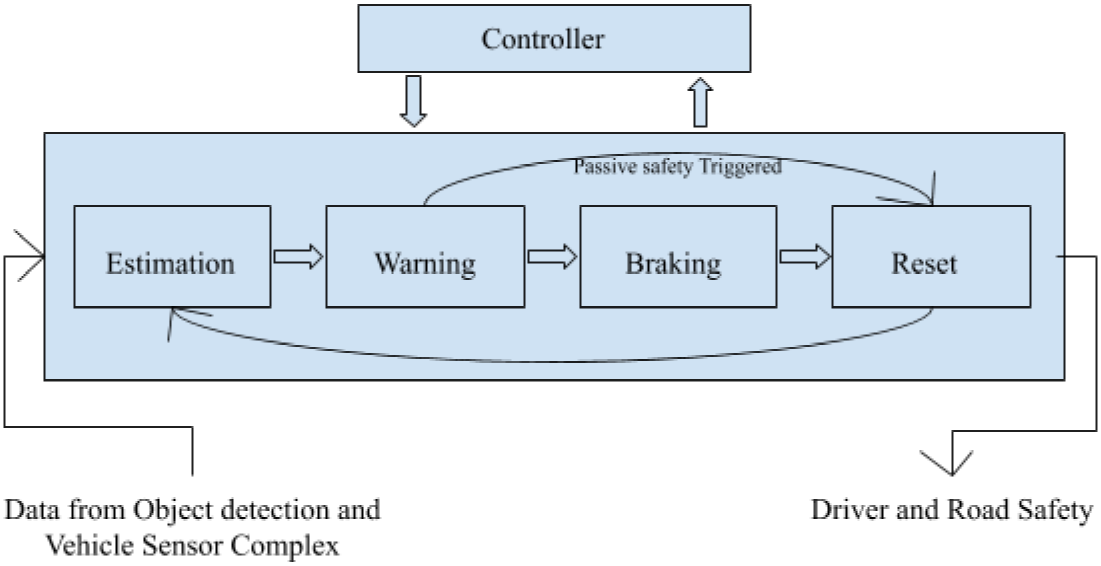
Assignment Security and Quality
Application of the System-Theoretic Process Analysis for Security (STPA-Sec)

Name	Personal Number	Mail
Denim Deshmukh	980401-6450	dede19@student.bth.se
Sai Pranav Koyyada	990429-9311	saky19@student.bth.se

1. Define and frame security problem

A system to do forward collision avoidance by the means of multiple controllers to detect, analyse, warn and override vehicle control in order to contribute to driver and road safety.

