaged, car.brake pedal sensor.pressed = true
- radioSensor - radio sensor detects imminent high speed collision, car.radio sensor.collision imminent = true

- impact(s) - impact detected on side s, car.s.impact pressure sensor.detected = true
- accelerate - acceleration pedal pressed, car.accelerator pedal sensor.pressed = true
- malfunction(s) - when any subsystem s is malfunctioned, car.s.malfunction = true
- collisionImminent - oversteering OR understeering OR extremeBraking OR radioSensor
- collisionAvoided - conditions indicate that the collision is no longer imminent
- carRestart - car has been turned off and then on, car.state = on -> car.state = off -> car.state -> on

3.2 Functional Requirements

3.2.1 Use Case Descriptions

The use cases for the blind spot detection system are shown in Table 1. The order of interactions between actors are show exactly which steps are being taken and when. Exceptions and alternatives that may happen during each use case are also outlined.

Table 1 Fully dressed use case descriptions for the blind spot detection system

<table>
<tr><td colspan="2">Name: Alerted of Blind Spot</td><td>UC1</td></tr>
<tr><td colspan="3">Authors: Group 10
System: Blind Spot Detection
Actors: Driver, Sensors
Pre-Conditions:
• System is enabled
• Car is above speed threshold of 30 km/h
Overview: The user is alerted by the corresponding side mirror that there is an object in their blind spot.
Related Use Cases: None
References: Customer Session 1, 2, 3, 4</td></tr>
<tr><td>Driver</td><td>Blind Spot Detection</td><td>Sensors</td></tr>
<tr><td>1. Car is in ‘Drive’, speed is over 30 km/h</td><td></td><td></td></tr>
<tr><td></td><td></td><td>2. Sensor(s) detect objects in range</td></tr>
<tr><td></td><td>3. System illuminates corresponding side mirror</td><td></td></tr>
<tr><td colspan="3">Alternative 1 – Driver speed falls below 30 km/h
Step 1, 2, 3
System does not activate
Exit Use Case</td></tr>
<tr><td colspan="3">Alternative 2 – Driver changes gear to something other than ‘Drive’
Step 1, 2, 3</td></tr>
</table>

System does not activate **Exit Use Case**		
Alternative 3 – Driver disables BSD system **Step 1, 2, 3** **Exit Use Case**		
Alternative 4 – Driver signals in direction of detected objects **Step 2**		
	3. System illuminates corresponding side mirror and activates sound alert	
VARIANT – Vibrating steering wheel **Alternative 5 – Driver signals in direction of detected objects and** **Step 2**		
	3. System illuminates corresponding side mirror, activates sound alert, and vibrates steering wheel	
Exception 1 – Sensors are not functional **Step 1, 2, 3**		
	1. System illuminates dash light indicating which sensor(s) is not functional	
	2. **Go To Step 2 in UC1**	
Exception 2 – No car enters blind spot **Step 1, 2** **System does not activate** **Exit Use Case**		
Exception 3 – Car leaves blind spot **Step 3**		
	4. System extinguishes corresponding side mirror	

The use cases for the parking assist system are shown in Table 1. The order of interactions between actors are show exactly which steps are being taken and when. Exceptions and alternatives that may happen during each use case are also outlined.

Table 2 Fully dressed use case descriptions for the parking assist system

Name: Alerted of Nearby Objects	**UC2**
Authors: Group 10 **System:** Parking Assist **Actors:** Driver, Sensors **Pre-Conditions:**	

- System is enabled – white “functional” dash light is illuminated
- Parking brake is off
- Car speed is below 18 km/h
- Car gear is in Drive (D), Reverse (R), or Neutral (N)

Overview: The user is alerted audibly and visually that their car is approaching an object while in a parking situation.
Related Use Cases: None
References: Customer Session 1, 2, 3, 4

Driver	**Parking Assist**	**Sensors**
1. Car is in D, R, or N, parking brake is off and traveling at a speed less than 18 km/h		
		2. Sensors detect objects in car's path
	2.1. System audibly and visually alerts the driver	
		2.2 While sensors detect decreasing distance between car and object
	2.2.1 System increases visual and audible alert frequency	
Alternative 1 – Car's speed increases past 18km/h **Step 1, 2.***		
	*. System stops alerts **Exit Use Case**	
Alternative 2 – Driver changes gear to something other than D, R, or N **Step 1, 2.***		
	*. System stops alerts **Exit Use Case**	
Alternative 3 – Driver disables PA system **Step 1, 2.***		
	*. System stops alerts **Exit Use Case**	
Alternative 4 – Parking brake is enabled **Step 1, 2.***		
	*. System stops alerts **Exit Use Case**	
Exception 1 – No object is nearby **Step 2.*** Driver is not alerted **Go To Step 1 in UC2**		

Exception 2 – Sensors are not functional **Step 1, 2.***		
	2. System illuminates grey dash light indicating a system malfunction and extinguishes white "functional" light	
	3. **Go To Step 2 in UC2**	

The use cases for the tire pressure monitoring system are shown in Table 1. The order of interactions between actors are show exactly which steps are being taken and when. Exceptions and alternatives that may happen during each use case are also outlined.

