International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-4, September 2018

Review of the use of Formal Specification Techniques in Safety Critical Systems

Manohar K. R. Dasannagari, Emanuel S. Grant

Abstract*: *In today's world, computers permeate control systems on which most human lives depend. Thus, the need for software safety is vital. One best approach to ensure the correctness of such systems is to apply formal specification techniques. The use of these techniques helps in the increase of human confidence in safety critical systems. This paper focuses on the review of the use of formal specification techniques in the fields of aviation, and railways. The first section gives a brief description about safety critical systems and formal specification techniques. The second section provides background of the use of formal specification techniques in different areas. The application of formal specification techniques in the railway industry, its advantages and disadvantages will be discussed in third section. The next section provides an insight of application of formal specification techniques in the field of aviation, its pros and cons. The concluding section addresses future need of formal specification techniques usage in safety critical systems that can put human life at stake.

Index Terms: Safety Critical Systems, Formal Specification Techniques, Aviation, Railways, Medical.

I. INTRODUCTION

Safety is considered as one of the prime concerns in most situations in today's life. The term safety can be defined in many ways such as dispensation from getting exposed to threats or freedom from injury or exemption from damage, suffering. [1] In today's world, the use of computers is growing rapidly in almost all areas of interests such as aviation, railways, medical, military etc. A need for safety in such fields is vital because any malfunction or failure in computer systems put human lives and the environment in menace. Such systems are termed as safety critical systems. A best solution to avoid hazards because of the failure in system's operation is to find and get rid of the dangers during system's design and development [1]. All these safety needs paved a way for the use of formal specification techniques in safety critical systems to get rid of errors during the requirements, specification and design steps of system's implementation [1]. Mathematical based methods or notations which are highly used in the development of safety critical systems that are precise and error-free are termed as formal methods or formal specification techniques [2]. A formal specification can also be thought as specifying a stack of properties at some level of idea that a system must fulfill in some formal language [3].

A system can be depicted and its functionalities can be examined with the use of formal methods [2]. If a language expressed is made up of three segments such as protocols for deciding the syntax, rules for depicting the semantics within the consideration of the system domain, standards for gathering important verification hypothesis from the specification, then a specification is said to be formal [3]. The amount of time spent in figuring out specification is one of the major obstruction during formal methods usage in practice [2]. However, safety critical systems precision and stability can be achieved using formal methods which concentrates at the beginning stages of requirements development [2]. Need for safety in ever changing technology used by humans is the drive force to make this paper focus on review of use of formal methods in safety critical systems which contribute to the systems accuracy and consistency.

Revised Manuscript Received on 30 September 2018.
***** Correspondence Author
Manohar K. R*. Dasannagari, University of North Dakota, Grand Forks, ND 58202, USA
Emanuel S. Grant, University of North Dakota, Grand Forks, ND 58202, USA.

II. BACKGROUND

Formal methods can be applied in various areas within the boundary of safety critical systems. Some of the areas where use of formal methods plays a vital role are acquisition of requirements, modelling of the system (design), code composition, formulation of hardware, documentation of system designed, interface between humans and designed system. Now, let's briefly see how important it is to use formal methods in the above-mentioned areas. [4]

A. Acquisition of Requirements

Requirements acquirement plays an important role in the implementation of any safety critical system. For any system to run without any failures, requirements in that system design must be accurate. If any mistake takes place at the stage of requirements capture, it will be followed throughout the implementation of system. To get rid of the mistake that has been identified when the system is in use is very expensive. The cost to make any changes in system that has already been developed is high when compared to making changes in the system at the early stage of requirements acquisition. The best way to verify the correctness of formalizing the requirements acquired is to confirm them against the real world. To justify the requirements, the language used to specify them need to be clear which can easily be understood and simple. [4]

B. Modelling of the System

The formal specification of the requirements captured are refined to a program by the system modelling process using conceivable transformations or any other sort of thorough refinement method.