2. Abstract Functional



3. Losses, Hazards, Constraints and Assumptions

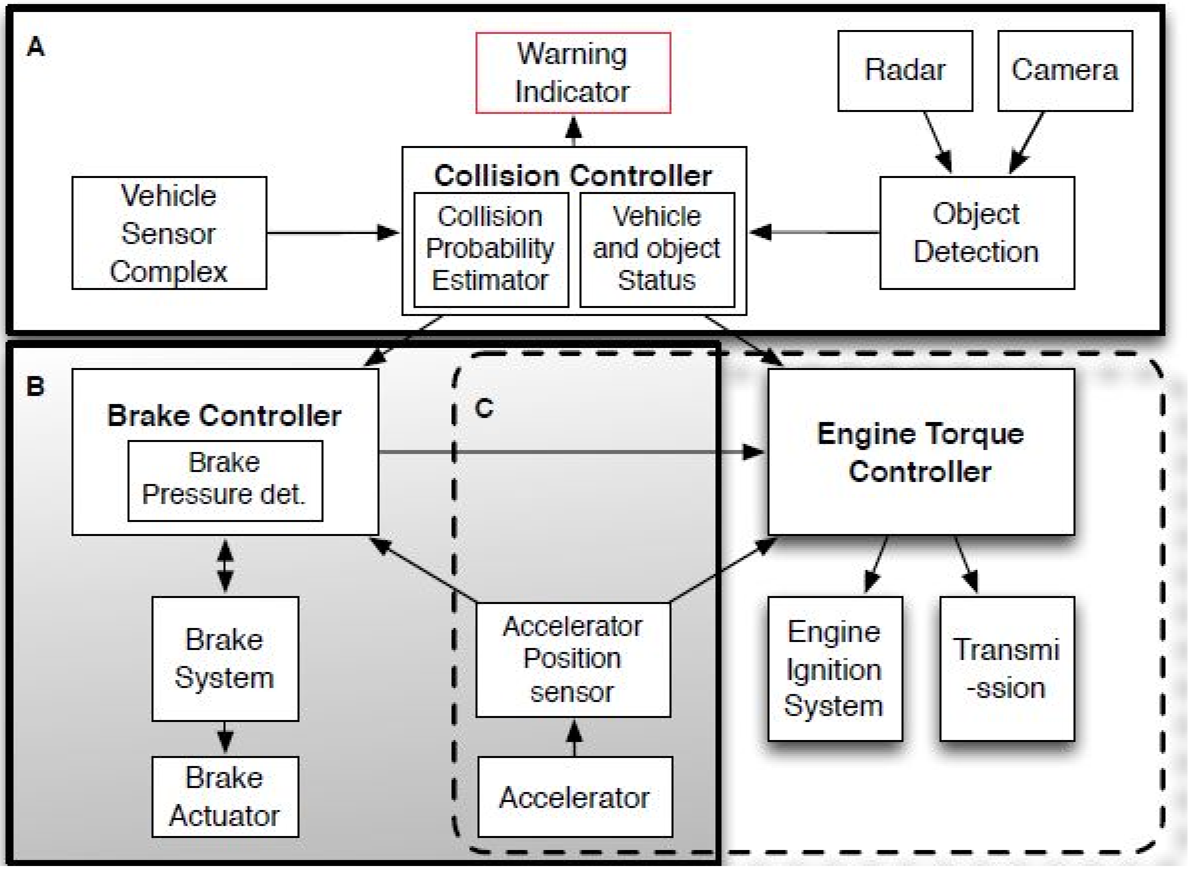
L1: Road injuries and deaths.
L2: Vehicle and property damages.

H1: Failure in triggering estimations/warning/breaking.
H2: Death or injury to Driver caused by shock of abrupt braking.
H3: Incompetence to react if the required breaking time to avoid collision is critical in comparison to passing warning for passive safety.
H4: Automated breaking is not overridden by human intervention.

C1: Complete system check must be performed to validate engine start.
C2: Inversely apply braking pressure against existing torque of the vehicle for even slow down.
C3: Decision support to triggered autonomous braking over passive safety in critical state.
C4: Override Automated braking on human intervention

A1: Every vehicle is equipped with a forward collision avoidance system to counter abrupt braking of the vehicle ahead.

4. Component Structure



A - Collision Controller : Triggers Collision warning signal through the connected Warning indicator as a response to collision assessment evaluated using the inputs from Object Detection System and Vehicle Sensor Complex. If passive safety fails, send vehicle status signal, detected-object status signal and collision-assessment signal to brake controller and Engine Torque Controller.

B - Brake Controller : Determine brake pressure via the signals from the collision controller and accelerator position sensor signal from accelerator. Trigger active safety and override it provided human action intervenes. Send status signal to Engine Torque Controller.