Table 3 Fully dressed use case descriptions for the tire pressure monitoring system

Name: Reset Base Tire Pressure	**UC3**
Authors: Group 10 **System:** Tire Pressure Monitoring **Actors:** Driver **Pre-Condition:** • Driver presses button after changing tire pressure(s) • System is always on and active unless malfunctioning **Overview:** The tire pressures have been modified and the driver wishes to set the current pressures as the new points of comparison **Related Use Cases**: 4 **References:** Customer Session 1, 2, 3, 4	
Driver	**Tire Pressure Monitoring**
1. Driver presses button to set new tire pressure baselines	
	2. System executed **UC 4**
	3. System updates "base" tire pressures
	4. System clears tire pressure warnings, displays green dash light
Exception 1 – New tire pressures are not valid **Step 2** **Exit Use Case**	
Exception 2 – Incompatible wheels are installed **Step *** **Exit Use Case**	

Name: Reset Base Tire Pressure	**UC3**
Authors: Group 10 **System:** Tire Pressure Monitoring **Actors:** Driver **Pre-Condition:** • Driver presses button after changing tire pressure(s) • System is always on and active unless malfunctioning **Overview:** The tire pressures have been modified and the driver wishes to set the current pressures as the new points of comparison **Related Use Cases**: 4 **References:** Customer Session 1, 2, 3, 4	
Driver	**Tire Pressure Monitoring**
1. Driver presses button to set new tire pressure baselines	
	2. System executed **UC 4**
	3. System updates "base" tire pressures
	4. System clears tire pressure warnings, displays green dash light
Exception 1 – New tire pressures are not valid **Step 2** **Exit Use Case**	
Exception 2 – Incompatible wheels are installed **Step *** **Exit Use Case**	

The use cases for the pre/post collision protection system are shown in Table 1. The order of interactions between actors are show exactly which steps are being taken and when. Exceptions and alternatives that may happen during each use case are also outlined.

Table 4 Fully dressed use case descriptions for the pre/post collision protection system

Name: Notified of imminent collision	**UC5**
Authors: Group 10 **System:** Pre/Post Collision Protection **Actors:** Driver, Steering Sensor **Pre-Conditions:** • System is always on • Car is travelling above speed threshold **Overview:** User is notified of imminent collision when the vehicle has entered an unavoidable collision situation. **Related Use Cases**: 6, 7, 8	

References: Customer Session 1, 2, 3, 4		
Driver	**PCP System**	**Steering Sensor**
1. Driver is above speed threshold.		
		2. Steering sensor detects understeering or oversteering
	3. System warns the driver that a collision is imminent	
VARIANT – Collision Warning System **Exception 1 – Collision warning system detects imminent collision** **Step 2**		
Driver	**PCP System**	**Collision Warning System**
		2. Collision warning system detects imminent collision
	3. System warns the driver that a collision is imminent	
Exception 2 – Break sensor detects imminent collision **Step 2**		
Driver	**PCP System**	**Break Pedal Sensor**
		2. Break pedal sensor detects extreme braking
VARIANT – Radio Sensor **Exception 3 – Radio sensor detects imminent high speed collision** **Step 2**		
Driver	**PCP System**	**Radio Sensor**
		2. Radio sensor detects imminent high speed collision
	3. System warns the driver that a collision is imminent	
Exception 4 – PCP System Malfunctions **Step *** System fails to notify user about imminent collision **Exit Use Case**		
Exception 5 – Sensor/collision detection system malfunctions **Step *** System enters malfunction state **Exit Use Case**		

Name: Maximize safety before collision	**UC6**

Authors: Group 10
System: Pre/Post Collision Protection
Actors: Driver, Seatbelt Sensor, Window System, Sunroof System
Pre-Conditions:

- System has detected imminent collision

Overview: System tightens seatbelts, brake assist is engaged if driver initiates braking, open windows are mostly closed leaving a slight opening, if sunroof is present and open it is closed.
Related Use Cases: 5, 7, 8
References: Customer Session 1, 2, 3, 4

Driver	PCP System	Seatbelt Sensor	Window Sys.	Sunroof Sys.
1. Driver is in an imminent collision situation				
	2. System initiates pre-collision protection features			
3. If brakes are engaged by driver				
	3.1 System activates brake assist			
		4. If seatbelt pressure sensors detect pressure above threshold		
	4.1 System tightens seatbelts			
			5. If window state sensor detects open windows	
	5.1 System closes windows leaving a small opening			
				6. If sunroof sensor detects open sunroof

	6.1 System closes sunroof			
8. Driver collides with object or vehicle				
Alternative 1 – Seatbelts not fastened **Step 4**				
		4. Seatbelt pressure sensor detects that seatbelt(s) is not fastened **Go to Step 5 UC6**		
Alternative 2 – Driver taps accelerator **Step *** System disengages brake assist **Return to step that was executing before interruption**				
Exception 1 – Brake assist malfunctions **Step 3.1**				
	2. System fails to activate break assist **Go to Step 4 UC6**			
Exception 2 – Seatbelt sensor malfunctions **Step 4**				
		4. Seatbelt pressure sensor fails to detect pressure **Go To Step 5 UC6**		
Exception 3 – System fails to tighten seatbelts **Step 4.1**				
	4.1 System malfunctions and fails to tighten seatbelts **Go to Step 5 UC6**			
Exception 4 – Window state sensor malfunctions **Step 5**				
			4. Window state sensor fails and does	

			not detect open windows **Go to Step 6** **UC6**	
Exception 5 – System fails to close windows **Step 5.1**				
	5.1 System malfunctions and fails to close windows **Go to Step 6** **UC6**			
Exception 6 – Sunroof state sensor malfunctions **Step 6**				
				6. Sunroof state sensor fails to detect open sunroof **Go to Step 7** **UC6**
Exception 7 – System fails to close sunroof **Step 6.1**				
	6.1 System malfunctions and fails to close sunroof **Go to Step 7** **UC6**			

Name: Minimize damage during collision	**UC7**
Authors: Group 10 **System:** Pre/Post Collision Protection **Actors:** Driver, PCP System **Trigger Event:** User collides with object or vehicle. **Overview:** Brake assist continues even if driver disengages brakes during collision. **Related Use Cases**: 5, 6, 8 **References:** Customer Session 1, 2, 3, 4	
User	**PCP System**
1. User collides with object and has released brake	
	2. System engages brake assist
Alternative 1 – User does not disengage brake	

