

Human Safety requirements based on a steering by wire system

Safa Jameel Dawood Al-Kamil

Obuda University, Faculty of Mechatronics Engineering, Budapest, Hungary
engsafa12@gmail.com

Tamas Szakacs

Obuda University, Faculty of Mechatronics Engineering, Budapest, Hungary
szakacs.tamas@bmk.uni-obuda.hu

Abstract: Steering systems are one of the most significant components in vehicles since they directly related with drivers, and their performance considerably affects the steering feel. However, steering failure can cause hazardous driving situations. Therefore, the contribution of this paper is two-fold. First, it describes the research effort to assess the functional safety requirements related to a steer-by-wire (SBW) system by applying a number of hazard analysis techniques. Second, it presents a fault-tolerant architecture that can be used for SBW systems to improve vehicle safety through better steering capability. The results of this study provided support for drivers with their driving tasks, and an alternative controllability SBW system was used.

Keywords: SBW, hazard, safety, fault.

1 Introduction

There is an ever-increasing demand on the automotive industry in areas like safety, driving pleasure and environment. This requires new complex functionality to be implemented in cars. Transport safety and road safety especially has been accorded high importance on international development because of its magnitude and effect on the society and economy. Global key risk factors, identified by WHO in [1] for traffic accidents are speed, drink driving, motorcycle helmets, seat belts, and child restraints. The general highway traffic safety administration instituted the electronics reliability research area to study the reduction and safe management of electronic control system failures and operator response errors, the

hazard analysis techniques have been used in the development of conventional automotive systems and the fast progress in automotive electronics have increased The number of new characters for automobiles. In many cases, these are new entertainment or driver information features [2]. The increased use of microcontrollers in modern automotive systems have created many advantages, such as merging chassis control systems to achieve active safety with passive-safety systems. when chassis control electronics discover an out of control condition. Stability control can be linked to steering or implement automatic control of oversteering, it has also carried the potential for catastrophic failures [3].

Steering systems are very important components in automobiles because they straight interact with drivers, and their performance greatly affects the steering feel. Steer-by-wire (SBW) systems, which have no mechanical linkage between the steering wheel and front wheels, are assumed to improve vehicle safety during better steering capability. SBW system failures, however, can cause hazardous driving situations. Electronic stability control (ESC) has been developed to improve automobile stability via braking force control. Many vehicles are now equipped with ESC, which is to distinguish as a beneficial device to improve vehicle stability. In the future, a new automobile regulation will demand every vehicle to be equipped with ESC. However, these devices assume in normal driving conditions without steering system failure. Two areas, within driver steering interaction, were identified as most valuable to be able to design effective active safety systems. first was to find a map for results that received in research on cars and The other was to better understand driver behavior at a sudden lateral disturbance. Hazards are potentially unsafe events or conditions that could lead to undesired consequences or events. System safety engineering is the application of engineering and management principles, criteria, and technology to provide a reasonable and achievable level of safety together with other system design constraints throughout all phases of the system lifecycle [4]. A separate set of analysis techniques are suitable to determine the completeness of specifications [3].

This paper reviews some existing vehicles systems that are forerunners to x by wire systems and suggests a fault-tolerant architecture. We will focus on describing the main design analysis techniques.

2 Control By-Wire Technology

Embedded electronics, quick developing area, and software-based systems are progressively replacing the mechanical or hydraulic ones. First by wire technologies have been advanced in a flight, in enormous aircraft hydraulic and mechanical connections between input devices of a pilot and the actuators have

been replaced by electronic wires. The pilot provides his orders by the cockpit [5]. There are several different types of drive by wire systems, which is why it's sometimes referred to generally as x by wire the main by wire systems. Steer by wire, throttle by wire, brake by wire. In this paper, we are especially use a steer by wire subsystem. The lower reliability and different fault behavior inherent in the electronic and electrical components used in drive by wire systems without mechanical backup have made the transition from systems with mechanical backup extremely challenging. Nevertheless, fault-tolerant electronic systems must be incorporated to meet the high safety requirements set by governments, especially in developed countries. An example for replacing the mechanical or hydraulic system is a steering system. However, there is no steering column between the steering wheel and the front wheels in a steer by wire car, instead of the mechanical linkages there are electrical signals. Therefore, there are new dependability requirements for the electrical system. The causes of this evolution are technological in addition to economical. Consequently, the cost of hardware components is decreasing while their performances and reliability are increasing. This evolution, formerly confined to functions such as motor control, wipers, lights, or door controls, now affects all car domains, even for critical functions such as throttle, brake or steering control. an increasing number of vehicle engines have been manipulated by an electronic pedal and an electrically driven throttle or injection, which represent the first drive by wire components, such systems are equipped with a fail-safe function. The future systems become more advanced in functionality, design, and applied technology, the need for a comprehensive hazard analysis approach becomes more clear. Technologies such as by wire that do not rely on mechanical linkages for backup must be analyzed so that an adequate level of redundancy is designed into the system, and that other appropriate hazard controls are satisfied.

