AutoCar

Case study title: AutoCar Project

Description

Autonomous cars are automobiles that can move without any human intervention by detecting the car, traffic flow, and its surrounding environment using its own control system. Although the state of autonomous cars is still in its early stages, self-driving technologies are becoming increasingly common. User interaction with the car's system is expected to be minimal, thus there is the assumption that the user has little or no knowledge of the system. For example, the State of California now allows driverless taxi (Robotaxi) services to operate in San Francisco [1], with Cruise being approved to charge for rides in vehicles that will have no human backup driver.

This case study is drawn from the AutoCar Project which aims to add emergency vehicle priority awareness features to autonomous cars. We look at the Software Requirement Specification (SRS) Report intended for software developers, software architects, testers, project managers, and documentation writers. An example of a requirement would be "When an object appears in front of the car, the system shall stop the car until the object is cleared upon which the car will continue to its destination." Current autonomous cars have lane detection and following, object recognition and auto brake, virtual drive assistant, and route planning features. This project seeks to add a fifth feature: emergency vehicle priority awareness. This SRS report includes requirements for all five features. This will allow autonomous cars to detect emergency vehicles as well as their location and direction. A critical assumption in this project is that the system works well when there are no environmental factors, such as bad weather, and that lane markings are distinct. For example, Robotaxis in California are not allowed to operate in heavy rain or fog, and they are currently restricted to being in places and times where there is less traffic and fewer pedestrians on the streets. This system also assumes that all traffic signs and the presence of all objects around the vehicle can be clearly seen - thus the autonomous car is required to have multiple cameras mounted. It also assumes that emergency vehicles, such as ambulances and fire trucks, can be recognized by the autonomous car's voice and image recognition.

The primary assumption in all of this is that the system is operating properly and that there are no abnormal conditions. When the assumptions are not true, the autonomous car's system becomes ineffective and should give the user warning. This project does not fully cover the uncertainties that may occur in the environment that the system has to deal with, but aims to implement the basic external interface requirements, and functional, and non-functional requirements necessary for the emergency vehicle detection feature to be implemented. The natural language rules were developed from the document's use case scenarios for functional requirements.

[1] Driverless taxis are coming to the streets of San Francisco

Stage of Development (Technical contributor)

Design

Expert info

Stakeholder names	Expertise
TS-1	Engineer/Goal Modelling
N-TS-1	Moral Psychology, Law

Normative requirements

1. **Normative requirements in natural language**

   Normative requirements in natural language, in blue the corrected requirements after using N-Tool.

rule id	rule	impact	label(s) (social, legal, ethical, empathetic, or cultural)	stakeholder expertise	authors identifiers
1	When user turns on the system to use the vehicle, the system will turn on the sensors and check components (i.e. tire pressure, engines, and brakes)	+A +S +E +T	Legal	Engineer/Goal Modelling	TS-1
1b	When the user turns on the system and has not turned it off, the system should not turn off its sensors				
1bb	When the user turns off the system, the sensors				

	should turn off eventually				
2	When the system is turned on and ready, it will wait for destination input from user	+A +E +T	Legal	Engineer/Goal Modelling	TS-1
3	When the user gives destination input, it calculates the shortest path to destination and shows route ● Unless it can't find it on GPS, then display error message	+E +T	Legal, Ethical	Engineer/Goal Modelling	TS-1
4	When users requests speed change, then check environment and change speed ● Unless unsafe to do so ● Unless illegal to do so, e.g. the change requested is over the speed limit	+S +E -A	Legal, Ethical, Empathetic	Engineer/Goal Modelling	TS-1 N-TS-1
5	When user changes route with voice order, calculate new shortest path ● Do not stop vehicle while calculating new route ● If new voice order is unclear, ask for clarification	+A	Legal, Empathetic	Engineer/Goal Modelling	TS-1
6	When user withdraws path, park vehicle on shoulder or parking areas - If unsafe to do so, vehicle must not stop until it calculates that it can safely park	+/-A +S	Legal, Ethical, Empathetic	Engineer/Goal Modelling	TS-1 N-TS-1
7	When the car is in	+S	Legal	Engineer/Goal	TS-1