Step 1 **Exit Use Case**	
Exception 1 – System fails to engage brake assist **Step 2**	
	2. System malfunctions and fails to engage brake assist **Exit Use Case**

Name: Minimize damage after collision	**UC8**
Authors: Group 10 **System:** Pre/Post Collision Protection **Actors:** Driver, Emergency Communication System, Hazard Lights, Horn, Door State sensors **Trigger Event:** User has collided with object or vehicle. **Overview:** Hazard lights are switched on, doors are unlocked and horn is sounded. If available, emergency services are contacted with vehicle position. **Related Use Cases**: 5, 6, 7 **References:** Customer Session 1, 2, 3, 4	

User	**PCP System**	**Emergency Communication System**	**Impact Pressure Sensors**	**Hazard Lights**	**Horn**	**Door State Sensors**
1. User has collided with an object or vehicle						
			2. Pressure sensor detects collision			
	3. PCP system initiates post-collision protection features					
		4. Emergency Communication				

		System requests user to call emergency services				
				5. Hazard lights are switched on		
					6. Horn is turned on	
						7. If door sensors detect locked doors
	7.1 System unlocks doors					
Exception 1 – Emergency communication system fails **Step 4**						
		4. Emergency Communication System fails to request user to call emergency services **Go to Step 5 in UC14**				
Exception 2 – Hazard Lights fail to turn on **Step 5**						
				5. Hazard lights fail to switch on **Go to Step 6 in UC14**		
Exception 3 – Horn fails to sound **Step 6**						
					6. Horn	

				fails to sound **Exit Use Case**	
Exception 4 – Sensors fail to detect locked doors **Step 7**					
					7. Sensors malfunction and fail to detect locked doors **Exit Use Case**
Exception 5 – System fails to unlock doors **Step 7.1** **Exit Use Case**					
Exception 6 – Impact Sensors fail to detect collision **Step 2** **Exit Use Case**					

3.2.2 State Machines

For descriptions of interface elements including input and output events please refer to Section 3.1 External Interfaces.

The state machine for the blind spot detection system is shown in Figure 9. The state machine shows the different states the system can be in as well as the transition between the various states.

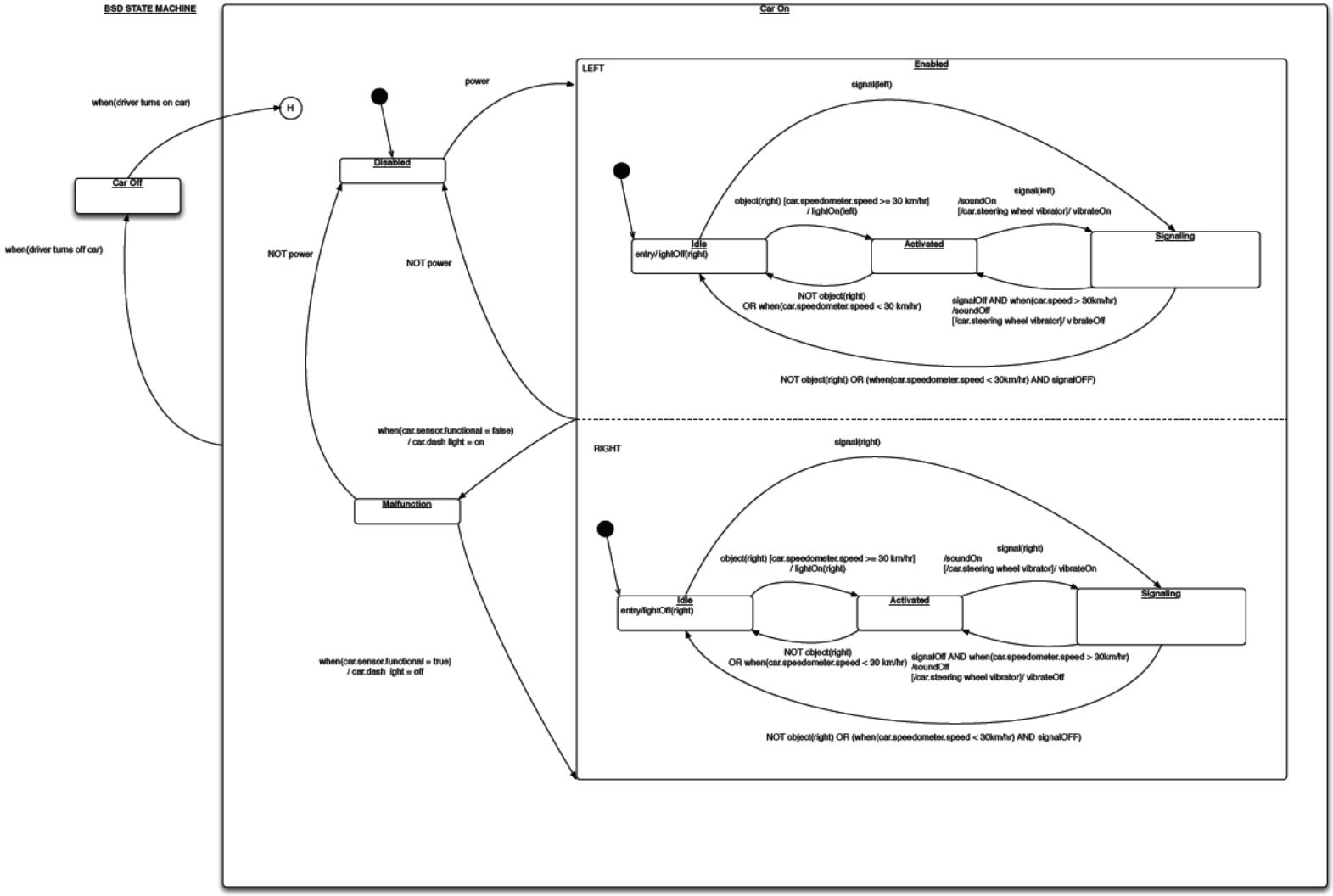

Figure 9 The state machine for the blind spot detection system

The state machine for the parking assist system is shown in Figure 10. The state machine shows the different states the system can be in as well as the transition between the various states.