3 Steer-by-Wire System

Steer by wire (SBW) systems are a relatively new advance compared to the traditional mechanical, hydraulic, or electric steering systems that are nowadays used for motor vehicles, It provides the potential advantages of enhanced vehicle performance [6]. Figure 1.a shows the steering wheel (SW) rotation given by a driver is transmitted through the intermediate shaft. The column is linked to the rack and road wheels. Thus, the road wheel angle is proportional to the SW rotation. An amplified hydraulic pump is used to decrease the driver's steering efforts. In SBW, Figure 1.b, the intermediate shaft, and the hydraulic pump are removed. And several position sensors and actuators are involved in the SW and Vehicle wheel (VW). In a steer-by-wire system, there is no mechanical coupling between the steering wheel and the steering mechanism. Although the mechanical linkage between the steering wheel and the road wheels has been eliminated, a

steer-by wire steering system is probably not only to implement a similar function like a conventional mechanically linked steering system but are additionally expected to present the advanced steering functions. Electronic power assisted steering systems (EPAS) and SBW is exchanging hydraulic power steering in many new vehicles nowadays [7].

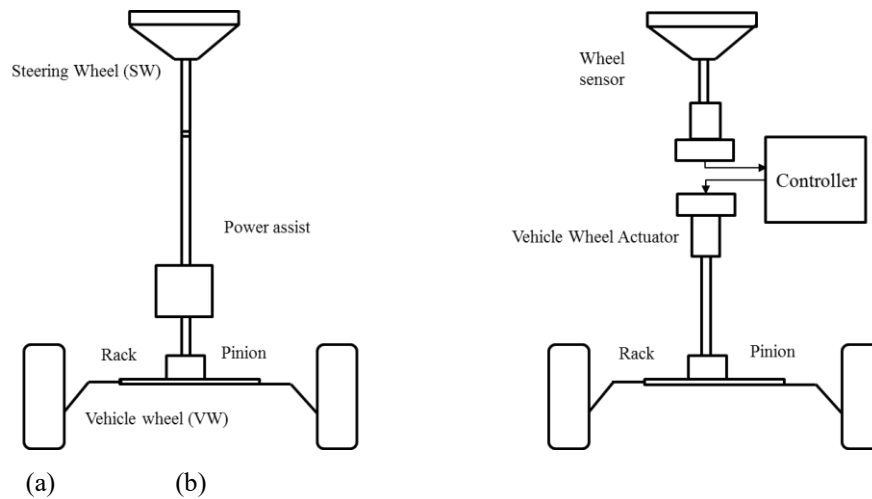


Figure 1: Conversion from conventional steering system to SBW [8].

SBW system is definitely the most complex drive by wire system which is also the large safety critical by wire system in a vehicle. In a pure steer by wire system, the steering column is eliminated. In a pure steer by wire system, the steering column is eliminated. Sensors mounted on the steering wheel are interpreted by the controller to generate the correct amount of road wheel angle using electric motors based on the vehicle velocity. If a sensor stops functioning properly, the controller will not be able to actuate the motors to generate the correct road wheel angle, potentially causing a hazardous situation. (SBW) systems allow the amount of steering wheel operation to be transmitted in the form of electric signals to the vehicle wheels. These systems help improve control performance for vehicle safety while increasing vehicle design freedom. Thus, this type of system seems to have promise as a next-generation automotive steering system.

As shown in Figure 2, the conventional hydraulic steering assembly has been replaced by an electric motor actuator to drive the road wheels in the road wheel mechanism. Road wheels are connected to a rack and pinion mechanism by tie rods. An angle sensor mounted in the motor or the rack and pinion mechanism is used to sense the road wheel angles. The steer by wire controller receives road wheel angle signals and makes a control signal to the permanent magnet brushless direct current (DC) motor through its electric drive. The most important aim for controlling the road wheel mechanism is to save the road wheel tracking for the reference road wheel angle. The reference road wheel angle signal comes from the

steering wheel assembly and changes according to the vehicle driver's intent and the vehicle dynamics requirements. This system consisting of the road wheel mechanism and its control is referred as the road wheel control subsystem.

