Volume 4, Issue 10, October 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Hazard Analysis for Software Safety in Road Traffic Control System

K. Jayasri*, P. Seetha Ramaiah
Department of CS & SE,
Andhra University, India

Abstract*— Software safety is the notion that software will execute within a system context without contributing to hazards. Software for safety-critical systems must deal with the hazard analysis. Hazards are identified by hazard analysis in order to make the system safe. A software–controlled Road Traffic Control System (RTCS) requires the high level of safety since this has to ensure safe operation. The hazard identification and hazard control is necessary for system lifecycle. This paper implements safety methods for hazard control using the PHA and HAZOP techniques, which would be suitable for analysing software safety. This paper also implements a software prototype called a software–controlled Road Traffic Control System (RTCS), which is commonly used in city traffic, to validate its utility.

***Keywords*— Software safety, GQM, RTCS, PHA, HAZOP.**

I. INTRODUCTION

The role of software is becoming increasingly important and is being used in many critical applications, such as avionics, vehicle control systems, medical systems, manufacturing, power systems, and sensor networks [1], [2].The electronic and computerized Road Traffic Control System (RTCS) as shown in Fig.1, is an automatic high performance system. The existing electrical and mechanical systems, empirical approaches and engineer's intuition are mainly used to identify any faults, assuring a certain degree of safety in the traffic signal systems. However, the new computerized road traffic control systems do not allow the safety assurance based on such empirical approaches to detect faults. The hazard analysis activity is consisted of various stages such as hazard identification stage, hazard risk assessment stage, hazard risk control stage, etc. There are many techniques such as PHL (Preliminary Hazard List), FMEA (Failure Mode Effect Analysis), PHA (Preliminary Hazard Analysis) and HAZOP (Hazard and Operability) etc. to identify hazard, which is the basis of whole hazard activities. The application of PHA and HAZOP methods are highly recommended for the hazard analysis in signal systems. Among these two techniques, PHA method is to identify the early stage of hazards, and the HAZOP method is often used as a technique for identifying potential hazards in a system and identifying operability problems [4], [5].

The NASA Technical Standard [3] gives the following definitions on Software Safety. Safety-Critical: Those software operations, if not performed, performed out-of sequence, or performed incorrectly could result in improper control functions (or lack of control functions required for proper system operation) that could directly or indirectly cause or allow a hazardous condition to exist.

Safety critical Software: Software that (1) exercises direct command and control over the condition or state of hardware components ; and, if not performed , performed out-of-sequence, or performed incorrectly could result in improper control functions (or lack of control functions required for proper system operation), which could cause a hazard or allow a hazardous condition to exist. (2) Monitors the state of hardware components; and, if not performed, performed out-of-sequence, or performed incorrectly could provide data that results in erroneous decisions by human operators or companion systems that could cause a hazard or allow a hazardous condition to exist. (3)exercises direct command and control over the condition or state of hardware components; and if performed inadvertently, out-of-sequence, or if not performed, could, in conjunction with other human, hardware, or environmental failure, cause a hazard or allow a hazardous condition to exist [9],[10].

This paper proposes safety methods for hazard control in RTCS using PHA and HAZOP. The hazard identification is the basic activity in hazard management procedure. It is impossible to mitigate hazards in system development lifecycle, if the hazards were not identified. The paper concentrates on two of the hazard analysis methods like PHA and HAZOP for traffic signal systems to identify the initial hazards.

In this part of paper, Section 2 reviews hazard control methods PHA and HAZOP, Section 3 presents the proposed software safety model, Section 4 describes Results and discussions of RTCS, the final section gives a summary of the work done.

