SafeSCAD

Case study title: SafeSCAD: Safe of Shared Control in Autonomous Driving

Description

The Safe-SCAD project developed a proof-of-concept driver attentiveness management system to support safe shared control of autonomous vehicles. This system comprises a deep neural network (DNN) responsible for predicting the driver control-takeover behaviour, methods for verifying this DNN, and a discrete-event controller that issues optical, acoustic and/or haptic driver alerts based on the predictions of the DNN and the results of its online verification. Sensors for detecting the state of the human driver include an eye-tracking camera, and wearable sensors to measure the driver's heart rate (PPG) and galvanic skin response (GSR) signals.

Taking this beyond the initial project though it can be observed how SafeSCAD can benefit from utilising SLEEC requirements. The safety of the passengers and those around the car is paramount, and laws are in place to ensure this safety. Thus the controller of this autonomous system needs to be legally compliant, and identify when it can no longer be legally safe. For simplicity this can be initially thought of as when the system does not have sufficient control, or can accurately predict future states. It is at this instance that the system will need to alert the user of the switch over. This of course would not cover all legal nuances of driving, and a full set of legal requirements will need to be drafted. Further, these legal requirements will need to be in a manner that can be understood by the system. Providing cues that will accurately convey the specific situation's concerns, and magnitude of said concern, is vital and would be encapsulated by the SLEEC requirements.

Further, to ensure a successful takeover from the human driver when prompted the human must be attentive. The controller was assumed to have a light source, speakers, and be able to haptically interact with the driver (vibrations in seat/steering wheel for example). This allows the car to alert the human driver whenever the driver is observed to be less attentive. DeepDECs is employed to generate pareto optimal controllers utilising the different objective tradeoffs; risk due to attentiveness level, and nuisance caused by the alerts.

Stage of Development (Technical contributor)

PROOF-OF-CONCEPT

Expert info

Expertise of the stakeholders involved in devising the SLEEC rules
Number of stakeholders writing the rules

Stakeholder names	Expertise
TS-1	Safety analyst
N-TS-1	Psychology/Ethics
N-TS-2	Moral Psychology, Law
TS-2	Engineer/Goal Modelling

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	~~Ensure that the user maintains a certain level of alertness while driving.~~ ~~- Identify the user heart rate variability and eye movements to identify any signals of drowsiness.~~ ~~- If drowsiness is detected, interact with the user~~ ~~(Ensure that user maintains a certain level of alertness while driving.~~ ~~- Identify the user heart rate variability and eye movements to identify any signals of drowsiness.~~ ~~If drowsiness is detected, interact with the user)~~	PH+ S+ N+	Social Legal	Psychology Ethics	N-TS-1
2	Ensure that the user level of alertness varies with the demands of the driving task. - Identify the user heart rate	PH+ S+ N+	Social Legal	Psychology Ethics	N-TS-1

	variability and eye movements to identify any signals of drowsiness. - If drowsiness is detected, ~~interact with the user~~ alert the user - If user encounters a situation that requires further attention (e.g., multiple vehicles, overtaking vehicles), ensure his body reacts appropriately (e.g., higher heart rate, lower heart rate variability, increased galvanic skin response) by alerting them ~~interacting with them, if needed~~				
3	If any of the sensors are not properly placed, inform the user as soon as possible ~~(before they start driving)~~ that they should fix it (e.g., decrease impedance of heart rate monitor)	PH+ S+ N+	Social Legal	Psychology Ethics	N-TS-1
4	Avoid communicating unnecessary information while the user is driving to avoid distractions. - Unless the information is important, sensors are not properly placed, or the user has become impaired, or there is an object nearby (relevant or not), or a blind spot	PH+ S+ N+	Social Legal	Psychology Ethics	N-TS-1
5	Determine what information is necessary to ensure user safety.	S+ N+	Social Legal	Psychology Ethics Engineer/Goal Modelling	N-TS-1 TS-2
6	If baseline information from sensors is too different from usual (e.g., heart rate higher or lower than the expected for that user), confirm with the user if they are feeling good enough to drive.	PH+ S+ N+	Social Legal	Psychology Ethics	N-TS-1
7	If user has to take the vehicle over, ensure that they are physically and mentally able to drive. - Ensure that their current health condition allows them to control the vehicle - Ensure that they are allowed to drive (e.g., they should have a	PH+ S+ N+	Social Legal	Psychology Ethics	N-TS-1