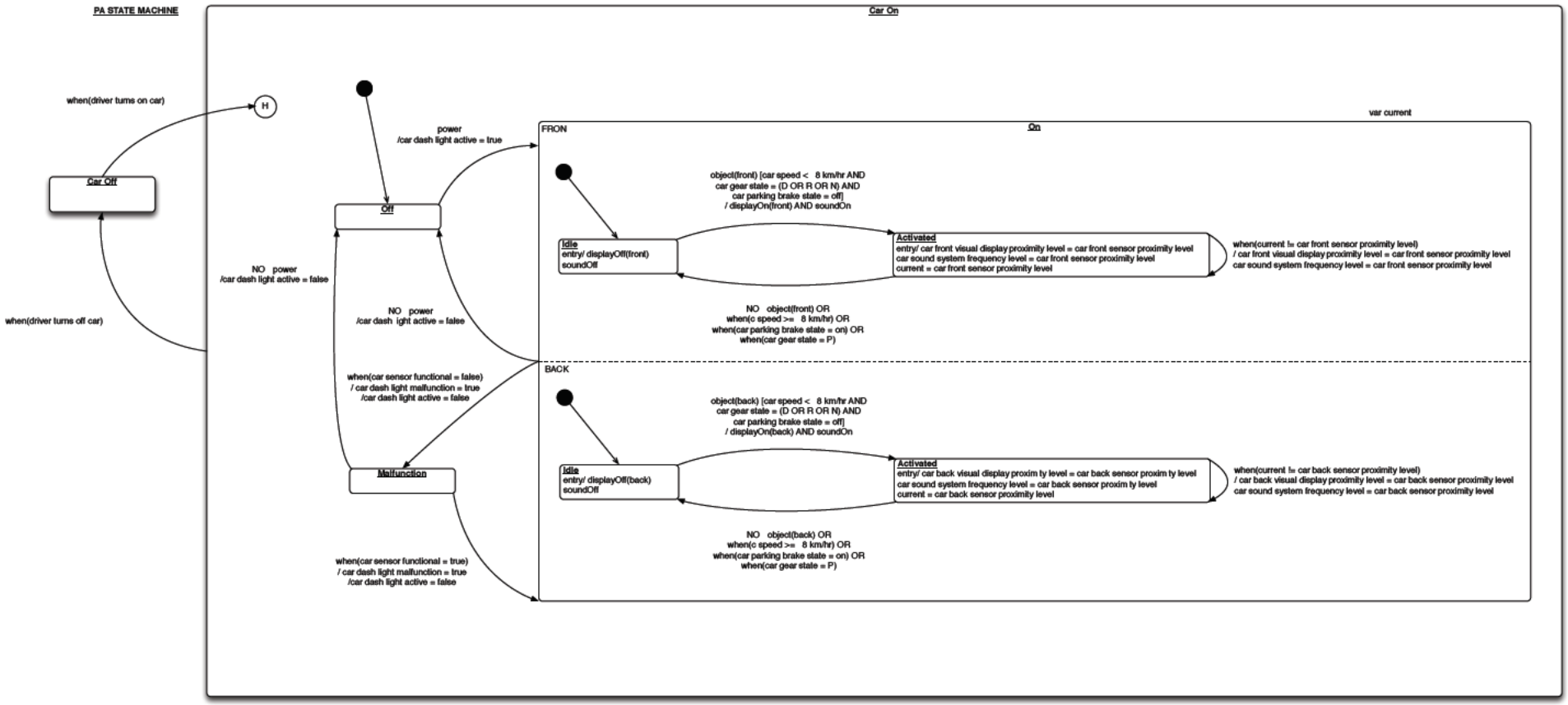

Figure 10 The state machine for the parking assist system

The state machine for the tire pressure monitoring system is shown in Figure 11. The state machine shows the different states the system can be in as well as the transition between the various states.

The state machine for the tire pressure monitoring system is shown in Figure 12. The state machine shows the different states the system can be in as well as the transition between the various states.

3.3 Quality Attributes and Constraints

The most important attribute of all four active-safety systems is reliability. These systems need to be working at all times or they won't help the user when a potential accident scenario arises. Specifically, given sufficient power and working sensors all of the four active-safety features should be operating. Should the sensors fail it is expected that the system to which those sensors pertain will shut down gracefully and alert the user of a malfunction.

These systems also need to be easy for the driver to use and understand. If the alerts do not give the driver meaningful information that can be reacted to instantly then these active-safety features will not increase the driver's safety and may decrease it if the alerts distract the user too much.

Finally the systems must be robust. If one of the systems fails then the user should be notified so they do not rely on the system being functional. If a system fails and starts producing false alerts to the user they will become very distracted which is dangerous.

For the tire pressure monitoring system the system should be polling the sensors every 15 seconds. The system should take at most 20 minutes to notify the user of a bad tire pressure reading. Additionally, the system should know which sensor reading corresponds with which tires.

For the blind spot detection system it is expected that the system should respond within 0.7 seconds. Additionally, the system is only expected to detect cars when the difference in speeds between the car and the detected vehicle is no larger than 12 km/h.

For the PCP system it is expected that should sensors fail when a collision situation has arisen, the PCP process should still be carried out.

For all systems it is expected that objects outside of their range will not be detected and will note activate the those related systems.