	between two cars in a lane (i.e. front and back), then ensure car is equidistant from both			Modelling	
8	When obstacle appears in front of car, stop until obstacle is cleared, then continue - Unless unsafe to stop then change lanes - If there are no lanes, then turn on hazard lights to alert drivers in the environment that the vehicle is stopping	+S +T +E +SR	Legal, Ethical, Empathetic, Social	Engineer/Goal Modelling	TS-1
9	When driving, stay in the center of lane ● Unless user recommends lane change, then check environment and change lane ● Unless there is no lane, then display warning on dashboard	+S +A +E +T	Legal	Engineer/Goal Modelling	TS-1
10	When the user wants to turn off the system, the car will park automatically in a safe area and then stop the system	+S +A	Legal	Engineer/Goal Modelling	TS-1
11	When there is a priority vehicle alert, display the alert on the dashboard - Alert the user of what the vehicle plans to do (i.e. park on shoulder to allow emergency vehicle to pass)	+S +E +T	Legal, Ethical, Empathetic	Engineer/Goal Modelling	TS-1

12	When there is an emergency vehicle behind the car going in the same direction, then switch to an available lane to clear the emergency vehicle's way ● Unless the emergency vehicle is coming from the left lane or there is only one lane, then try to make emergency corridor or use the shoulder of the road ● Unless it is unsafe for the vehicle to change path in that context	+S	Legal	Engineer/Goal Modelling	TS-1 N-TS-1
13	When there is a traffic light in front of the car with a solid red light, then car will slow down and stop until next signal input from computer vision	+S	Legal	Engineer/Goal Modelling	TS-1
14	When there is a traffic light in front of the car with a solid yellow light, then car will slow down until next signal input from computer vision - Unless the yellow light follows a red light, in which case the vehicle (from a stopping position) should prepare to drive again	+S	Legal	Engineer/Goal Modelling	TS-1
15	When there is a traffic light in front of the car with a solid green light, then car will continue driving	+S	Legal	Engineer/Goal Modelling	TS-1

	● Unless there is an obstacle on the road				
16	When there is a traffic light in front of the car with no lights on or more than one light on (unusual traffic light), then the car will slow down and check its environment carefully with Distance Management, and if environment clear then continue to its destination	+S -T	Legal	Engineer/Goal Modelling	TS-1
17	When doors are still open or safety belt is not worn, do not start driving and notify the user	+S +E +T -A	Legal, Ethical	Engineer/Goal Modelling	TS-1
17b	When the doors are closed and the seat belt is worn and the destination is known and the user has not said yes, then ask if the user is ready to drive				
17b b	When the system is ready and doors are closed and the seat belt is worn and the destination is known but the user has not said yes, then stop the vehicle's autonomous assistance.				
17b bb	When the system is ready and doors are not closed and the seat belt is not worn and the destination is not known and the user has not said yes, then display error on the screen				
17b bbb	When an error is displayed on the screen, then stop the vehicle's				

	autonomous assistance.				
18	When car is turned on and ready to drive (doors closed, seatbelt on, destination ready, system checked), then ask the user for consent to start driving	+S +E +T +A	Legal	Engineer/Goal Modelling	TS-1
19	~~After obtaining consent from the user to start driving, then start driving to destination~~ After asking if the user is ready to drive and the user does not say yes, then stop the vehicle's autonomous assistance.	+A	Legal	Engineer/Goal Modelling	TS-1
19b	After asking if the user is ready to drive and the user does not say yes, then the car should not start driving				
20	When system is on, display information about car on dashboard so the user can see	+E +T	Legal, Empathetic	Engineer/Goal Modelling	TS-1
21	System should take the shortest route available to get the user to their destination ● Unless taking the shortest route would pose danger/health risk to user ● Unless taking the shortest route would require the vehicle to drive illegally	+S	Legal	Psychology Law	N-TS-1
22	System cameras should not record the faces of users, pedestrians, or	+P +A	Legal Ethical	Psychology Law	N-TS-1