	valid driver's license) - Ensure that they are not under the effect of substances				
7_1-7_2	When the user wants to take control of the vehicle and their current health condition does not allow them to control the vehicle, they are not allowed to drive (e.g., they do not have a valid driver's license), or they are under the effect of substances, then do not allow the user to drive and the system should take over instead.				
8	As soon as a user enters the vehicle for the first time, ensure that they consent to driving the vehicle if needed. - Ensure the user speaks and understands the language. - Ensure the user understands what is being requested of them.	PH+ S+ N+	Social Legal	Psychology Ethics	N-TS-1
9	If user is not following local driving rules: - Remind them about the rule in the first few times they should behave according to the rule - If they continue to forget about the rule, continue reminding them each time they should do it - If user learned to drive in a city other than the one they are currently driving, inform them of any specific rules or norms that might be in place in that location.	PH+ S+ N+	Social Legal	Psychology Ethics	N-TS-1
10	If a relevant stimulus is nearby but the user does not seem to notice it (e.g., a person crossing the street), inform the user that they should be alert to that specific stimulus.	PH+ S+ N+	Social Legal	Psychology Ethics	N-TS-1
11	Track their field of vision with the eye tracker and make sure all relevant stimuli are in their field of vision. - ~~Alert user about any potential blind spots.~~ - If there are objects in their blindspots, inform the user (important information)	PH+ S+ N+	Social Legal	Psychology Ethics Engineer/Goal Modelling	N-TS-1 TS-2

12	~~If use of system impacts user and manufacturer's legal liability in the case of accident, ensure that the user is aware of and explicitly consents to potential liability allocated to the user~~ Ensure that the user is aware of and explicitly consents to potential liability allocated to the user, and if the user does not consent, then stop the autonomous component of the car.	+N +SR +S	Social Legal Ethical	Psychology Law	N-TS-2
13	In the first interaction with the user, show consent form which outlines most common accidents and most common responsibility attributions based on past data - If use of system impacts user and manufacturer's legal liability in the case of accident ensure that the user is aware of and explicitly consents to potential liability allocated to the user	+S	Legal Ethical	Psychology Ethics Engineer/Goal Modelling	N-TS-1 TS-2
14	If user's visual, auditory, or bodily abilities require specific accommodation, ensure that alerts (visual, auditory, or haptic) are adequately accessible and understandable to the user - Allow user to choose from a variety of options the settings that best suit the user's unique needs - System must not disenfranchise certain users over others from the full benefits of the system by virtue of their visible or invisible disabilities	+S +SR +A	Social Legal Empathetic Ethical	Psychology Law	N-TS-2
15	All alerts designed ought to be independently noticeable and sufficiently different from each other such that the user can a) notice them and b) not confuse their meanings	+S +T +N	Legal Social Empathetic	Psychology Law	N-TS-2
16	If driver is sensed to have become incapacitated in some way, system ought to provide user with a warning that system will take control and steer vehicle to safety quickly, then proceed to do so - Unless user explicitly turns off	+S +B +N	Legal Social	Psychology Law	N-TS-2

	warning signal, indicating that an emergency stop is not needed				
17	If system notices an upcoming high-stakes decision point, system ought to immediately yield control to the user/driver - Unless user explicitly re-yields control to the vehicle/system	+S +N +T	Legal Social	Psychology Law	N-TS-2
18	Allow user to quickly and easily turn off system use and data collection when desired - User ought to always have the option to opt out of system use/monitoring	+P +T +SR +A	Legal Social Ethical	Psychology Law	N-TS-2
19	When the system is driving and the sensors are not properly placed, then stop unfunctioning sensor assistance				
20	When the system is driving and the feature consent is removed, then stop unfunctioning sensor assistance				
Concern					
1	When the system is driving and the sensors are not properly placed, then stop the unfunctioning sensor assistance				
2	When the system is driving and the feature consent has been removed, then stop the unfunctioning sensor assistance				
3	~~The user can drive when the heart rate variability or eye movements are low~~				
4	The user can drive after having consent and while under substance use				
Purpose					
1	The system must be able to inform the user of things				
2	The system must be able to remind the user of things				
3	The system must be able to take control of the vehicle for safety				
4	When the user is driving and heart rate variability is low or eye movements are low, the system must be able to inform the user of this				
5	When the user enters the car for the first time and has already given consent, the system must not show the user the consent form				
6	When the system has informed the user of the rules, and the user is now following the rules, then				

	the system must not remind the user within 10 minutes.

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.