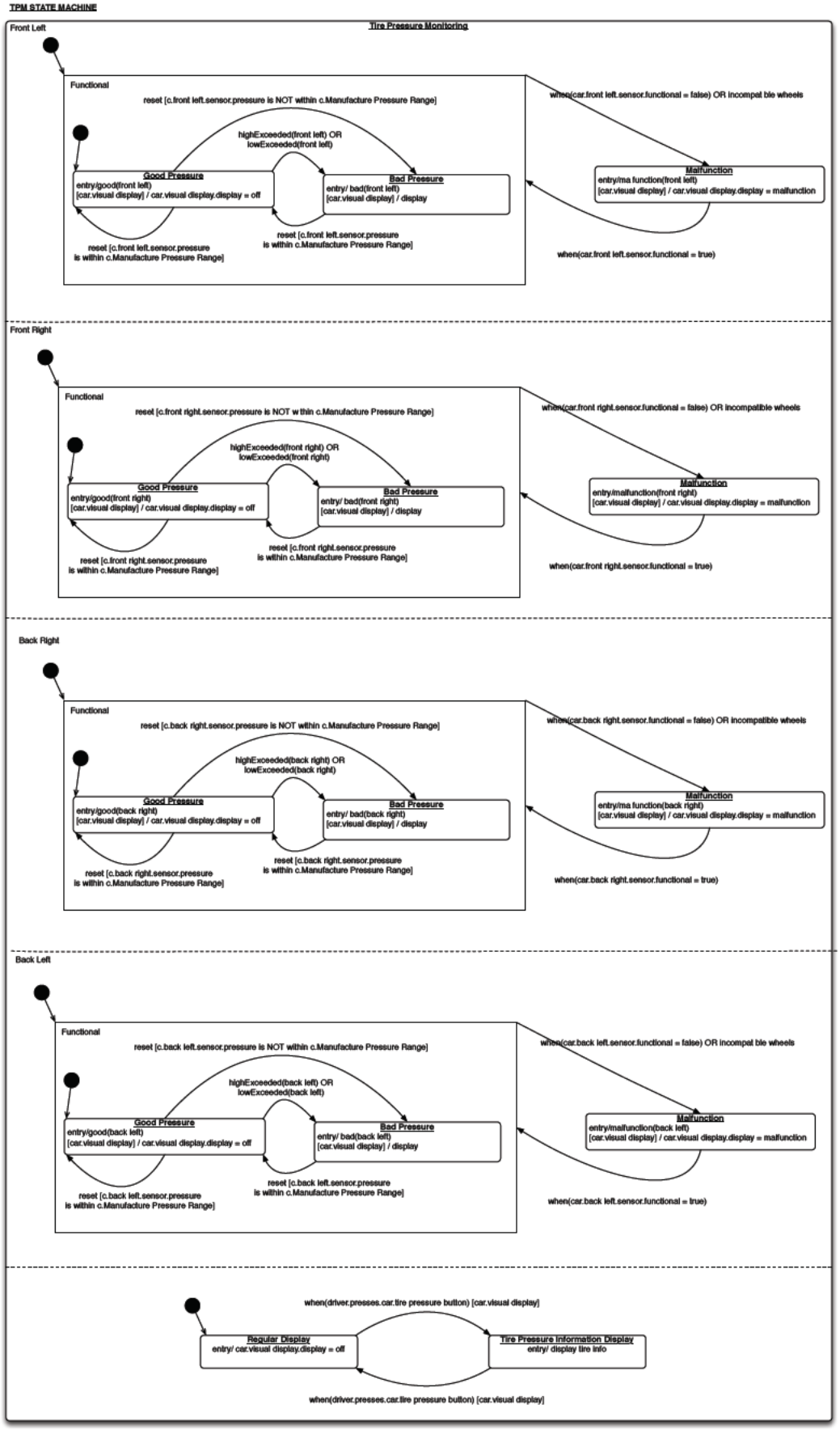

Figure 11 The state machine for the tire pressure monitoring system

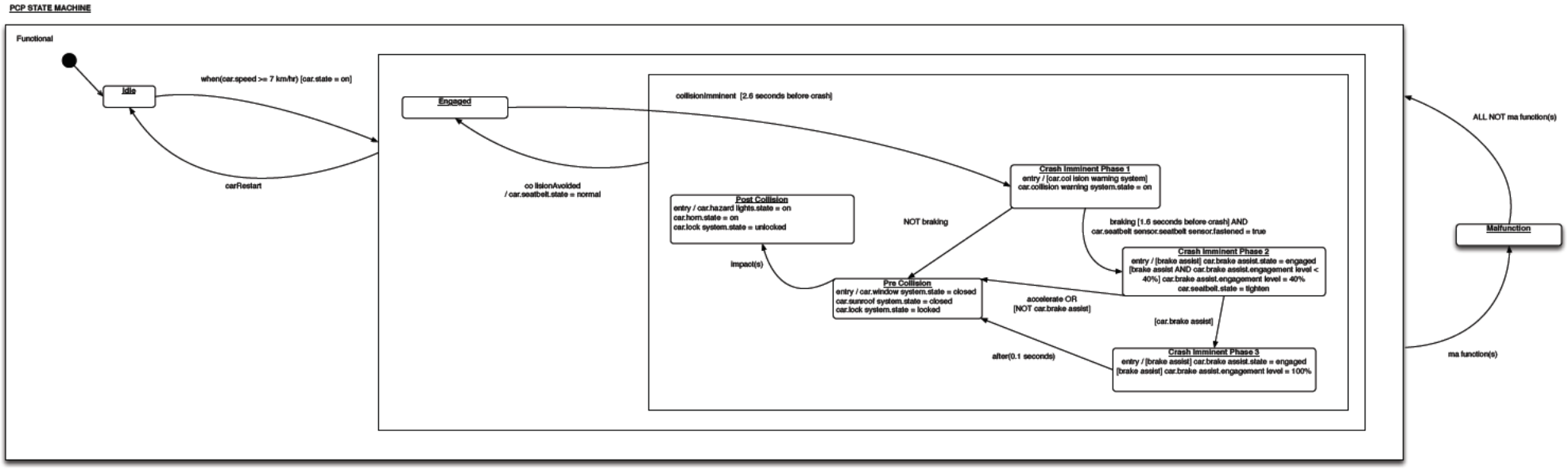

Figure 12 The state machine for the pre/post collision protection system

Appendix A

CS 445 / ECE 451 / CS 645
Software Requirements Specification and Analysis
Winter 2014 Project: Active Safety Features