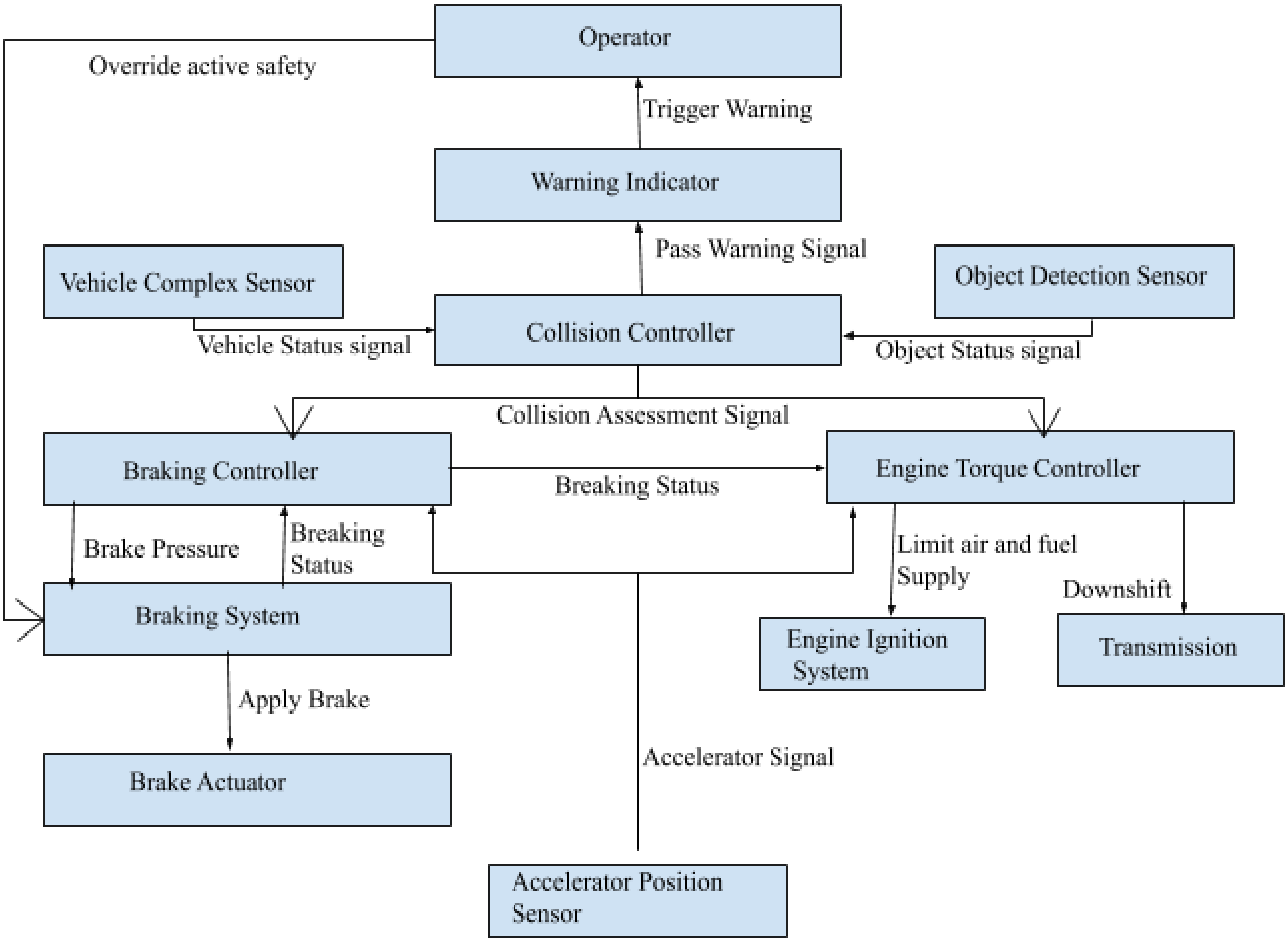
C - Engine Torque Controller : Reduce torque to zero post receiving signals from Collision Controller and Brake Controller during the application of active safety based on the accelerator position sensor signal from accelerator.

5. Control Structure

High-Level Functional Activity	Model Elements
Warn	Object detection sensor, Vehicle Complex Sensor,Collision Controller, Warning Indicator
Break	Collision Controller, Brake Controller, Brake System, Brake Actuator, Accelerator Position Sensor, Engine Torque Controller, Engine Ignition System, Transmission

Elements	Responsibility Description
Warning Indicator	- Trigger warning signal.
Object Detection Sensor	- Send object status to Collision Controller.
Vehicle Complex Sensor	- Send vehicle status to Collision Controller.
Collision Controller	- Collision assessment - Pass warning signal.