As there will be numerous programs that support a specification, the input should be clearly given by the engineer. During these transformations, there is a timing issue which is not yet clearly addressed by the formal methods. One of the reason for this timing issue can be intractability.
The things should be kept as simple as possible even during addressing of problems that really matters. A response that is missed is treated equal to failure in functionality in most safety critical systems. [4]

C. Code Composition

When timing aspect is particularly considered, the code that compiler compose is extremely difficult to scrutinize as it involves some unknown things into the process of development and sometimes the code itself is erratic. Compiler should be strictly developed and controlled in a way that high level safety critical code is developed. Many recent studies have shown that a compiler prototype in the form of a logic program can be produced that is almost equal to the original specification. The studies have even showed that compiling specifications can be validated effectively. [1]

D. Documentation of System Designed

A documentation provides a clear view about any system that has been designed. If any changes have been made in the system design, all the changes will be present in the documentation of that system. Uncertainty and errors can be minimized with the help of formalizing the documentation. The timing concerns in safety critical systems are vital and ways to document these concerns are important. Formal methods can be thought of as a support for robust documentation as they provide a way to document the functionality of a system that is expected and even derived. Documentation of a system can be thought of as a record that contains formal notations representing requirements and specifications along with suitable English narration. [1]

E. Interface between Humans and System

The interface between humans and system designed is very important in safety critical systems as it is mutually dependent and user-friendly. In real, it is difficult to formalize interface between humans and system because of the problems such as allocation of tasks and perceiving of the allocated tasks. Many efforts are being made to classify different interface characteristics that can promote the trust on interface between humans and computers. [4]

F. Formulation of Hardware

Formalizing the design process of Programmable Logic Controllers which are used in process control has been initiated. Field Programmable Gate Array is a new hardware technology which can be used in safety critical systems as they allow the engineers to directly program the hardware same as how they do normal computer programs. The timing issue which is a major concern in safety critical systems can be simplified with the help of circuits that are synchronous and it is one of the feature that is supported by direct implementation of hardware. Now, the compilers could be produced even from low-level languages which is a goal that they can be proved formally correct. [4].

G. Formal Methods Use in Railway Systems

Railways can be considered as one of the safety critical systems because any failure in the system leads to loss of human lives and damage to the environment. There are many areas in railways where the use of different formal methods can bring a significant change. Here, we are considering an area of railway interlocking system using Z formal specification technique for our review. The main review focus is to present use of Z formal specification technique in railway interlocking system but implementation of Z representation is not centered.

H. Z Specification Language

A formal specification language which is being widely accepted for the software systems specification is Z. Z specification language is based upon the design of model and concepts in mathematics such as relations, set theories, logical predicate. The specification of complex systems is divided into schemas where each schema constitutes a name of schema, declarative part with the attribute names and their types, predicate part with constraints and relationships among the attributes in declarative part. The specification can be implemented by using one of the tools such as Z/EVES. [5] A description of the structure of a Z schema is illustrated in Fig. 1.

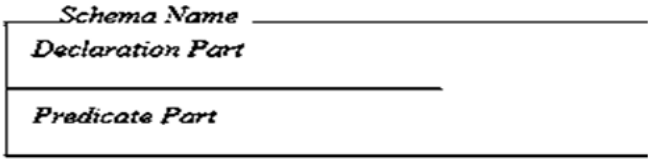

Figure 1. Z Schema Description

I. Use of Z in Railway Interlocking System

The problem statement is defined in an informal way in the initial step of Z specification method. To control and regulate the safe movement of trains on railways, certain rules and regulations will be imposed by some authority of people maintaining the railways. These rules need to be considered when developing an application for that railway network and this can be thought as a form containing all the possible situations under which the railways operate. This form can be thought as an informal specification of requirements in railway interlocking system. Not all the railways follow similar way to specify the requirements but the specification which is final and given by some staff will undergo verification process. Formal methods are the best in automation of validation process. [6]

To specify some invariants on the railway interlocking system which are to be followed by trains for the safe movement on railways, we first need to investigate the components that this system constitutes and the states of those components. Partitioning the tracks into segments and identifying whether the tracks are occupied or not is done by track circuits. Guiding the trains over intersections and making them end up in some defined positions such as control plus, control minus and undefined is done by objects such as points. Arranging the train ahead of the time on section of track they control, controlling the train from entering certain sections of track by giving permissions or refusals is done by signals. The track segments between an entry signal and exit signal are termed as routes whose state can be route set or route unset.