	drivers of other cars in its environment - Unless prior informed consent is given by the relevant party				
23	~~System cameras should not record the faces of users, pedestrians, or drivers of other cars in its environment~~ ~~- Unless prior informed consent is given by the relevant party~~	+A +S	Legal	Engineer/Goal Modelling	TS-1
24	When the system is ready and the action is illegal, then the vehicle should change its current driving to be legal	+S	Legal	All stakeholders	All stakeholders
25	When the car is driving and people's consent has not been obtained, the the car should not record people in the environment	+A +P	Legal, Ethical	All stakeholders	All stakeholders
27I-27XII	For all events, if people's consent has not been obtained, the the car should not record people in the environment	+A +P	Legal, Ethical	All stakeholders	All stakeholders
Concerns					
c1	When the system is ready and the user has not consented, or the door is open, or the seatbelt is unbuckled or the destination does not exist, the vehicle must drive				
c2	When the system is ready but the action is legal, the vehicle must not change its current driving state				
c3	When the vehicle recognizes a red traffic light it must not temporarily stop itself				
c4	When the system is ready and the user has not consented, the door is closed, the seatbelt is buckled and the destination exists, the vehicle must not ask if the user is ready to drive				
c5	When asking if the user is ready to drive and the user says no, the vehicle must drive				
c6	When the vehicle is driving and people have not consented to being recorded, the vehicle must				

	record people
c7	When taking user input and the destination does not exist, or a path does not exist, the vehicle must not display an error
c8	When there is a priority vehicle nearby and it is behind the vehicle, and not on the opposite lane, not next to the vehicle, the must not change lanes even when the risk level is low and there are multiple lanes available
c9	When the vehicle is ready to drive then it must become ready to drive eventually
c10	When the user turns on the system then the vehicle must turn off sensors
c11	When the user turns off the system the vehicle must not turn off sensors eventually
c12	When the vehicle is changing speed and consent from people has not been obtained to record them, the vehicle must record people
Purposes	
p1	When the car is driving and risk level is greater than low and the action is legal, the car must take the shortest path
p2	The vehicle must be able to ask if the user is ready to drive while the door is closed, the seatbelt is buckled, and the destination exists
p3	The vehicle must be able to display car information while the system is ready
p4	The vehicle must be able to make space while there is a priority vehicle nearby
p5	The user must be able to change route while the car is driving
6	The user must be able to cancel the path while the car is driving
7	The user must be able to request a speed change while the car is driving
8	The vehicle must be able to drive while a user has requested a lane change
Impact keys: A = autonomy, PH = psychological health (non-maleficence), P = privacy, E = explainability, T = transparency, CS = cultural sensitivity, SR = social requirement, B ‘beneficence’ (doing good), N ‘non-maleficence’ (preventing/avoiding harm), and S ‘safety’. ‘’+” and “-” for positive and negative impacts respectively.	