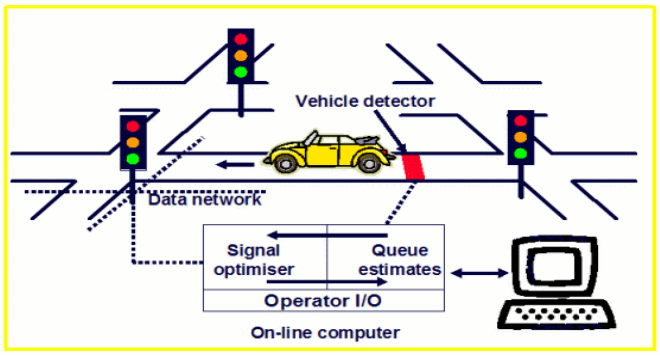

Fig.1. General RTCS diagram

II. HAZARD ANALYSIS

Hazard analysis deals with risks during software development. Hazard analysis contains hazard identification, hazard control and mitigation [6]. Hazard control is a system used in software industry to minimize or eliminate hazards. It is a widely accepted system promoted by numerous safety organizations. There are many techniques such as PHL (Preliminary Hazard List), FMEA (Failure Mode Effect Analysis), PHA (Preliminary Hazard Analysis) and HAZOP (Hazard and Operability) etc.

A. Preliminary Hazard Analysis

PHA technique is the starting stage of hazard control which finds out hazards possible to be occurred in each of the systems. PHA will analyse potential hazards which can be occurred in the system by drawing hazards. The preliminary design stage Hazard analysis activity is to be performed during the PHA process which shall perform the initial stage evaluation on the severity of drawn hazards and frequency of occurrence. Results are used to determine whether the quantified analysis will be necessary in the future, and they make the complete analysis and risk evaluation [7], [8]. This is possible to be performed through repetition and complementation according to the progress in the detailed design of system. Since PHA starts in the early stage of project in the design stage, the usable data are in the incomplete level. In case where these incomplete data are modified and complemented, they must be modified and added in the next stage accordingly.

B. HAZOP Technique

HAZOP technique is the formalized systematic technique to draw the hazard, and it examines the cause of the hazard. The most important technology in the deduction of hazard is to analyse the cause and result of hazard, and if HAZOP is used in this stage, the hazard can be drawn usefully at the early stage of safety analysis procedure. HAZOP method is often used as a technique for identifying potential hazards in a system and identifying operability problems. HAZOP includes sufficient explanation about the system to prove how deviations can be occurred from the intention of design, and the systematic survey on the whole parts of it. Once verified, the analysis will be made to see whether these deviations and results according to them can have an adverse effect on the safe and efficient operation of system.

III. PROPOSED SAFETY MODEL FOR RTCS

The proposed model for software safety is based on the Goal Question and Metric (GQM) approach as shown in Fig.2.GQM is a generic framework for defining and organizing software metrics according to organizational objectives.GQM is a top-down, goal-driven approach, which ensures that all metrics are selected for a goal-driven purpose. The aim of GQM is to provide safety.

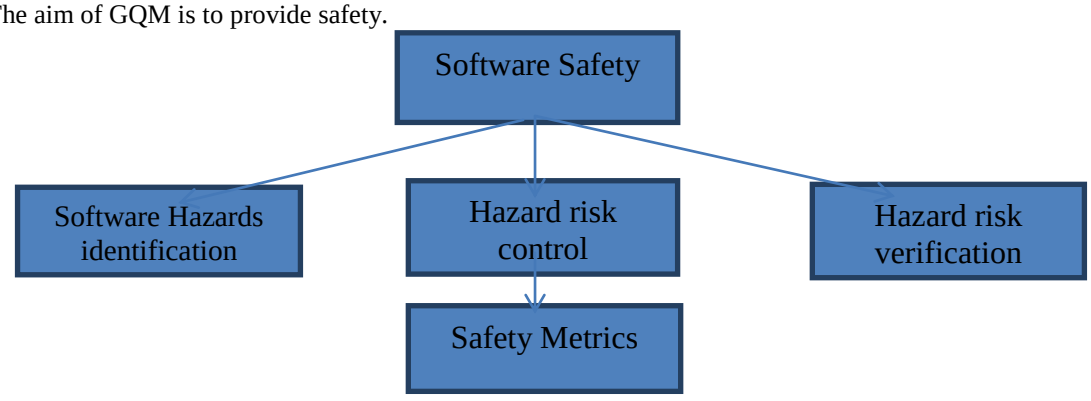

Fig.2. GQM approach for Hazard Analysis

Fig.2 shows the process of hazard analysis. i.e., the safety activity requires the identification of hazards, hazard risk control and risk verification to manage and mitigate the potential risks. This process will be carried out repeatedly until it receives the feedback at its each stage. As explained previously, the hazard management activities of RTCS is