Each track circuit is associated with a set of sub-sections of routes which can either be free or locked. As we have seen the components and states of railway interlocking system, we can now specify the invariant conditions. [6]
Some of the invariants from [6] are:
• At any point of time, only one of the sub-routes of the route can be blocked on the track circuit.
• The points on the locked sub-route of track section should be aligned correctly.
• The sub-routes of a route which is set are locked.
• All the points on a track circuit are locked when they are occupied.
• All the sub-routes ahead of a locked sub-route on a route are locked.
The safety of railway interlocking system can be achieved when the specification of requirements is satisfied. As the computer interlocking systems have geographic data consideration programs that deal with local data, the points mentioned above can be used to verify the safety of systems by building a similar data model of local geographic information. All the above-mentioned invariants need to be satisfied for the local data to be error-free. [6]

J. Advantages of Z in Railway Interlocking System

Z specification language use in railway interlocking system aided for several benefits. Some of the advantages from [6] are:
• Improved development process quality.
• Improved characteristics of system such as trustworthy, stability etc.
• Reduced number of errors in specification.
• Improved and clear definition and documentation of requirements.
• To make the design and development of a system free from errors.
D. Disadvantages of Z in Railway Interlocking System
Some of the disadvantages of use of Z in railway interlocking systems from [6] are:
• Very large and medium systems cannot be verified for safety using Z approach explained above.
• Non-functional requirements such as usability of system, performance of system cannot be described by Z.
• Parallel behaviors and timed behaviors of the system cannot be described by Z.

III. FORMAL METHODS USE IN AVIATION

Any fault in the aviation puts most of the human lives in danger and even sometimes lead to human's death. Aviation is considered as one of the safety critical systems as any small error in this system puts humans and surroundings environment in risk. An important area in aviation that we focus in this review is automation of air traffic control systems using Z specification language. The representation of Z is not emphasized in this review. As Z specification language is explained in above section, we won't be describing it again in this section.

A. Use of Z in Air Traffic Control System

Before the use of Z specification language in air traffic control system, it has been designed using graph theory as a directed graph containing nodes and edges of zones in the airspace and segments of airways. The Z specification language is used on this directed graph of air traffic control system modelled. Now, let's look at the components in the system and then the invariants that have been applied on the system for the verification of system safety. [7] Physical layouts that are fixed to perform a task and constitutes components that are related to each other is called static topology which is a component in air traffic control system. An element in airspace which is three dimensional is zone. A link between two zones is connection. The entire static topography is represented by these zones, connections and aircrafts. Aircrafts movement within a zone is represented by a network state component where the state of aircraft is occupied if it is within a zone and clear if it is not within the zone. The data of a flight which is making use of air traffic control services is described by the component aircraft. A component that controls and redirects the movement of an aircraft within the zones assigned to it in the airspace is controller. The final component which integrates all the above discussed components into one component is air traffic control system. We can now specify the invariants as we have seen all the components in the system. [7]
Some of the invariants in air traffic control system from [7] are:
• Possibility for an aircraft to move in the reverse direction of an allowed direction is difficult because of the asymmetric connection relation.
• At time, an aircraft cannot be present in two airspace zones.
• The source and destination zones of an aircraft should be different.
• An aircraft's current speed should always be less than or equal to the maximum speed limit of that aircraft.
• An aircraft's current altitude should always be less than or equal to the maximum altitude limit of that aircraft.
• An aircraft's heading should always be less than or equal to 360 degrees.
• A state value must be assigned for all the zones present sector.
• A sector that consists of zones having state values will be controlled by a controller.
• State value of zones must be 'occupied' when they are filled with aircrafts.
• A sector should have a finite number of aircrafts that can fly within it.
• The limit of capacity assigned to the controller must be greater than the number of aircrafts within the sector.
• A state value must be defined for all connections between zones in static topology.
• All the connections between zones in static topology must contain all the zones that have state value.
• All the connections between zones in static topology must include the aircraft destination flying within airspace.
• A sector under the control of a valid controller must include the zones present in static topology connection.
• Connections of a static topology must include all the zones that belong to a sector controlled by a valid controller.
• A controller controls the aircrafts present in the system.
• All the aircrafts being controlled by a controller must belong to the system.

