FASE Coursework – Electric Car Safety Controller

Alan Morrison (40400403)

SET10112

Abstract. In this paper, the design, and construction of an electric car controller optimised for safety will be explored. The introduction will give insight into the general problem cars pose to the welfare of people and why the solution proposed is suited to help this. A high-level overview of the safety controller structure, descriptions of the various procedures and functions which were used, and extensions to the minimum requirements are also detailed. The controller was implemented using Ada-SPARK and has achieved a SPARK level of Platinum. Finally, this report will also demonstrate how the proof of consistency for a procedure.

1 Introduction

Cars can be hazardous to individuals because of human error. However, by utilising automation to enable systems to make these safety-critical decisions for us, this error can be minimised and in some cases, removed, thus making car travel safer for individuals on and off the road. For these reasons this driver assistance system has been developed. To be considered successful, this controller must adhere to the following minimum requirements:

- The car cannot be turned on unless it is in Parked.
- The car cannot be driven unless there is a minimum charge in the battery.
- Once in motion, the system will warn of low charge
- The speed limit can never be exceeded.
- The speed of the car must be zero in order to change gear.
- If the car's sensor detects an object, then the car cannot move towards that object.
- The car must have a diagnostic mode which renders it incapable of any other operation

Along with the minimum specification, extensions have been included in the form of a sophisticated sensor system, which is able to differentiate between a general obstacle and another car being present. Various details about these obstacles are used to make safety-critical decisions such as when to perform an emergency stop and when automatic cruise control should be activated to match the speed of a vehicle in front. To ensure the correctness of this implementation, formal proofing is done using the

SPARK method. All the procedures and functions in this controller pass a SPARK level of Gold therefore this system passes at a Platinum level of SPARK.

2 Controller Structure

This chapter aims to give a high-level overview of the structure of the driver assistance controller for the electric car. Through Ada-SPARK, the electric car has been designed and implemented as a record that consists of various subrecords. These subrecords contain various user-defined data types as well as additional subrecords. This electric car record is defined as a global variable to allow various procedures to pass in information about the car's current state and alter variables about the car when required. The subrecords used to construct the safety controller are the engine record, the support record and the front sensor record.

2.1 Engine Record

The engine record contains all the variables which describe the current state of the car's engine.

EngineType			
Variable	**Type**	**Value**	**Description**
BatteryLevel	BatteryRange	(0..100)	The current level of charge present in the battery of the car
Gear	Gears	(ParkGear, ReverseGear, DriveGear, NeturalGear)	The gear which the car's gearbox has been set to.
Power	PowerState	(On, Off)	Whether the engine has been powered on or off.
Speed	SpeedRange	(0..200)	The speed at which the car is currently traveling at

2.2 Support Record

This record contains additional support information about the car's environment, its limits and its current state.

SupportType			
Variable	**Type**	**Value**	**Description**
BatteryWarning	BatteryWarningLight	(Lit, Unlit)	A light which is lit if the car has low battery and is in motion

DiagnosticMode	DiagnosticModeState	(Active, Inactive)	A diagnostic mode that when active, renders the car incapable of other actions
LowBattery	BatteryRange	(0..100)	Sets the limit at which the low battery light should be lit up.
MinBattery	BatteryRange	(0..100)	The minimum battery level required for the car to be able to be driven.
MinDistance	DistanceRange	(1..500)	The minimum distance an object can be from the car to prevent it from moving fowards
SpeedLimit	SpeedRange	(0..200)	The speed limit of the current road

2.3 Front Sensor Record

This record concerns the front sensor which is used to detect if anything is present in front of the electric car. The record utilises a variant subrecord which uses a case statement to determine the variables which should be set if an obstacle is present, absent, or is another car. If obstacles are absent, no additional variables need to be set.

ObstacleType				
Case When	**Variable**	**Type**	**Value**	**Description**
ABSENT	Null	N/A	N/A	If there is no obstacle present in front of the car, then the sensor reads there an obstacle is absent
PRESENT	PresentObstacle	PresentObstacleType	Record	If there is a present obstacle, the type for a present obstacle is set
OTHER_CAR	OtherCar	OtherCarType	Record	If there is front sensor detects another car, the type for another car is set

Present Obstacle Record

The front sensor is set to be the present obstacle record if the front sensor detects an obstacle is present.

PresentObstacleType			
Variable	**Type**	**Value**	**Description**
DistanceFromObstacle	DistanceRange	(1..500)	When an obstacle is present, it is a certain distance from the electric car

Other Car Record

If the front sensor detects another car, the other car record is set.

