CHAPTER 5

CONCLUSION AND FUTURE ENHANCEMENT

The research work on safety enhancement of automotive software for passenger cars aims to propose new enhanced safety software models based on the analysis of the existing safety models as per the standards. The various issues originating through hazardous environment, lazy actions of the human driver and the unexpected behaviour of the software system are considered in the designing of a safe design model for automotive functional safety and integrated safety. The limitations of the current safe design models are their poor abstraction and application due to heterogeneity in the design of various brands and models of automotive. The safety challenges are in the deployment of multi-functional software developed for these models and unpredictable environmental conditions. Even an experienced human user or remote driver may perform some quick actions for which the unexpected reactions would be really dangerous. The context action reaction based advanced safety logic can be used for codifying suitable safety instructions in the electronic control units or microcontrollers. In the future work, the driving patterns of different categories of users and the predictable traffic data will be included in the architectural model in order to give not only an action driven functional safety but also the system’s reaction driven public safety.

A safety assessment model for any distributed software application is proposed as an In-Safe model and designed as a cluster of interacting distributed software components with traceability. The advanced safety challenges in the automotive software are the composability of the distributed design components through safety assessment documents. System safety can be thought of an integrated outcome of the different types of proposed design
components as in-presence or in-absence or in-connection nature to minimize the transformation of an incident into an accident. The traceability of the fully assembled or partially assembled design software components after executing the software modules is derived as forwards encoded traceability and reverse encoded traceability in a real time software environment as a platform. The needed platform and the infrastructure components are assumed to be available on the test bed, the needed database for the testing component specifications are assumed to be stored in the multiple data dictionaries. Traffic and regulation policies are incorporated to determine the safety of the platform and system to be tested as a composition of three categories of software components as In-absence, In-connection and influence categories. This phase of the research work proposed a suitable computational logic as a safety assessment with a set of decision rules and implemented in the model. These safety assessment rules for software systems can be listed as a set of D-SAR primitives with their computational combinations as advanced safety policies. Safety assessment is done in the domain of automotive systems by checking the critical properties in the various subsystems or assemblies as satisfaction property, fairness property and reachability property.

Safety Assessment is done for accomplish of an integrated safety for automotive software by evaluating the safety of automotive software system as the product of the individual integrity level of the components and the operational safety methods incorporated in the vehicle design. All the safety assessment documents are collected from different development centers and composed to determine the overall safety of the system. These safety documents are designed to be portable and at the same time the information and the data have to be extracted by the demanding computing node for further processing. The document model and the contents in a standard template had been designed such that the same document can be reused for successive nodes with suitable modifications. The Safety Assessment Document (SAD) carries the important field as safety goal at that instant of
processing and the method with which the goal is achieved. The quantitative and qualitative safety assessments are made for any automotive system with distributive, categorical and dynamic collection of safety documents for three subsystems like AIRBAG subsystem, Antilock braking subsystem and Parking assistance subsystems. The respective safety standards and compliance acts had been cross checked and compared during the document verification phases. As the result of the said work, it was identified that with respect to the influence monitoring component say airbag, the relation between vehicle speed in kilo metre per hour and airbag release time in millisecond were observed where he airbag release time is linearly varying till the vehicle speed reaches 70 kilo metre per hour and then after 70kmph, the release time for the airbag for deployment was found faster which is the expected post-accidental safety. At the same time, with respect to the In-connection monitoring component for ABS subsystem, the relation between speed limit of ABS in km/h and ABS subsystem controlled in seconds was studied. The speed limit of ABS subsystem was found to be constant till 90kmph in the experimental studies and when the vehicle speed reaches 115kmph, the ABS responds quicker than the earlier stages which is safer. Similarly with respect to the In-absence monitoring component, say parking subsystem, the relation between parking speed in kmph and distance between the obstacle and vehicles before collision was measured in centimeters. In this advanced safety scenario, the distance between the obstacle and the vehicle was safe till it reached 130cm thereafter when speed increased, the parking lighting subsystem indicated the unsafe condition.