If all the invariants mentioned above are satisfied syntactically and successfully proved by the Z/EVES tool, then the air traffic control system can be said as an error-free and accurate system. [7]

B. Advantages of Z in Air Traffic Control System

The use of Z specification language in air traffic control system has advantages in [7] such as:

- Any complex safety critical system can be modelled without any ambiguity using formal methods.
- In depth knowledge of a system can be attained with the help of formal methods.
- At a very early phase of development process, formal methods helped to identify inconsistencies in formal specification of air traffic control system.
- Formal methods used in air traffic control system has proved that more consistent system specifications can be generated.

C. Disadvantages of Z in Air Traffic Control System

Modelling the specification always undergo a refinement process at some point of time, which guarantees some advancement but with some drawbacks.

- Refining the models can be applied only to the functional specifications.
- It is tough to implement Z with systems having non-functional requirements.
- Z conciliates thee above case by annotating supplementary descriptive text to the specifications, but such information may not be reliable to analyze the system behavior.

IV. CONCLUSION

The demand for high quality and error free software is gradually increasing and formal specifications come to the rescue. The reimbursements of implementing Z are candid and it has also been proved that they have been performing exceptionally well in some enormous zones which entail software engineering to be incorporated, which is also one of the reasons for them to be acclaimed in the industry. Despite the performance, formal specifications must still evolve in a manner to compete with the cheaper alternatives for traditional defect removal techniques. In this paper, we have discussed the use of formal specification techniques at the most important phases of the software development in the railways, and aviation industries. Going forward areas such as research, technology and use for formal specifications in all aspects of software development should be promoted.

REFERENCES

1. Bowen, Jonathan P., and Victoria Stavridou. "Formal methods and software safety." Safety of Computer Control Systems 1992 (SAFECOMP'92). 1992. 93-98.
2. Singh, Monika, Ashok Kumar Sharma, and Ruhi Saxena. "Why Formal Methods Are Considered for Safety Critical Systems?" Journal of Software Engineering and Applications8.10 (2015): 531.
3. Lamsweerde, Axel van. "Formal specification: a roadmap." Proceedings of the Conference on the Future of Software Engineering. ACM, 2000.
4. Bowen, Jonathan, and Victoria Stavridou. "Safety-critical systems, formal methods and standards." Software Engineering Journal 8.4 (1993): 189-209.
5. Zafar, Nazir Ahmad, Sher Afzal Khan, and Keijiro Araki. "Towards the safety properties of moving block railway interlocking system." Int. J. Innovative Comput., Info & Control8.7 (2012): 5677-5690.
6. Janota, Ales. "Using Z specification for railway interlocking safety." Periodica Polytechnica. Transportation Engineering28.1-2 (2000): 39.
7. Jamal, Maryam, and Nazir Ahmad Zafar. "Requirements analysis of air traffic control system using formal methods." Information and Emerging Technologies, 2007. ICIET 2007. International Conference on. IEEE, 2007.
8. Keenan, Peter. "Formal methods and air traffic control-opportunities and limitations." Software in Air Traffic Control Systems-The Future, IEE Colloquium on. IET, 1992.