1. **Rules in the SLEEC DSL**

The stakeholders corrections after analyzing the well-formedness of the rules using our N-Tool are commented and in blue.

```
def_start
  // Events before driving starts
  event UserTurnOnSystem
  event UserTurnOffSystem
  event TurnOnSensors
  event TurnOffSensors
  event CheckSystemComponents
  event SystemReady
  event TakeUserInput
  event CalculateShortestPath
  event ReadyToDrive
  event GetReadyToDrive
  event AskIfUserReadyToDrive
  event DisplayCarInformation
  // Events during driving
  event CarDriving
  event SlowDown                  // But not stop completely
  event TurnOnHazardsAndTemporarilyStop // Different than temporarily stopping just by hazards, i.e. situation is
dangerous and we’re not just temporarily stopping for lights
  event TemporarilyStopCar        // Different than parking, system not turned off
  event ParkVehicle       // On road shoulder or parking area
  // Parking also implies stopping car and turning of system
  event DisplayError      // Error is internal, i.e car systems not properly working
  event DisplayAlert      // Alert is external, includes information
  event DisplayRoute
  event ChangeSpeed
  event ChangeLanes
  event ChangeCurrentDriving
  event TakeNewInput
  event TakeShortestPath
  event MaintainEqualDistance
  event StayCenteredinLane
  event SeeTrafficLight
  event WaitUntilChanges
  event RecordPeople
  // User requests related
  event UserChangeRoute
  event UserCancelPath
  event UserRequestSpeedChange
  event AskForClarification
  // Priority vehicle related
  event PriorityVehicleNearby
  event MakeSpace                 // Such as emergency corridor or use the shoulder

  // Measures before driving starts
  measure destinationExists: boolean
  measure pathExists: boolean
  // Events during driving
  measure objectInPath: boolean            // Sth in front of car, i.e pedestrian, animal, stationary vehicle
  measure carsInFront: boolean    // Moving thing in front
  measure carsBehind: boolean
  measure actionIsLegal: boolean
  //********  Resolve situation 2 (ADD event)
  event StopAutonomousAssistance
  //************************************************************************
```

```
    // Priority vehicle related
    measure userRequestedLaneChange: boolean
    measure ambulanceBehindCar: boolean
    measure ambulanceOnOppositeSide: boolean
    measure ambulanceNextToCar: boolean

    measure environmentClear: boolean    // Other moving vehicles on road, either next to, in front, behind
    measure riskLevel: scale(low, medium, high)
    measure withinLane: boolean
    measure multipleLanes: boolean              // Whether 1 lane or multiple
    measure commandClear: boolean
    measure laneExists: boolean
    measure userTurnedOffSystem: boolean
    measure recognizeInput: boolean
    measure redLight: boolean
    measure yellowLight: boolean
    measure greenLight: boolean
    measure previousLight: scale(red, yellow, green)
    measure doorClosed: boolean
    measure seatBeltOn: boolean
    measure userSaysYes: boolean
    measure peopleConsentObtained: boolean
def_end

rule_start
    R1 when UserTurnOnSystem then TurnOnSensors
    //****** Resolve concern 10 (ADD rule R1b and R1bb)
    // Uncomment R1b and R1bb
    // R1b when UserTurnOnSystem then not  TurnOffSensors
    //R1bb when UserTurnOffSystem then TurnOffSensors eventually
    //*************************************************************************
    //*************************************************************************
    //****  Resolve situation 1 (REFINE existing corrected rule: R1b)
     // comment R1b, and uncomment R1b below.
    //  R1b when UserTurnOnSystem and (not {userTurnedOffSystem}) then not TurnOffSensors
    //*************************************************************************
    R1_cont when TurnOnSensors then CheckSystemComponents
    R2 when SystemReady then TakeUserInput
    R3 when TakeUserInput then CalculateShortestPath
            unless ((not {destinationExists}) or (not {pathExists})) then DisplayError
    R3_cont when CalculateShortestPath then DisplayRoute
    R4 when UserRequestSpeedChange and {environmentClear} then ChangeSpeed
           unless ({riskLevel} > low)
           unless (not {actionIsLegal})

    R5 when UserChangeRoute then CalculateShortestPath