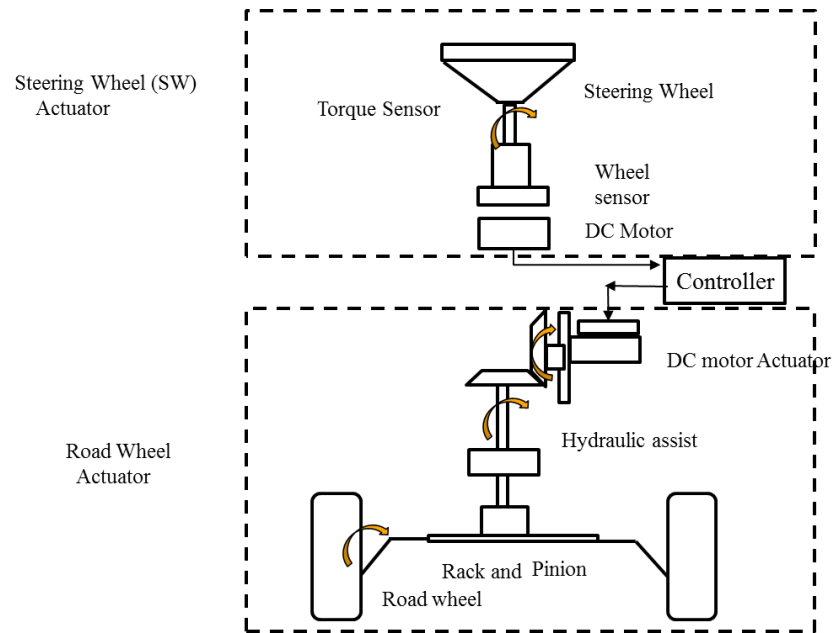


Figure 2: Schematic Diagram of the Steer-by-Wire System [8]

On the other hand, SBW system failure can cause unsafe driving situations. In the case of airplanes, significant redundancy in a fly by wire systems are effective to avoid hazardous failures. In the case of a mass-produced passenger vehicle, however, it is hard to install SBW systems with sufficient redundancy, as a result increase the cost, volume and weight.

4 Hazard and Safety Analysis Methods

Hazards are potential unsafe happenings or conditions that could cause undesired consequences or events, it also means the occurrence of an event that puts people in risk of danger [9]. Example of a hazard is losing a wheel of the vehicle when driving. This event puts the driver, walkers or other road users at risk of getting injured. A hazard happens when a fault propagates to an error that is not covered by safety mechanisms in a system. The interaction of undesired causes typically combines to result in a hazard in conducting a hazard analysis, the term hazard will be also used to describe scenarios that may cause harm. The Hazard Analysis

and Risk Assessment (HARA) as shown in Figure 3 is derived in combination with our customer, and availability is part of the safety goals.

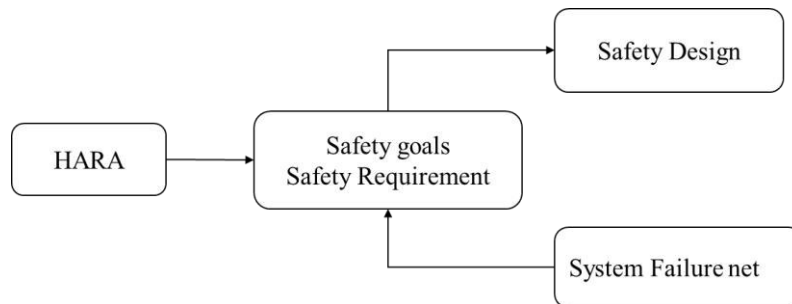


Figure 3: Hazard analysis and risk assessment.

Faults are potential physical or logical defects in the design or implementation of a device or system. Under certain conditions, they cause errors like incorrect system states which can induce failures or a deviation from appropriate system behavior. The failure is a hazard when it leads to an incident. Notice that not all hazards can lead to faults. Hazards can also be produced by unexpected sequences of interactions between components or subsystems. Safety is intimately connected to the concept of risk, and generally means a relatively high degree of freedom from harm. As shown in Figure 4, the risk is a combination of the likelihood and the severity of an unplanned, undesirable event. A system is commonly considered to be safe if the level of risk is reasonable [10]. Reasonable risk must be evaluated according to societal, legal, and corporate concerns [11].