	- Send vehicle status signal, detected-object status signal and collision-assessment signal to Brake Controller and Engine Torque Controller.
Brake Controller	- Determine and pass brake pressure to Brake System. - Send status signal to Engine Torque Controller.
Brake System	- Communicate signals between Brake Actuator and Brake Controller. - Override operator active safety on Operator intervention.
Brake Actuator	- Apply Brake.
Accelerator Position Sensor	- Determine Accelerator position.
Engine Torque Controller	- Reduce Torque to zero.
Engine Ignition System	- Limit air and fuel supply based on signals from Engine Torque Controller.
Transmission	- DownShift transmission based on signals from Engine Torque Controller.



6. Hazardous (unsafe/unsecure) control actions

Control Action	A control action required is not provided	An unsafe (incorrect) control action is provided	A control action is provided too early or too late		A control action is stopped too early or applied too late
			Too Early	Too Late	
CA1: Override active safety	Active safety will save from collision. (1a)	Active safety will save from collision.(1a)	-	Active safety will save from collision.(1a)	-
CA2: Trigger warning	Active safety will save from collision.(1b)	Active safety will save from collision.(1b)	-	Active safety will save from collision.(1b)	-

CA3: Pass warning signal	Active safety will save from collision.(1c)	Active safety will save from collision.(1c)	-	Active safety will save from collision.(1c)	-
CA4: Vehicle status signal	Brake pressure determination fails.(2a)	Brake pressure determination fails.(2a)	-	Brake pressure determination fails.(2a)	-
CA5: Object status signal	Brake pressure determination fails.(2b)	Brake pressure determination fails.(2b)	-	Brake pressure determination fails.(2b)	-
CA6: Collision assessment signal	Complete Collision avoidance system fails.(3a)	Complete Collision avoidance system fails.(3a)	-	Complete Collision avoidance system fails.(3a)	-
CA7: Brake Status signal	Torque reduction fails. Chances of collision and vehicle damage.(4a)	Torque reduction fails. Chances of collision and vehicle damage. (4a)	-	Delayed Torque reduction. Injury to operator caused by braking shock.(4a)	-
CA8: Break Pressure	Complete Collision avoidance system fails. (3b)	Complete Collision avoidance system fails. (3b)	-	Complete Collision avoidance system fails. (3b)	-
CA9: Apply Brake	Complete Collision avoidance system fails.(3c)	Complete Collision avoidance system fails. (3c)	-	Delayed Braking. Injury to operator due to minimal collision.(3c-1)	-
CA10: Accelerator Signal	Wrong Brake pressure determination. Leads to collision. (5a)	Wrong Brake pressure determination. Leads to collision. (5a)	-	Wrong Brake pressure determination. Leads to collision.(5a)	-
CA11: Limit air and fuel supply	Torque reduction fails. Chances of collision and vehicle damage. (4b)	Torque reduction fails. Chances of collision and vehicle damage. (4b)	-	Delayed Torque reduction. Injury to the operator caused by braking shock. (4b-1)	-

CA12: Downshift	Torque reduction fails. Chances of collision and vehicle damage. (4c)	Torque reduction fails. Chances of collision and vehicle damage. (4c)	-	Delayed Torque reduction. Injury to the operator caused by braking shock. (4c-1)	-