            unless (not {commandClear}) then AskForClarification
            otherwise not ChangeCurrentDriving

    R6 when UserCancelPath then ParkVehicle
            unless ({riskLevel} > low) then WaitUntilChanges
    R7 when CarDriving and ({carsInFront} and {carsBehind}) then MaintainEqualDistance
    R8 when CarDriving and {objectInPath} then TemporarilyStopCar
    unless ({riskLevel} > low) then ChangeLanes
```

```
  unless (not {multipleLanes}) then TurnOnHazardsAndTemporarilyStop
         unless (not {objectInPath}) then CarDriving
  //invalid rules
  R9 when CarDriving and {withinLane} then StayCenteredinLane
         unless ({userRequestedLaneChange} and ({environmentClear} and ({riskLevel} = low)))
         then ChangeLanes
         unless ((not {withinLane}) or (not {laneExists})) then DisplayAlert
  R10 when UserTurnOffSystem then ParkVehicle
  R10_1 when ParkVehicle and {userTurnedOffSystem} then TurnOffSensors
  R11 when PriorityVehicleNearby then DisplayAlert
  R12 when PriorityVehicleNearby and ({ambulanceBehindCar} and (not {ambulanceOnOppositeSide}))
          then ChangeLanes
          unless ({ambulanceNextToCar} or (not {multipleLanes})) then MakeSpace
          unless ({riskLevel} > low)
  R13 when SeeTrafficLight and ({redLight} and {recognizeInput}) then TemporarilyStopCar
          unless (not {redLight}) then TakeNewInput // unless is being used as an ‘until’ here
  R14 when SeeTrafficLight and ({yellowLight} and {recognizeInput}) then SlowDown
          unless (not {yellowLight}) then TakeNewInput
          unless ({previousLight} = red) then GetReadyToDrive
  R15 when SeeTrafficLight and ({greenLight} and {recognizeInput}) then CarDriving
          unless {objectInPath} then WaitUntilChanges
  R16 when SeeTrafficLight and (not {recognizeInput}) then SlowDown
  R16_cont when SlowDown and {environmentClear} then CarDriving
  // Rules 17 and 18 combined
  R17 when SystemReady and (not (({doorClosed} or {seatBeltOn}) or {destinationExists}))
  then DisplayAlert otherwise AskIfUserReadyToDrive
 R19 when AskIfUserReadyToDrive and {userSaysYes} then CarDriving
  //******* Resolving situation 3 (REFINE rule) comment R19 and uncomment R19 below
  R19 when AskIfUserReadyToDrive and (not {userSaysYes}) then StopAutonomousAssistance
  //*************************************************************************
  //**  Resolve concern 1 (ADD rule r17b)
  // R17b when SystemReady and ({doorClosed} and (({seatBeltOn} and  {destinationExists}) and (not
{userSaysYes}))) then AskIfUserReadyToDrive
  //*************************************************************************
  // Resolve concern (ADD 3 rules, 17bb, 17bbb, and 17bbbb,and REFINE r19)
 // Uncomment   17bb, 17bbb, and 17bbbb, r19b, and comment r19
  // R17bb when SystemReady and ({doorClosed} and (({seatBeltOn} and  {destinationExists}) and (not
{userSaysYes}))) then not CarDriving
  // R17bbb when SystemReady and ((not {userSaysYes}) and (((not {doorClosed}) or (not{seatBeltOn})) or (not
{destinationExists})))  then DisplayError
 //  R17bbbb when DisplayError then not CarDriving
 //  R19b when AskIfUserReadyToDrive and (not {userSaysYes}) then not CarDriving
  //*************************************************************************
  //****** Resolve situation 2 (REFINING , previous resolved rule, R17bbbb)
  // comment  R17bbbb and uncomment the rule below.
  // R17bbbb when DisplayError then StopAutonomousAssistance
  //*************************************************************************
  // Resolve situation 4 (REFINE previous solved rule r17bb)
  // comment  R17bb and uncomment the rule below.
  R17bb when SystemReady and ({doorClosed} and (({seatBeltOn} and  {destinationExists}) and (not
{userSaysYes}))) then StopAutonomousAssistance
  //*************************************************************************

  R20 when SystemReady then DisplayCarInformation
  R26 when UserTurnOffSystem then TurnOffSensors eventually
  R21 when CalculateShortestPath then TakeShortestPath
        unless ({riskLevel} > low)
        unless (not {actionIsLegal})
  R22 when SystemReady then not RecordPeople
        unless {peopleConsentObtained}
 R23 when SystemReady then not RecordPeople
      unless {peopleConsentObtained}