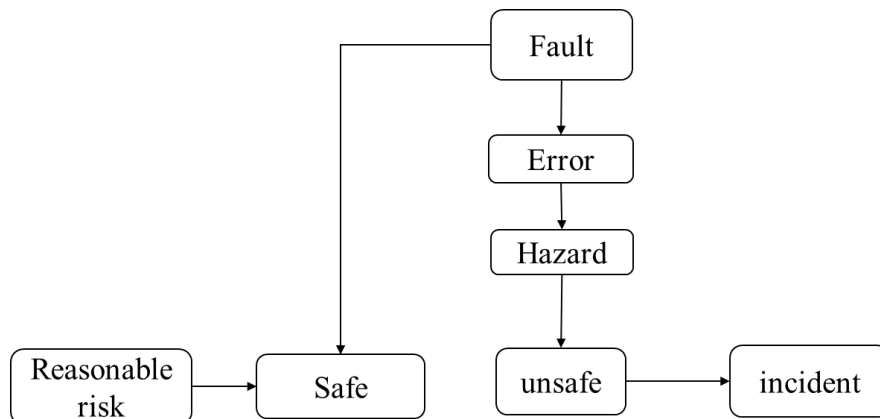


Figure 4: The safe diagram.

System safety also means a particular system of engineering that supports program risk management. It is the application of engineering and management principles, criteria and techniques to optimize safety. The aim of System Safety is to optimize

safety by the identification of safety-related risks, controlling them by design and procedures, based on suitable system safety precedence. System safety engineering is the application of engineering and management principles, criteria, and technology to provide a reasonable and achievable level of safety together with other system design constraints throughout all phases of the system lifecycle. A system-safety program for by-wire systems or any other type of system must be coordinated between vehicle manufacturers and suppliers. Application of a system safety program (see Figure 5) agree with a good method for improving and documenting the safety of a product design [12].

The objectives of a system safety program exclude:

- Identify potential hazards and associated avoidance requirements,
- Convert the safety requests into engineering requirements.
- Supply the design assessment to the continuing design
- Control the hazard by using the relative compliance of design for requirements and document findings.
- Straight and monitor specialized safety testing.



Figure 5: The Safety program.

5 Fault Tolerance Techniques

To create a safer system and more reliable, safety mechanisms have to be added for the system to be able to tolerate certain faults and avoid the system from propagating to a critical failure. This paper describes some techniques for increasing the reliability of a system. Fault tolerance can be implemented in both hardware (HW) and software (SW) fault [13]. The detection of significant faults that endanger steering control is an important aspect of the system. Figure 6 shows the concept of fault tolerance is related to dependability:

- Availability
- Reliability
- Safety
- Maintainability

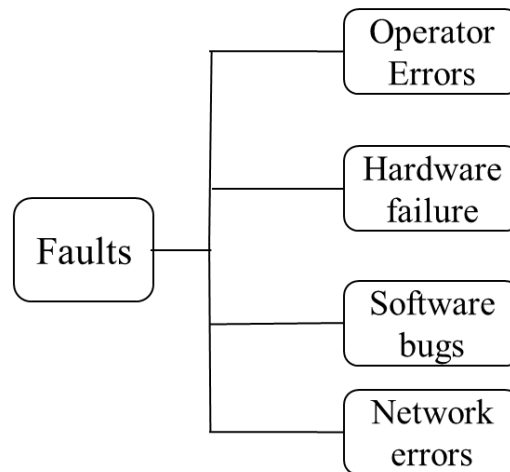


Figure 6: Illustration of the fault concept.

In the event of the SBW control module detects a fault in the system, the system will still need to provide directional control for the vehicle. In the intermediate SBW system designs, the SBW system is equipped with a mechanical clutch that completes a direct mechanical connection between the steering wheel and rack and pinion. In full SBW systems, the design may include redundancy of the power and control components of the SBW system. But because of the fact that there is no mechanical linkage between the steering wheel and the road wheels for SBW system, a fault from a sensor, actuator or microcontroller that form the control system may result in unwanted steering effects, if not controlled quickly in a fault tolerant manner. Hence, a fault-tolerant control system is safety critical in SBW automobiles, requiring highly dependable sensors and actuators, fast fault