7. Scenarios

No.	Hazard	Severity	Factors
1a	Operator is unable to override vehicle control. The system will avoid collision providing active safety is functioning correctly.	Negligible	- Brake pedal sensor failure - Communication error - Delayed Communication
1b	The system will avoid collision providing active safety is functioning correctly if the warning signal is not passed to the warning indicator	Negligible	- Faulty Warning Indicator - Communication error
1c	The system will avoid collision providing active safety is functioning correctly if the warning indicator doesn't or make a delayed signal to the user	Negligible	- Faulty Warning Indicator - Communication error
2a	If the vehicle status is not passed to the brake controller, it fails to determine the right pressure to be applied to avoid collision.	Catastrophic	- Vehicle complex sensor failure - Communication error
2b	If the object status is not passed to the brake controller, it fails to determine the right pressure to be applied to avoid collision.	Catastrophic	- Object Detection sensor failure - Communication error
3a	Delayed or absence of the collision assessment signal will fail to trigger Brake controller and Engine Torque controller leading to failure of the complete system.	Catastrophic	- Inappropriate or inadequate collision assessment algorithm. - Inadequate parameters. - Object Detection sensor failure. - Vehicle complex sensor failure - Communication error - Delayed Communication error
3b	Insufficient break pressure will lead to collision	Catastrophic	- Accelerator sensor failure - Inappropriate or inadequate collision assessment algorithm.

			- Inadequate parameters. - Object Detection sensor failure. - Vehicle complex sensor failure - Communication error - Delayed Communication
3c	No application of brake will lead to collision	Catastrophic	- Brake controller components failure - Communication Error - Delayed communication
3c-1	Delayed application of brakes will lead to collision although the damage done might be lower	Moderate	- Brake controller components failure - Communication error - Delayed communication
4a	Absence or Delayed brake status signal can cause failure in torque reduction during active safety has high potential to flip or spin the vehicle of the road.	Catastrophic	- Engine torque controller components failure - Communication error - Delayed communication
4b	The torque of the engine is not reduced if the air and fuel supply are not lowered hence will keep the vehicle moving with same speed while in active safety. This may lead to the vehicle getting flipped or spinning on the road.	Catastrophic	- Engine torque controller components failure - Communication error - Delayed communication
4b-1	The torque of the engine is reduced unevenly with respect to breaking due to delayed lowering of air and fuel supply. This may lead to injuries to the operator due to abrupt braking shock.	Moderate	- Engine torque controller components failure - Communication error - Delayed communication
4c	The torque of the engine is not reduced if the transmission is not shifted down hence will keep the vehicle moving with same speed while in active safety. This may lead to the vehicle getting flipped or spinning on the road.	Catastrophic	- Engine torque controller components failure - Communication error - Delayed communication
4c-1	The torque of the engine is reduced unevenly with respect to breaking due to delayed transmission downshifting. This may lead to injuries to the operator due to abrupt braking shock.	Moderate	- Engine torque controller components failure - Communication error - Delayed communication

8. New Constraints and features

C5 : Equip vehicles with secondary damage reduction systems calibrated with Forward Collision avoidance systems.
C6: Adopt synchronized multi way communication to avoid system failures.
C7: Continuous assessment and updation of situation to alter and apply critical parameters to avoid or minimise the damage of collision.

F1: Equip vehicles with Airbags calibrated with Forward Collision avoidance systems to respond to inappropriate functioning.
F2: Equip vehicles with synchronized multiple communication methods to interact with various components of the system.
F3: Collision controller must analyse and evaluate the real time scenario in brief intervals post triggering active safety to change critical parameters like acceleration position and braking pressure to avoid or minimise the damage of collision.

9. Personal reflection on the application of STPA-Sec

With STPA-Sec emphasis on system theory, visualisation and analysis of the defined complex systems is rationalized and channelised with progressive and detailed decomposition of individual components and their actions.

The constructive step by step approach simplifies the hazard analysis of dynamic systems. Although translation of physical layout to control structure demands deep understanding and practice of the domain and working of the system. Defining a security problem and identifying losses, hazards and constraints is considerably easy even with early understanding of the system.

STPA-Sec facilitates to understand the criticality of controls and functions of the system allowing to define secure counter measures to mitigate hazardous scenarios early in the development thus reducing the late breakages and cost to fix them in addition to improved effectiveness.

STPA-Sec will be a crucial segment of development for any major software project or assignment involving dynamic systems undertaken by me in the future to deliver impact.