  // *** Resolve redundancies  (Delete rule r23 ) ************************
        //Comment R23
   //************************************************************************
  // Resolve concern 2 (ADD rule R24)
  // Uncomment R24
  // R24 when SystemReady and (not {actionIsLegal}) then ChangeCurrentDriving
  //************************************************************************
  //************************************************************************
  // Resolve concern 6 (ADD rule R25)
  // Uncomment R25
  // R25 when CarDriving and (not {peopleConsentObtained}) then not  RecordPeople
  //************************************************************************

  //************************************************************************
  // Resolve concern 12 (ADD rule R27I-R27XII)
  // Add a rule for all car event, to ensure that the recording is consented
  // Uncomment rules R27I to R27XII
  R27I when UserTurnOnSystem and (not {peopleConsentObtained}) then not RecordPeople
  R27II when TurnOnSensors and (not {peopleConsentObtained}) then not RecordPeople
  R27III when SystemReady and (not {peopleConsentObtained}) then not RecordPeople
  R27IV when ReadyToDrive and (not {peopleConsentObtained}) then not RecordPeople
  R27V when AskIfUserReadyToDrive and (not {peopleConsentObtained}) then not RecordPeople
  R27VI when CarDriving and (not {peopleConsentObtained}) then not RecordPeople
  R27VII when SlowDown and (not {peopleConsentObtained}) then not RecordPeople
  R27VIII when ChangeSpeed and (not {peopleConsentObtained}) then not RecordPeople
  R27IX when ChangeLanes and (not {peopleConsentObtained}) then not RecordPeople
  R27X when ChangeCurrentDriving and (not {peopleConsentObtained}) then not RecordPeople
  R27XI when MaintainEqualDistance and (not {peopleConsentObtained}) then not RecordPeople
  R27XII when StayCenteredinLane and (not {peopleConsentObtained}) then not RecordPeople
 /************************************************************************

rule_end

concern_start
  // Safety of the driver and of others in the environment
  c1 when SystemReady and ((not {userSaysYes}) and (((not {doorClosed}) or (not{seatBeltOn})) or (not
{destinationExists}))) then CarDriving
  // Legal - road rules must be followed
  c2 when SystemReady and (not {actionIsLegal}) then not ChangeCurrentDriving
  c3 when SeeTrafficLight and ({redLight} and {recognizeInput}) then not TemporarilyStopCar
  // Autonomy - user must remain in control as much as possible
  c4 when SystemReady  and  ({doorClosed} and (({seatBeltOn} and  {destinationExists}) and (not
{userSaysYes}))) then not AskIfUserReadyToDrive
        c5 when AskIfUserReadyToDrive and (not {userSaysYes}) then CarDriving
  // Privacy - use of cameras attached to car
        c6 when CarDriving and (not {peopleConsentObtained}) then RecordPeople
  // Accuracy - for deciding routes and destinations
  c7 when TakeUserInput and ((not {destinationExists}) or (not {pathExists})) then not DisplayError
  // Emergency vehicle related
  c8 when PriorityVehicleNearby and ({ambulanceBehindCar} and ((not {ambulanceOnOppositeSide}) and ((not {ambulanceNextToCar}) and ( {multipleLanes} and  ({riskLevel}  < medium) )))) then not ChangeLanes
  //autonomy
        c9 when ReadyToDrive then not ReadyToDrive eventually
        c10 when UserTurnOnSystem then TurnOffSensors
        c11 when UserTurnOffSystem then not TurnOffSensors eventually

        //privacy
        c12 when ChangeSpeed and (not {peopleConsentObtained}) then RecordPeople
concern_end

purpose_start
        // Safely transport user from A to B
        P1 exists CarDriving and (({riskLevel} > low) and {actionIsLegal}) while TakeShortestPath
        // Maintain user autonomy
        P2 exists AskIfUserReadyToDrive and (({doorClosed} and {seatBeltOn}) and {destinationExists})
        P3  exists DisplayCarInformation while SystemReady
        // Ensure emergency vehicles are able to carry out their function without unreasonable impediment
        P4  exists MakeSpace while PriorityVehicleNearby
        // Enable user freedom of movement
        P5  exists UserChangeRoute while CarDriving
        P6  exists UserCancelPath while CarDriving
        P7  exists UserRequestSpeedChange while CarDriving
        P8  exists CarDriving and {userRequestedLaneChange}
purpose_end
```