2. **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
    event InformUser
    // resolve situational conflict add EVENT ********
    event Alert
    event RemindUser
    // event GiveInformation - used to be in rule 4, now replaced with inform user
    event FindInformation
    event DetermineImportance
    event UserDriving
    event UserWantsControl
    event UserEnters
    event UserCanTurnOffSystem
    event UserCanTurnOffMonitoring
    event PreparingSystem
    event SystemDriving
    event SystemOn
    event EnsureAlertness
    event EnsureAccessibility
    event EnsureAlertIndependence
    event TrackMetrics
    event SensorsConnect
    event BaselineDiffers
    event ConfirmWithUser
    event ObtainConsentForUserDrive
    event TrackVisionField
    event ShowConsentForm
    event CreateConsentForm
    event TakeControlForSafety
    // resolve purpose 1 ADD EVENT ****
    event FirstInteractionUser
    // resolve situation 8 ADD EVENT ****
    event StopAutonomousComponent
    // resolve concern 1
    event StopUnfunctioningSensorAssistance
    // resolve concern c4:
    event SytemTakesOver

        measure hearRateVariability: scale(low, medium, high)
```

```
        measure eyeMovements: scale(low1, medium1, high1)
        measure fullAttentionNeeded: boolean
        measure properlyPlaced: boolean
        measure informationImportant: boolean
        measure health: boolean
        measure hasLicense: boolean
        measure substanceUse: boolean
        measure commonLanguage: boolean
        measure userUnderstands: boolean
        measure sameCity: boolean
        measure rulesFollowed: boolean
        // RESOLVE SITUATION ADD measure
        measure relevantObjectNearby: boolean
        measure objectNearby: boolean
        measure userNotice: boolean
        measure blindSpot: boolean
        measure obtainConsent: boolean
        // RESOLVE CONCERN c2 add measure
        measure removeFeatureConsent: boolean
        measure needsAccomodation: boolean
        measure userImpaired: boolean
        measure warningSignalOff: boolean
        measure userGivesControl: boolean
        measure decisionPoint: boolean
def_end

rule_start


R1 when UserDriving then EnsureAlertness

 R1_1 when EnsureAlertness then TrackMetrics

 // Drowsiness detected
 R1_2 when TrackMetrics and (({hearRateVariability} = low) and ({eyeMovements} = low)) then InformUser

 // *** Resolve redundancy: comment (MERGE, R1 - R1_1- R1_2 (move to r2))
 // Comment R1 - R1_1- R1_2
 //*****************************************************************************************

 R2 when UserDriving and {fullAttentionNeeded} then EnsureAlertness

 R2_1 when EnsureAlertness then TrackMetrics

 R2_2 when TrackMetrics and (({hearRateVariability} = low) and ({eyeMovements} = low)) then InformUser

 //***** Resolve situational conflict, (REFINE rule + ADD event)
 // Comment R2_2, uncomment with R2_2b
 //R2_2B when TrackMetrics and (({hearRateVariability} = low) and ({eyeMovements} = low)) then Alert
 //*****************************************************************************************

  R3 when SensorsConnect and (not {properlyPlaced}) then InformUser
  R3_1 when SensorsConnect and (not {properlyPlaced}) then not UserDriving
```

```
 //********** Resolve situation 2, (DELETE a rule)
 // Comment R3_1
//*******************************************************************************************

 R4 when UserDriving then not InformUser
     unless {informationImportant}


// ***Resolve situation 3 (REFINE)
// Comment R4, uncomment R4b
// R4b when UserDriving then not InformUser
//       unless ({informationImportant} or (not {properlyPlaced}))
//*******************************************************************************************
// *** Resolve situation 4 (REFINE resolved rule)
// Comment R4b, uncomment R4b2
//R4b2 when UserDriving then not InformUser
//         unless ({informationImportant} or ((not {properlyPlaced}) or {userImpaired}))
//*******************************************************************************************
// *** Resolve situation 6 (REFINE resolved rule)
// Comment R4b2, uncomment R4b3
//R4b3 when UserDriving then not InformUser
//    unless ({informationImportant} or ((not {properlyPlaced}) or ({userImpaired} or {relevantObjectNearby})))
//*******************************************************************************************
// *** Resolve situation 7 (REFINE resolved rule)
// Comment R4b3, uncomment R4b4
// R4b4 when UserDriving then not InformUser
//         unless ({informationImportant} or ((not {properlyPlaced}) or ({userImpaired}
//         or ({relevantObjectNearby} or ({blindSpot} and {objectNearby}))))
//*******************************************************************************************