OtherCarType			
Variable	**Type**	**Value**	**Description**
DistanceFromCar	DistanceRange	(1..500)	When another car is present, the front sensor detects how far it is from the electric car
Facing	FacingType	(Away, Towards, Perpendicular)	The direction in which the other car is facing in comparison to the electric car
OtherCarSpeed	SpeedRange	(0..200)	The speed at which the other car is/is not traveling at

3 Description of Procedures and Functions

The goal of this chapter is to explain the procedures and functions implemented to meet the requirements set out for this controller. However, before these are specified, the electric car record is initialised in the specification file. For all procedures, the electric car is a global variable which is passed in as a ‘In_Out’ variable. This allows these procedures to pass in information about the current state of the car and to assign to all variables contained within the car. Each of the procedures and functions also contain preconditions and postconditions which specify the condition of the car before and after a procedure or function takes place. The correctness of these functions and procedures were validated using SPARK proofing and it was found that each passed at Gold level. Due to this it has been concluded that the safety controller as whole passes at Platinum level.

3.1 PowerOn Procedure (SPARK Gold Level)

The procedure changes the engine of the car to be powered on. As a result, the preconditions are the car's engine must be off, the car must be in Parked gear, the car must not be moving and the car battery level must be over the minimum level of charge. The post condition for this procedure is the car's engine must be set to be powered on.

3.2 PowerOff Procedure (SPARK Gold Level)

This procedure sets the car engine's power to be off. Therefore, the preconditions are the car must be powered on, the car gear must be in Parked gear, the car's speed must be 0 and the diagnostic mode must be inactive. The postcondition is that the power must be set to be off in the electric car.

3.3 MoveUpGear Procedure (SPARK Gold Level)

The car must be allowed to change gears; however, it should only be able to change gears in order from Parked to Reverse to Drive to Neutral. Hence, this procedure only changes the current gear to be the next gear in the enumerated type. From this, the preconditions are the car must be powered on, it must not be moving and the diagnostic mode must be inactive. Also, for the car to move up a gear it cannot be the last value in the enumerated type (i.e. Neutral gear). The postcondition for this procedure is the gear the car is set to is the next gear in the enumerated type for gears.

3.4 MoveDownGear Procedure (SPARK Gold Level)

As described in the "MoveUpGear" procedure, the electric car must only be able to change gears in order. Therefore, this procedure sets the current gear to be the gear before in the enumerated type for gears. The preconditions are the car must not be powered on, not moving and the diagnostic mode must inactive. Also, the current gear cannot be the first gear in the enumerated type for gears. (i.e. Parked gear). From these preconditions, the postcondition for this procedure is that the current gear is set to be the gear before in the enumerated type for gears.

3.5 Accelerate Procedure (SPARK Gold Level)

This procedure takes in a new speed as an input and then increases the current speed of the car by that amount. The preconditions are the car must be powered on, it must be in either Drive or Reverse gear, the current speed with the new speed added must be less than or equal to the speed limit, the diagnostic mode should be inactive, and the battery level must be above the minimum battery level set for the car. The new speed taken in as input must be bigger than zero however it cannot be over the speed limit. Some more preconditions include the front sensor must detect the road is absent or if does detect an obstacle or another, it must not be within a minimum distance of the car. The postcondition for the procedure is that the new speed of the car must be less than or equal to the speed limit and it must be larger than the speed the car was travelling at before the procedure took place.

3.6 Decelerate Procedure (SPARK Gold Level)

In this procedure, a new speed is taken as an input and the car's overall speed is decreased by that amount. For this, the preconditions are the car must be powered on, it must be in either Drive or Reverse gear, its current speed subtracted by the new speed taken in as an input must be more than or equal to 0, its current speed and the speed inputted must be more than 0. Diagnostic mode should also be inactive. The postcondition is that the speed of the car must be less than the old speed of the car.

3.7 WarningLight Procedure (SPARK Gold Level)

When the car is in motion, a warning lit will be lit if the battery level is low. The preconditions are the car must be powered on, it must be in Drive gear or Reverse gear, its speed must be above 0, diagnostic mode must be inactive and finally the car's battery level must be lower than or equal to the low battery amount. Since the outcome of this procedure is conditional, contract cases have been used instead of a postcondition. The contract cases are the warning light is lit once the car meets the preconditions however if not the warning lit remain unlit.

3.8 DiagnosticModeToggle Procedure (SPARK Gold Level)

This procedure toggles a diagnostic mode which renders the car incapable of other actions. The preconditions are the car must be in Parked gear, it must not be in motion and the car must not have low battery. The postcondition is that after the diagnostic mode procedure has taken place, the car must have switched from being Active to Inactive or from Inactive to Active.

3.9 WithinStopDistance Function (SPARK Gold Level)

This function takes in the speed of the car and the distance to an object and determines if another car is within stopping distance. The stopping distance is calculated by taking the car's current speed, converting from miles per hour to meters per second and then multiplying by 2 to find the meters the car will travel in 2 seconds.

3.10 EmergencyStop Procedure (SPARK Gold Level)

When the car is in motion, an emergency stop is performed if an obstacle or another car is detected by the front sensor and is within stopping distance. The preconditions for this procedure are that the car must be powered on, it must be in Drive gear, its speed must be above zero, the diagnostic mode must be inactive, the front sensor detects an obstacle and this obstacle is within stopping distance. Other preconditions include, the car detects another car, it is facing towards the car and the other car's speed is more than or equal to zero or the other car is not facing towards the electric car and its speed is zero. The postcondition for this procedure is the speed of the electric car must be zero.