based on the identification of hazards, and do the hazard analysis to mitigate hazards. There are many techniques for hazard analysis such as PHL (Preliminary Hazard List), PHA, HAZOP, FMEA (Failure Mode Effect Analysis), etc. Among these techniques, PHL and PHA are methods to identify the early stage hazard, and the FMEA and HAZOP are used as methods at detail to draw hazards based on the hazard drawn at the early stage. The identified hazards from above two methods have to be analysed to reduce risk factor. The proposed safety model based on the GQM approach is applied to RTCS to validate its effectiveness.

A. Normal Operation of RTCS

The traffic light control system is a RF (Radio Frequency) which is a wireless operated system. This is a fully automatic, timing based system. The system is custom designed for multi-road junctions and different traffic sequences [7]. We design and manufacture traffic light control system and sequencer for wide variety roadways and railways applications. The complete system consists of a programmable master controller unit (control and operate) and multiple slave units (to control the traffic lights). The slave units have multiple (potential-free) relay outputs points. The master control unit can be programmed to control a variety of different light on / off sequences for various directions of traffic. These sequences contain individual timing of Red->Green, Flash light timing etc. The individual timing parameters can be programmed as per requirement or traffic load conditions. This system is also capable of operating in manual mode, with a dedicated sequence button for each of type of traffic conditioning.

IV. RESULTS

The safety model is applied to RTCS. First of all, the system-level hazard analysis was to identify possible hazardous failure conditions at the system level**.** Here four types of roads and traffic controls were shown by below figures. The four types of roads are of Ring roads, Lane-closing, On-Ramps and Uphill grades. RTCS contains different parameters like average-density, type of vehicle, time-warp factor, desired velocity, Acceleration, Time-gap and Distance to monitor and control the traffic flow. Average density indicates number of vehicles per kilometre/lane. Desired velocity indicates the speed of the vehicle. Traffic lights are used in all types of roads to control the flow of vehicles. In on-ramp roads, the new lane traffic will be added to main lane from other side to the main flow. The ramp-inflow parameter is used to avoid collisions. The snapshots of the RTCS are shown in Fig.3 to Fig.6.Each snapshot represents a type of road in RTCS.