R5 when FindInformation then DetermineImportance

R6 when BaselineDiffers then ConfirmWithUser

R7 when UserWantsControl and (({health} and {hasLicense}) and (not {substanceUse}))
     then UserDriving

//***** Resolving while concern c4 (add two rules)
//** Uncomment R7_1 and R7_2
//R7_1 when UserWantsControl and ((((not {health}) or (not {hasLicense})) or {substanceUse}) and {obtainConsent})
//         then not UserDriving
//R7_2 when UserWantsControl and ((((not {health}) or (not {hasLicense})) or {substanceUse}) and {obtainConsent})
then SytemTakesOver
//*******************************************************************************************

R8 when UserEnters and ({commonLanguage} and {userUnderstands})
    then ObtainConsentForUserDrive

R9 when UserEnters and (not {sameCity}) then InformUser

R9_1 when InformUser then RemindUser within 10 minutes

R9_2 when InformUser and (not {rulesFollowed}) then RemindUser
```

```
//***  Resolve situation 5 ** (DELETE, merged with R9_2)
// Comment R9
//*****************************************************************************

//*** Resolve purpose 2, refine existing rule (MERGE)
// Comment R9_1
//*****************************************************************************

R10 when UserDriving and ({objectNearby} and (not {userNotice})) then InformUser

//***** Resolve SITUATION 7 (Refine R10 + add measure)
// Comment R10 and uncomment R10b
// R10b when UserDriving and ({relevantObjectNearby} and (not {userNotice})) then InformUser
//*****************************************************************************
R11 when UserDriving then TrackVisionField
R11_1 when TrackVisionField and {blindSpot} then InformUser

//** Resolve purpose 2, refine existing rule (REFINE R11_1)
// Comment R11_1 and uncomment R11_1b
//R11_1b when TrackVisionField and ({blindSpot} and {objectNearby}) then InformUser
//*****************************************************************************

R12 when UserEnters then ShowConsentForm
//************ Resolve purpose 1 (DELETE R12 + add event + add rule)
// Comment R12
//*****************************************************************************



R12_1 when ShowConsentForm and (not {obtainConsent}) then not UserDriving

//**** Resolve situation 8  (REFINE)
// Comment R12_1, and uncomment R12_1b
// R12_1b when ShowConsentForm and (not {obtainConsent}) then StopAutonomousComponent
//*****************************************************************************


R13 when PreparingSystem then CreateConsentForm

//**** Resolve purpose 1  (ADD a rule + event)
// Uncomment R13b
//R13b when FirstInteractionUser then ShowConsentForm
//*****************************************************************************

 R14 when UserEnters and {needsAccomodation} then EnsureAccessibility

 R15 when PreparingSystem then EnsureAlertIndependence

 R16 when UserDriving and {userImpaired} then InformUser

 R16_1 when UserDriving and {userImpaired} then TakeControlForSafety
         unless {warningSignalOff}
```

```
 R17 when SystemDriving and {decisionPoint} then UserDriving
       unless {userGivesControl}

 R18 when SystemOn then UserCanTurnOffSystem

 R18_1 when SystemOn then UserCanTurnOffMonitoring

 //***** Resolve concern 1  (ADD event + add a rule R19)
 // Uncomment R19
 // R19 when SystemDriving and  (not {properlyPlaced}) then StopUnfunctioningSensorAssistance
 //*****************************************************************************************

 // ***** Resolve Concern c3  (ADD one rule)
 // Uncomment R20
 // R20 when SystemDriving and {removeFeatureConsent} then StopUnfunctioningSensorAssistance
 //*****************************************************************************************

rule_end

concern_start
   c1 when SystemDriving and  (not {properlyPlaced}) then not StopUnfunctioningSensorAssistance
   c2 when SystemDriving and {removeFeatureConsent}  then not StopUnfunctioningSensorAssistance
   //c3 exists UserDriving and (({hearRateVariability} = low) and ({eyeMovements} = low))
   c4 exists UserDriving and ({substanceUse} and {obtainConsent})
concern_end

purpose_start
   p1 exists InformUser
   p2 exists RemindUser
   // event GiveInformation - used to be in rule 4, now replaced with inform user
   p3 exists TakeControlForSafety
   p4 when UserDriving and (({hearRateVariability} = low) and ({eyeMovements} = low))  then  InformUser
   p5 when UserEnters and {obtainConsent} then not ShowConsentForm
   p6 when InformUser and  {rulesFollowed} then not RemindUser within 10 minutes
purpose_end
```