detection and identification algorithms and a means for maintaining reliable vehicle control in the event of a fault. The steer by wire architecture involving the following components: ECU's, communication lines like CAN buses, and appropriate sensors and actuators. Thus the system requirements apply to the entire distributed architecture (i.e., hand wheel, road wheel, controller, ECU's, buses, software, sensors, and actuators). The overall safety-critical requirements for a given system belong to the following classifications: Failure requirements, safety goal requirements, domain requirements, and development environment requirements. There is a variety of real-time bus systems that are used to connect electronic control units in automation or in the automobile. Most of these communication protocols are one channel systems, although there are possibly some fault tolerance mechanisms, there is no really redundant transmission of messages. In some safety-critical applications, however, redundant message transmission becomes a requirement. A time-triggered variant of CAN, denoted in the sequel by TTCAN, is defined by the ISO standard 11898-4 as displayed in Figure 7. Basically, CAN and hence TTCAN is a one channel system, redundancy can only be provided by using multiple TTCAN buses. However, compared with intrinsically redundant systems similar to (FlexRay, TTP/C), the use of multiple single channel busses presents the problem of management of redundancy.

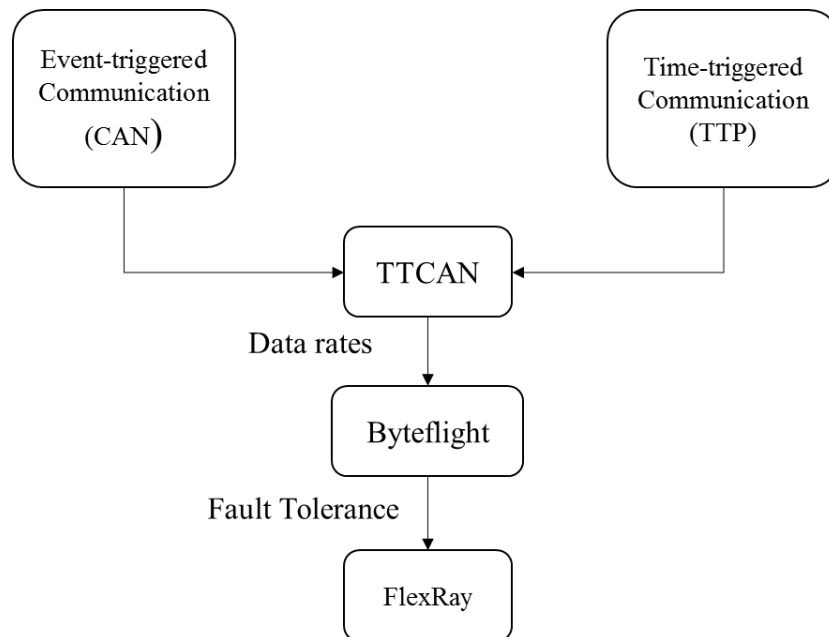


Figure 7: General structure for event triggered and time triggered.

6 Hazard analysis techniques

The hazard analysis techniques include analyzing different views of the system over the entire product design cycle and integrating the results, therefore a consistent and complete representation of the system's hazards, failure modes, faults, and hazard controls is made. A set of hazard analysis techniques as shown in Figure 8 can provide this useful multi-view analysis. These techniques are Preliminary Hazard Analysis, Reliability Block Diagrams Failure, Modes Effects Analysis, Failure Modes Effects and Criticality Analysis, And Common Cause. The Preliminary Hazard Analysis technique aims to identify great level system hazards and to find the criticality of potential mishaps that can arise. The most important steps for making it Provide a description of the hazard, and potential mishap scenarios related with the hazard, identify potential reasons of the hazard, find the risk of the hazard and mishap scenarios determine if the controls can be added to the system to eliminate or mitigate the risks. At this stage, only a hazard control feasibility study and system requests to control the hazards are wanted. while the basic steps for creating the reliability block diagrams technique Starting from the input and working toward the output, classify system components that could contribute to the specific hazard if they failed. For every element, made a block and place it in a position relative to its location in the input to output flow of the system. At each level, and for each intermediate event or component, consider command path faults and secondary faults, and primary failures for the failure modes effects analyze technique and also generate a Boolean expression of the tree to determine the combinations of principal events that can lead to the high-level hazard of the tree. Failure modes effects analysis and failure modes effects techniques used to Identify and list individual components, the function they provide, and their failure modes. And consider all possible working modes. The second important step to find the severity of the failure, the potential causes of the failure. For the Common cause analysis first step is to define and group the critical components to be evaluated. Within the groups, order for commonalities such as physical location, common manufacturers, a common design process that could lead a generic design defect, these techniques have been commonly used in the military, aerospace, and nuclear productions and the vehicle industry and each technique can lead more quickly to results that are closely linked to the particular strength of that technique. The use of multiple techniques raises the accuracy of a safety analysis program and increased the opportunity of assets that must be supplied.