3.11 MatchSpeed Procedure (SPARK Gold Level)

This procedure occurs when another car facing away, and the electric car reaches a minimum distance from the other car. When this happens, the electric car will match the speed of the other car. The preconditions for this procedure are the car's power must be on, it must be in Drive gear, its speed must be more than zero, diagnostic mode should be inactive, the front sensor must detect another car and it must be within a minimum distance from the other car. This other car must be facing away, its speed must be more than zero and travelling below the speed limit. Finally, the postconditions for this procedure are the speed of the car must match the other car, it must be above 0 but below the speed limit.

4 Proof of Consistency

Being able to decelerate is a key ability for the car therefore a formal proof of consistency for this has been provided below. A sequent calculus diagram has been constructed based on the premises and conclusions of the procedure and it has been shown that all branches end as axioms. This shows the formula is derivable and gives proof of consistency for this procedure.

The symbols used in this diagram are:

- p = car's current speed
- q = new speed
- SP = range of integer values for speed
- S = $S\text{P}'First$
- P = $S\text{P}'Last$
- L = current speed limit

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\ldots, p \in SP, q \in SP, p > S, p \le L, q > S, q \le L \Rightarrow p - q \in SP}\,\text{Ax} \qquad \dfrac{}{\ldots, p - q \ge 0 \Rightarrow p - q \ge 0}\,\text{Ax}}{\begin{array}{c}(p \in SP, q \in SP, P > S, L \le P, p > S, p \le L, p \le P, q > S, q \le L, q \le P, p \le q, p - q \ge S, p - q < p)\\ \Rightarrow \\ (p - q \in SP \land p - q \ge 0)\end{array}}\,\text{R}\land}{\begin{array}{c}(p \in SP \land q \in SP \land P > S \land L \le P \land p > S \land p \le L \land p \le P \land q > S \land q \le L \land q \le P \land p \le q \land p - q \ge S \land p - q < p)\\ \Rightarrow \\ (p - q \in SP \land p - q \ge 0)\end{array}}\,\text{L}\land..}{\begin{array}{c}\Rightarrow (p \in SP \land q \in SP \land P > S \land L \le P \land p > S \land p \le L \land p \le P \land q > S \land q \le L \land q \le P \land p \le q \land p - q \ge S \land p - q < p)\\ \supset \\ (p - q \in SP \land p - q \ge 0)\end{array}}\,\text{R}\supset$$

Fig. 1. Proof of Consistency for Decelerate Procedure

5 Extensions

This section of the report details the ways in which the minimum requirements have been extended. The safety controller was extended with the addition of the following features.

5.1 Sophisticated Front Sensor

The sensor system, as specified in the minimum requirements, only needed to be able to detect whether an obstacle was present or absent and based on this information make decisions such as if the car can move and when an emergency stop needed to be performed. With use of a variable record to specify exactly what the car detects; different types of obstacles can be specified with their own records and as a result information can be specific to them. For example, a generic obstacle and its distance from the car can be specified or another car, its distance from the electric car, the speed its travelling at and the direction in which its facing can be specified.

5.2 Nuanced Emergency Stop Decisions

Due to the inclusion of a front sensor which can determine the type of object is being detected. Decisions about when an emergency stop should happen can be more nuanced and specific to the object being detected. For example, if the front sensor just detects an obstacle and it's within the stopping distance then an emergency stop is performed however, if another car is detected, the decision to make an emergency stop may depend on the other cars speed, distance from the electric car and the direction in which its facing.

5.3 Automatic Cruise Control

The front sensor being able to detect if another car is in front of it and to store information about its speed and the direction its facing has allowed for the implementation of automatic cruise control. If another car is detected by the front sensor and it is facing away from the electric car, it will match its speed when it reaches a minimum distance from the other car.

5.4 Interactive Menu

An interactive menu has been implemented to allow a user to interact with the electric car controller to demonstrate the ways in which the controller has meet the specifications set out for it. In this menu, a user can display the current details of the car, toggle its power on or off, change its gear, accelerate, decelerate and toggle the diagnostic mode on or off.

6 Conclusion

The safety controller constructed for an electric car's gearbox is successful. This has been concluded due to the fact it meets all the minimum requirements and, in some areas, extended beyond this specification. Another reason this controller is successful is through SPARK testing, it was found that all procedures and functions implemented passed at a Gold level therefore the system as a whole is Platinum level.

Although, there are several ways in which the controller could be further extended. The front sensor could be further extended to be able to identify even more objects such as traffic lights and road signs. Additional sensors could be placed on the back and sides of the car so that it has even more awareness of its surroundings. Further safety hazards on the road could be accounted for such as changing to four-wheel drive if there is snowy conditions and headlights automatically turning on when visibility is low. Finally, certain flaws within the controller could be amended such as the fact it is assumed the car speed will be set to be below the speed limit when the simulation is run. Right now, there are only preventative measures to ensure the car cannot travel over the speed limit. This could be amended with a procedure that changes the cars speed to be the speed limit anytime it goes beyond it.