Overview
A decade ago, a high-end automobile had only 20 or so electronic control units (ECU) with one million lines of code that controlled mainly powertrain, body, and infotainment systems. The development costs of this software were around $400 per vehicle. Today's average vehicle has over 50 ECUs with 100 million lines of code; and has additional controls for telematics, active and passive safety, advanced propulsion, entertainment systems, and middleware software that interconnects all of the above. The software-development costs for a vehicle today is over $1000 – a significant portion of the total cost of a vehicle. The software content and complexity will grow even faster in the next few years as more advanced features are realized – especially new features to enhance the safety of both passengers and pedestrians. The automotive sector is a consumer market that demands feature-rich systems, rapid time-to-market, and zero tolerance for safety errors.

Active Safety
An active-safety feature is an automotive feature that proactively monitors a vehicle's environment and takes action to avoid a collision; or, if a collision is unavoidable, mitigates the damages. Such features have software controllers that monitor sensors, process the sensed data, detect hazards or errors, operate actuators, communicate with other systems (e.g., call emergency personnel in the event of an accident), and/or log events. In contrast, passive-safety features tend to be mechanical devices that need not be activated by software (e.g., seatbelts, airbags, bumpers). For example, Electronic Stability Control (ESC) is a collection of active-safety features that focuses on avoiding or reducing the severity of loss-of-control accidents. These features take affect when a driver is (or may be) about to lose control of his or her vehicle, such as when wheels slip on slippery roads or when the vehicle skids because it is speeding while turning. The goal of ESC is to detect such hazards and to take corrective action, so that the driver can maintain or more easily regain control of the vehicle. Most active-safety features are optional features, but some (like ESC) are mandated by law because studies have shown that the features demonstrably improve passenger safety.

For this project, you will elicit and specify the requirements of four new active-safety automotive features. Below are high-level conceptual descriptions of the new features.

Blind Spot Detection (BSD)
Blind Spot Detection (BSD) warns the driver if there are vehicles in the driver's blind spot (i.e., in an adjacent lane, either beside or just behind the driver's car).

Parking Assist (PA)
Parking Assist (PA) helps the driver to park in a tight parking spot, by warning the driver of objects that are near the vehicle.

Tire Pressure Monitoring (TPM)
As the name suggests, Tire Pressure Monitoring (TPM) aims to notify the driver if the air pressure in one of the vehicle's four tires is low.

Pre/Post Collision Protection (PCP)
Pre/Post Collision Protection (PCP) acts in the minutes before, during, and after a collision to mitigate damages and to make it easier for passengers to escape or to be rescued. If the feature determines that a collision might be imminent, it prepares the vehicle and passengers for impact (e.g., tightening seat belts). On impact, the feature deploys the airbags and helps to bring the vehicle to a stop. After impact, the feature attempts to avoid secondary consequences of the collision and to aid the passenger and emergency personnel (e.g., turning on hazard lights).

Your team's task is to flesh out the details of the above features: their goals, their functionality, their nonfunctional requirements, etc; to model various aspects of the features' requirements; and eventually to document all of the details in a Software Requirements Specification. The SE1 project exemplifies some of the key challenges of engineering software-controlled automotive systems:

Safety-critical functions: The features offer safety-critical functionality. Their operation must not cause undesirable and unsafe situations, such as unsafe braking or acceleration. *Your feature specifications must consider what should happen in the presence of failures or unexpected road conditions (e.g., no lane markings).*

Real-time constraints: The features must meet stringent deadlines in order to perform satisfactorily. For example, in PCP, the airbags should be fully deployed within 80ms of the start of the collision. *Your feature specifications must consider real-time constraints and other nonfunctional requirements.*

Interfacing with sensors and actuators: The features communicate with multiple sensors and actuators. *Your feature specifications must consider, at a high level, the numbers and types of sensors and actuators the features will monitor and control.*

Explosion of variants: Features can have dozens of major variants, based on the use of different sensors or actuators (e.g., number and types of airbags), different functionality (e.g., different warning levels depending the degree of hazard), or the presence of other features (e.g., whether the driver subscribes to a Collision Notification service that is called when the vehice is involved in a collision). *Your feature specifications must include a total of at least five variations.*

Appendix B1

Q and A Session 1 Minutes – Monday January 27, 2014

Blind Spot Detection

How does it know there is a vehicle? Radio sensors at the sides of the rear bumper. In case of sensor failure what happens?

There should be an indication to the user that a sensor is not working. Two sides should work somewhat independently. One side can be broken while the other side still works.

How should the system let the driver know about something in the blind spot?

On the mirror there should be a light that illuminates when there is a vehicle in the blind spot. When indicating that you want to do a lane switch there should also be a sound to indicate something in the blind spot. Should always be able to hear it over radio.

Does it try to control the vehicle?

No, never take control away from the driver. It is strictly a warning system.

Should it only detect vehicles?

Sensors detect anything in that region not strictly only vehicles.

What if you're stuck in traffic?

There is a minimum speed at which this feature is active. It won't alert below this threshold speed.