The advanced safety of the automotive software for passenger car had been considered along with the traceability of the individual software components for detecting any safety mismatch. The traceability of software component, say in the influence category as air bag subsystem, is calculated in a time domain as equal to the sum of intelligent airbag triggering time and time to inflate completely and time for dynamic inflation of the driver for the
airbag which is found to be less than 40ms. Similarly, the traceability of the ABS software subsystem as an in-connection category module is equal to the sum of in-connection ABS embedded component and the time out of speed limit of vehicle was found to be less than 30kmph and then the ABS control unit was applied. Traceability of the software module for parking sub system as an in-absence category was determined for various distances between the car and the obstacles. The result showed that when the distance of the obstacles was at a distance of 150cm, green LED glows with a beep sound and when obstacles were at distance of 30cm, all green, yellow and red LED light glowed with a beep sound. The automotive system safety is studied as a simulation using a standard tool RENO, and the safety specifications are included in the tool dictionary module. The serious limitations of the above safety model are the lack of performance assessment in terms of fuel, intertwined processes and time. A multicore programming model is very essential in solving the issues related to the parallel processing of all the data and safety documents on the fly. The optimized safety model for an automotive system with distributed components were studied with traceability. The safety requirements are transcripts which are fed into the service components with standard interfaces in the behavior of software modules of the safe design. In the reverse expected safety with traceability, the design models or modified code segments were translated into safety requirements. The challenges in the advanced safety assessment of an automotive system with distributed design models were seen as due to heterogeneous requirements in terms of system overall fuel efficiency, subsystem minimum carbon emission rate, expense of optimal electrical power for the air conditioner and infotainment, the aperiodic battery recharging, accurate tracking using GPS, in appropriate VANET interfaces. These limitations were also extended due to various types of the vehicles and their manufacturers and the system make of the year, along with the country’s dynamic driving rules and parking regulations.
An enhanced safety model for the automotive software system has been proposed with focus on the features like collision avoidance, crash worthiness of the subsystems and operation modes with the post-crash alert subsystem for passenger cars. The earlier safety models for manually driven cars focus on the uncertainties in various task scheduling techniques and wild jumps in the application software with an underlying operating system timing functions. Since the design complexity of the modern day cars has increased to a great extent with all infotainment and luxury items, the safety assurance and safety control have become serious issues. The category of fully automated cars and the cyber connected car with remote navigation face many hazardous threats and create a total damage not only within the network but also on the public road sides. The proposed integrated safety model consider the hardware and application program interfaces of the graphic processor with conventional central processor in exchanging critical data and jumping to various memory pages across the critical instructions. Safety enhancement is done on the basis of the initialization of virtual machines for their essential operations of the car and the policies in the network while navigation of the physical car was with virtual application services. The dynamic scheduling either based on the time or the data arrived at was carried out in multiple layers to land on a safe reachable state within the computational workspace of the car. The context with the data was transferred within the various types of memory devices like cache, virtual and graphics memory was carefully dealt with to attain maximum safety in all possible cases of use. The on demand virtualization process in the case of failure and recertification process of components and interfaces while offering network virtualization services were also considered to provide overall safety to the automotive system with a GPU employed and the essential program is executed through application program interfaces developed in CUDA. Safety was realized through multiple functions that can be segregated include the isolation of the safety-related functions from general-purpose functions. In the operational safety code, a set of kernel checks was introduced towards checking the condition of sensors
which are running parallel and random values generated in order to provide value to check. The automotive software safety model was implemented using CUDA C version 7.5 and tested for different sensors like Speed sensor, Position sensor, Optical sensor, Knock sensor and Oxygen sensor by giving different input data for the same default check and it was checked for the sensor high or low for which value the engine will be started. Two enhanced software safety metrics were Impact Specific Post-Crash Integrity (ISPCI) for automobiles and Design Specific Alert Latency (DSAL) and which were proposed for indications of the safety standards in the process that followed and the compliance of each and every subsystem in that level of integrity. The various car models from different manufacturers who were involved in the implementation of safety methods and their standard, like Nissan Altima, Toyota Rav4, Ford mustang and Volvo XC90, Hyundai and Maruthi. The various existing safety standards ISO 26262, AUTOSAR MISRA C are enumerated for safety compliance verification during the execution of program interfacing parts.

A major limitation of this research work lies in the selection of the correct GPU with as many cores optimized for much a safer operation of the automotive code. The number of luxury items involved in the assembly of the car and the macro and micro component compliance play a major role in safety assurance. The multiple vendors of the micro-kernel based execution of the connected cars will face a serious threat through side channel hardware attack and covert channel attack in the case of corrupted message passing and serious cross side cyber threat through insider hijacking of the subsystems. In the future work, the specific passenger car model will be chosen with the fixed number of traffic rules and the traffic conditions, the collision avoidance and crash worthiness of the individual software component cane enhanced through the latest multi core programming and portable libraries. In another part of the future research, smart traffic and smart city will be focused in the
context of automated safety for automobiles based on the physical and computational environments

This research work deals with an advanced safety enhancement model and techniques for passenger cars by considering crashworthiness, collision avoidance and post-crash alert subsystems features in addition to performance improvements with the help of graphic processors through parallel procession and safe scheduling techniques. The work utilizes the existing standard techniques like software safety hazard analysis, fault tree analysis, event tree analysis, cause-consequence analysis, hazards and operability analysis, failure mode effect analysis and fault hazard analysis for safety critical system. The work proposes new models and their design, suitable safety logic and multicore programming safe code, traceability feature with distributed software safety document service. The research work proposes new metrics for the pre and post-accident scenario to study the impact of accidents with assessments of safety due software and environmental factors.

Future passenger cars would have the ability to communicate with the changing traffic environment and required to provide the driver with relevant information to avoid hazardous situations and provide timely information and warnings to all of those involved in the traffic mixture. The vehicle to vehicle, vehicle to infrastructure communication and driver assistance systems would be able to improve the safety due to unprotected traffic participants including pedestrians. The safety of cyber connected cars resulting from streaming connections, regulated driving on highways, excess of data through modern information and entertainment services and driver assistance systems that are inside and outside the vehicle will increase the complexity of the safety issues.