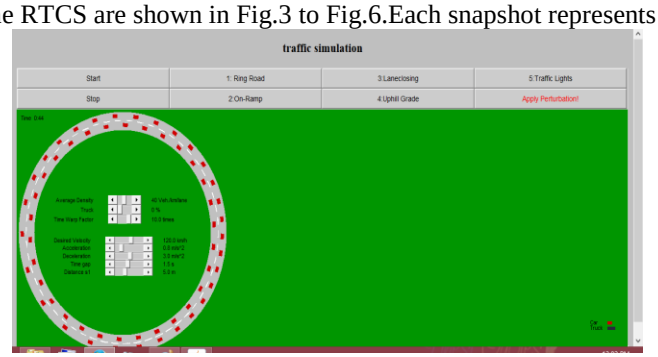

Fig.3. Ring-road of RTCS

Fig.4. On-ramp road of RTCS

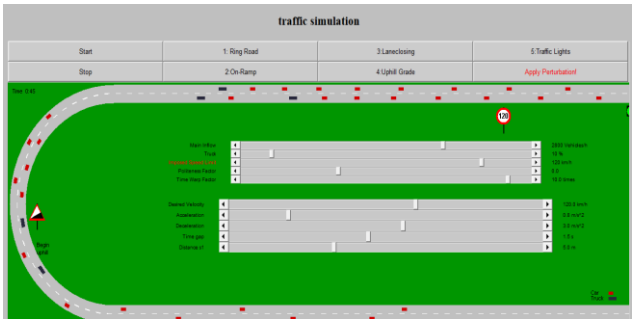

Fig.5. Uphill Grade Road of RTCS

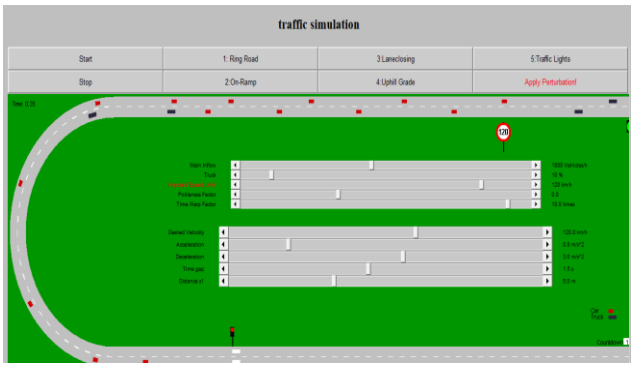

Fig.6. Traffic light systems of RTCS

V. CONCLUSIONS

The present paper identifies Hazard Analysis for Road Traffic Control System using PHA and HAZOP Methods. This paper implements a prototype called RTCS, which includes safety critical operations. PHA method is used to identify the early stage of hazards. The HAZOP method is often used as a technique for identifying potential hazards in a system. The aim of the hazard analysis is to identify and mitigate the hazards during system development. The results observed from RTCS are satisfactory. This work can be extended by incorporating various safety metrics to the existing RTCS system. Meticulous work is required to meet the complete requirements of software safety aspects that lead to consistency of RTCS with safety metrics.

REFERENCES

[1] Dongfeng Wang, Farokh B. Bastani, I.-Ling Yen: Automated Aspect-Oriented Decomposition of Process-Control Systems for Ultra-High Dependability Assurance. IEEE Transactions on Software Engineering, Vol. 31, No. 9 pp.1, september-2005.

[2] P. V. Bhansali: Software Safety: Current Status and Future Directions. ACM SIGSOFT Software Engineering Notes. Vol. 30 No.1, pp 3, January-2005.

[3] Software Safety. NASA Technical Standard, 1997. http:// atc.gsfc.nasa.gov/assure/distasst.pdf

[4] Raghu Singh: A Systematic Approach to Software Safety. Proceedings of Sixth Asia Pacific Software Engineering Conference (APSEC), Takamatsu, Japan – 1999.

[5] Ramakrishna, Satish: Run time Assertion Schemes for Safety Critical Systems. Ninth IEEE Symposium on Computer Based Medical Systems, Ann Arbor, Michigan -1996.

[6] Jayasri Kotti, Seetha Ramaiah.P: Software Safety Metrics for safety Critical Computer Systems, International Journal of Network and Information Security, Vol.1, pp. 15-18 June-2013.

[7] Ben Swarup. M, Seetha Ramaiah P.: An Approach to Modeling Software Safety, Proceedings of the 9th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD), Phuket, Thailand , *Aug*-2008.

[8] K.Jayasri and P.Seetha Ramaiah. "Metrics for assessing safety risks of software throughout the software development life cycle" Proceedings of the IEEE International conference on Advanced Research in Engineering and Technology (ICARAT-20013) at K.L.University-2013.

[9] V. Basili and H. Rombach, "The TAME project: Towards improvement- oriented software environments," IEEE Trans. Software. Eng., vol. SE-14, no. 6, pp. 758–773, -1988.

[10] James Bret Michael, *Senior Member, IEEE*, Man-Tak Shing, *Senior Member, IEEE*, Kristian John Cruickshank, andPatrick James Redmond, "Hazard Analysis and Validation Metrics Framework for System of Systems Software Safety",IEEE SYSTEMS JOURNAL, VOL. 4, NO. 2, JUNE 2010.