It is expected that the sensors have limits and there will be conditions at which we will no longer have accurate readings. If the sensor technology is such that we can monitor the conditions reliably and notify the driver we should do so.

If we see output that is outside of operational range this will likely indicate that it is faulty.

Does it take into account seat or driver height? No. The driver should know that they cannot fully rely on the system. Should the user be able to turn off this feature? Yes.

Tire Pressure monitoring

What is acceptable tire pressure?

The manufacturing company sets the safe delta for tire pressure.

25% approximately

The user resets the tire pressure "normal" whenever the tire is inflated or replaced.

Single signal that the user should check the tires or information for each tire as detailed number information.

There should be continuous monitoring of the tires.

The system should also measure the temperature to take into account the effect of temperature on pressure.

The sensor is accurate within 1-3 PSI. Should the user be able to turn off the system? No.

The system has an understanding of “normal” ranges. Dangerously low/high pressures are understood and the user is notified. This will handle mistaken resets.

The tire monitoring system communicates wirelessly (radio) with the main car system.

Do we get firmware updates? In theory yes at servicing but this is for exceptional circumstances.

Can other systems use this data? Yes. It is expected that sensors are suited to the operating conditions of the given market.

Parking Assist

Do we need to accommodate disabled drivers? There should be audio as well as visual alerts. How does the feature work? There are sensors in the front and in the back that notify the user about obstacles. How is it activated?

It is automatically activated. If not in park and no hand brake and it also has to be below a certain speed.

It can be manually disabled and enabled.

The sensors are distributed along the front and back bumpers including corners. The visual queue should let you know the approximate distance of objects. The front 100 cm, corner 60 cm, back 120 cm. Should not affect the vehicles dynamics. Does not take control of vehicle.

What kind of beeps? Audio queue frequency will change depending on the distance of objects.

Ultrasonic. Only those materials, which reflect the signal are “visible”.

If we can detect obstruction that let the user know. And let the user know about the limitations of the system.

How many sensors? 6 in the front and 4 in the back. If any sensors fail that side will fail. EDIT: Variable depending on vehicle. BSD and PA are independent. Can only temporarily turn off the system.

PCP

Should it be able to detect between different types of collisions? It can detect extreme braking, extreme over or under steering.

Collision Warning System (out of scope, separate system) - System will indicate to user to break and if user takes this action the system applies max breaking.

Collision warning system with camera (60 km/hr) radar (180 km/hr)

Can detect impact for side, front, back collision.

Once detected – Call 911, if available on the system.

Tighten seatbelts close windows (slight gap remaining) and sunroof.

Hazard lights, some cars have horns, unlock doors, dial emergency services if you can.

System is configurable to the features in the car.

Collision warning will do the breaking etc. If you interact with accelerator it will disable the max breaking.

Yes, you can turn it off until you restart the car. Break assist is activated by the system if available by pre-collision system. Uses other systems to detect collisions.

Appendix B2

Q and A Session 2 Minutes – Monday February 3, 2014

Pre/Post Collision System

What are all the systems that PCP controls?

Before collision – notification

During collision – Belts, brake, windows, sunroof

After collision – If airbag or seatbelts activated then send position to 911, lights, horn

Should battery power be cut?

No.

What equipment do these cars have installed?

Highly variable. Abstract away this variability. Every car must be able to alert the user in some way.

If something is attached to something at the back of car, will it still detect crash?

Radar is at front it can predict frontal collision. It wont detect it if it is at the front.

Is this system responsible for detecting the crash/asking the driver to react? Or is the system strictly responsible for preparing to crash?

It detects collisions that cannot be avoided and prepares for those collisions (by using radar with speed etc.). It notifies the user of an imminent collision but does not ask the user to take evasive maneuvers.

How does it take collisions that have already happened?

Pressure sensors.

What sensors are used by the system?

Radar in front, sensors for detecting which side of collision.

Should we notify user of tailgating?

No.

If car fails, will we notify other people/drivers?

No.

Does it work if idle?

No min. 7 km/hr.

The range of speeds that this feature works for depends on quality of sensors.

Minimum sensors required?

Radars/camera and pressure (mandatory for airbags).

Are airbags are outside the scope of this feature?

Yes, they act on their own.

When does braking not happen?

When seatbelt is not fastened it will take no braking action.

What happens with broken sensors?

It checks the status of other systems ABS, and sensors. Will notify if sensors are not reading well.

Does PCP take into account if the car is turning?

Other systems work together to take into account these types of scenarios.

Does it take into account the mode of the car?

No.

Will PCP apply brakes?

Will only apply brakes if wearing seatbelt. A little, it is the drivers responsibility to apply it then the system takes over to apply it fully until stop. (Even if not wearing seatbelt and it is tapped it will engage.) Seatbelts applies to front two seats.

Will system break if crash has already happened and break was not engaged?

I don't know.

Can this feature be disabled?

Cannot disable feature.

Does the hand break interact?

No.

Part Assist

Will moving forward enable front sensors and back back sensors?

Yes.

Does it take into account wheel direction?

No.

What are activation conditions?

Drive/or reverse and no hand brake.

Can system differentiate between driving and parking?

Yes by threshold speeds and gears.

Is there a button?

Yes, manual activation.

Does it automatically deactivate?

Yes.

What are the alerts?

Visual alert is distance with 3 levels. On display or series of LEDs. Audio is frequency of beeps. Level 1 beep every 2 seconds, level 2 every 1 second and the other is continuous.

Would system warn you in traffic?

Can be manually turned off. Threshold speed 18 km/hr.

Powering the system. Does it turn off until it is re-enabled or on car restart?

It will automatically be re-enabled.

How should the user be warned about sensor malfunction?

It will be specific for the sensor (front/back) through light in the dash.

When it manually enabled it will automatically disable when conditions are not met.

Tire Pressure Monitoring

How does the reset work?