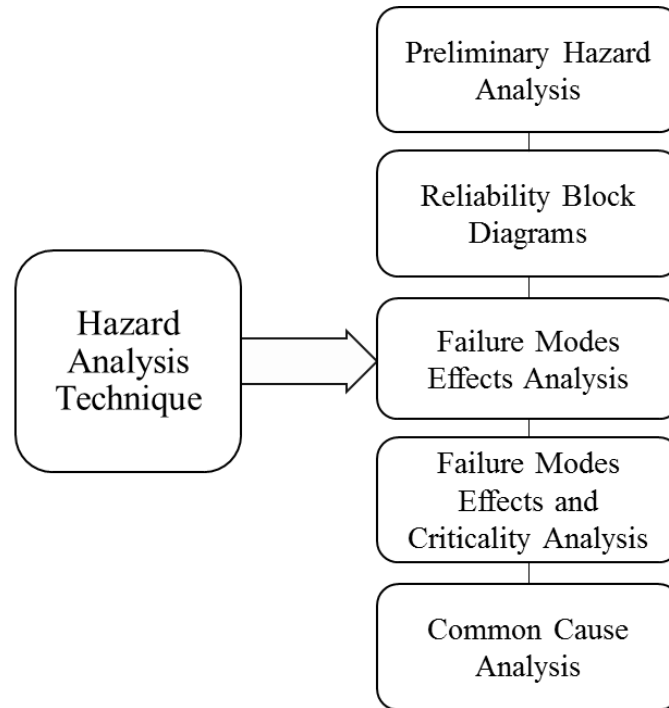


Figure 8: Hazard analysis techniques.

7 Conclusion

The proposed architecture has the potential to improve vehicle safety and reliability. This architecture is expected to facilitate the use of steer by wire system as an essential system for passenger vehicles. There are some possibilities for hardware and software architectures conditional upon the level of redundancy, and grade of error detection and fault recovery suggested by the system. Hazard analysis plays an important part in the growth of safety-critical systems. the application level for using the principles of engineering system that holistic approach was used to achieve safety at various levels.

References

- [1] Organization World Health, "Global status report on road safety 2013, Technical report," 2013.
- [2] S. Buckley and K. Johnson, "Concepts Designed to Enhance the Customer's Driving Experience," SAE International Congress on Transportation Electronics, 2000.

- [3] Nancy G. Leveson, "SAFWARE, System Safety and Computers," Addison-Wesley Publishing Company, 1995.
- [4] M. Allocco, G. McIntyre, and S. Smith,, "The Application of System Safety Tools, Processes, and Methodologies within the FAA to Meet Future Aviation Challenges," in Proc.17th International, pp. 1-9, 1999.
- [5] Balajee S B, Balaji P, Shreyas J, Satheesh K, "An Overview of X-By Wire Systems," International Journal of Innovative Research in Science, Engineering and Technology, vol. 4, pp. 152-159, 2015.
- [6] J. Nilsson, "Analysis and design of Real-Time Systems with Random Delays," Lunds University of Technology, pp. TFRT-3215, 1996.
- [7] A.Badawy, J. Zuraski, F. Bolourchi, "Modeling and analysis of an electric power steering system," SAE Technical Paper, 1999.
- [8] Mohamed Eid S., and Saeed A. Albatlan, "Modeling and Experimental Design Approach for Integration of Conventional Power Steering and a Steer-By-Wire System Based on Active Steering Angle Control.," American Journal of Vehicle Design, vol. 2, no. 1, pp. 32-42, 2014.
- [9] A. Avizienis, J. . Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, p. 11–33, 2004.
- [10] N. J. Bahr, "System Safety Engineering and Risk Assessment," A Practical Approach,Taylor and Francis, Wash, 1997.
- [11] P. L. Goddard, "Automotive Embedded Computing : The Current Non-Fault-Tolerant Baseline for Embedded Systems," Work shop on Embedded Fault-Tolerant Systems, pp. 76-80, 1998 .
- [12] M. Allocco, G. McIntyre, and S. Smith,, "The Application of System Safety Tools, Processes and Methodologies within the FAA to Meet Future Aviation Challenges," in Proc. 17th International System Safety Conference, pp. 1-9, 1999.
- [13] N. R. Storey, "Safety Critical Computer Systems," Boston, MA, USA: Addison-Wesley Longman Publishing Co, 1996.