It resets for the tire pressure of each tire.

Can you reset to factory?

No.

How does it display pressure?

Lights or exact values. It will depend on the system.

How often does it give notice?

Continuous monitoring.

Does it store historical data?

No.

Is it direct or indirect TPM?

Direct TPM.

Do you have to have compatible tires?

No it's the wheel must be compatible with the car.

How is it powered?

It depends. (Doesn't really matter)

What is the threshold?

25% percent difference is the threshold to indicate low or high pressure.

What happens for sensor malfunction?

A general system malfunction will be indicated.

What if reset value is out of range?

Some sanity checks in place to detect reset out of range. Warnings will be the same in the case that it is wrong on reset.

Gray – malfunction, Green – Good, Red – check tires.

Requires display for TPM.

Blind Spot Detection

How does it monitor lane change?

Signaling.

How does it detect blind spot?\

Sensors on the side of the rear bumper such that the range can detect.

What is the threshold speed?

30 km/hr

How does enabling work?

Must enable manually. Will disable every time car is turned off.

How do we tell user that sensors are not okay?

Light on dash.

Are lights always there?

Yes, mandatory.

How close does it have to be to work?

See drawing. (50cm + 3 m on sides and 3 m from back)

Within the thresholds are there other things that happen?

Maybe, they are out of scope.

Can you extend functionality based on trailer? No.

How do you indicate which sensor is broken?

Left and right dash light warnings.

When you're driving leftmost lane and there is a boundary will it activate?

Sure, depends on boundary conditions.

Does it make the car do anything?

Does not affect dynamics of the car.

Appendix B3

Q and A Session 3 Minutes – Monday March 17, 2014

PCP

Which of the things that the system controls have priority?

1. 2.6 seconds before a crash - get audio and visual warning

2. 1.6 seconds 40% strength braking and tighten seatbelts tighten

3. 0.6 seconds full braking

When will it call for help?

When airbags are deployed. Always ask user if they want to call for help, if they don't get a response then call for help.

How does the system know a collision is going to happen?

They know about the effectiveness of breaking for a given speed and distance to full stop. Does not adjust for snow etc.

What is the initial state?

Will perform check of all the sensors and see what is working etc.

What are the secondary features? Highly variable depending on the car

Explain the breaking feature?

press break it will press brake to fullest if you press acceleration it will disengage brake assist

Are airbags part of the system? No

How is PCP system reset? Yes, in the service center.

What is the speed threshold for this to be activated? 7 km

When does the system call/ask to call 911? After the crash ends

When are the features (lights) reset? turn car off then on again.

PA

What is the distance for

Front 1.6 meters

Back 4 ft

Can't detect anything within 6 to 8 inches

Will the warning levels change continuously or discretely? discretely

What if you have objects in front and back?

Alternating different sounds but only play sound for direction you are traveling

When is it active?

If user turns it off is it still monitoring? No.

If user turns it back on how long does it take? Negligible.

What are signals?

Grey - not active or engaged, White active and available, P for active and engaged

TPM

If reset button is pressed and there is error how quickly can they press button again? Right away. Will display that it is bad until you fix it.

Why don't we measure from thresholds?

Because we want to indicate changes from when you filled up last, it depends on the whether etc.

How many reset buttons? Just one for all tires

BSD

How quickly is it reacting to objects in the blind spots? Immediately, regard as real time system.

When does the steering wheel vibrate?

When you signal to change the lane and there is a car in that blind spot

How do we turn on/off?

Button but it stores the state between turning the car on and off. This also applies to BSD

Appendix B4

Q and A Session 4 Minutes – Monday March 24, 2014

TPM

How often poll?

15 seconds or so.. Should know about bad tire pressure within 20 minutes

What is the quality of the sensors? All about equal quality

How is malfunction detected?

Assume we know that there is a sensible range were values are valid.

What is the temperature range at which the system is functional Assume it will work given any temperature

What is the desired uptime?

It should always work given working sensors. System has 20 minutes to alert user of a malfunction.

What is the life of the sensors? 10-15 years. The life of the car.

During maintenance it's battery life is also communicated.

How reliable is the wireless communication system? It's so-so. There may be interference.

System should know what sensors corresponds to which location.

BSD

What is a graceful failure? System will shut down.

What should it be able to detect?

Some systems only detect cars, others detect larger objects.

What is the reliability?

Minimum size is a vehicle. It detects the speed of other vehicles. Difference between the two vehicles 12 km/hr. If it's more than this do not display the signal.

Response time: 0.7 seconds

Accuracy of reading. 1% error of accuracy PCP

What is the level of confidence with which it will predict a collision?

Can't accurately or quantitatively explain this. Rating agencies are separate. Minimally passable is reduction of 5 miles per hour in 2 out of 10 conditions.

Minimal acceptable response time for systems to initiate

(From the the previous timing information)

What are the conditions for functionality?

As long as there is power and there are sensor working then it should be engaging

Does it differentiate between crash severity?

Somewhat. Some systems e.g., lights will still be activated. Some kind of threshold for what an impact is. Pre crash is only for frontal. Post crash is for all types of crashes.

Doors should never lock they should unlock.

Does safety override security? Yes.

What are conditions for functionality? On.

What if sensors break during a crash? Still attempt all measures.

Maintainability: how easy etc.

Every year for maintenance. Upgrade and calibrate systems. "Out of scope"

Will the system shut down with malfunction? Depends on severity, may continue working. Need to continue monitoring for changing conditions.

What is the accuracy? 2 to 4 inches.

What type of error information will it get: nothing detailed. Just error message.

System should continue working if a sensor fails? If one fails. Shut down system.

What are minimum sizes? Anything below the sensors will not been seen.

How do we detect sensor failures? We assume we know absolutely.

What are power thresholds for these systems? Out of scope.