A Tool for Capturing Safety Properties from Critical System Specifications written in SOFL

Azma Abdullah, Hasan Khatan, Mansoor Abdulletteef, Rohani Abu Bakar, Roslina Abdul Hamid
Faculty Computer Systems & Software Engineering, Universiti Malaysia Pahang, 26300, Malaysia.
Corresponding author Email: azma@ump.edu.my
Received: 18 July 2017   Accepted: 20 September 2017

Requirements Engineering (RE) plays an essential role in software project success. RE illustrate system behavior such as safety that directly impacts the customer experience. However, literature reported challenges in safety requirements pertaining to several activities including elicitation, analysis, documentation and validation. Therefore, this paper aim to propose a tool for capturing the safety properties from the requirement specifications. The tool is written in SOFL language and compose three main steps; capturing safety-related function, deriving functional scenario from the safety-related function, and deriving safety properties from the functional scenario. For demonstrate the process an Auto-cruise Control (ACC) system for vehicles is presented as case study. The case study has verified that the proposed tool is capable of capturing the safety properties of ACC system.

Keywords: safety, safety-critical systems, safety properties, computational intelligence

1. INTRODUCTION

Requirement is a condition or capability required by customers to address their problem or meet an objective, a condition or capability that essential to be achieved or processed by a system or application to satisfy a formally imposed document such as specification, contract or standard. From the requirement documents for the system, a detailed safety specification of the system is produced, which is then correctly and completely documented. Safety is a property of a system that frees the system from all possible defects that can cause occupational illness, death, injury; harm to the environment or equipment damage. Hence, its main goal to restrain the fallout of the system and its disastrous consequences. Currently, due to the rapid changes in technology and computational intelligence, numerous safety critical systems are operating in various industries that are beneficial to humanity, such as in the fields of medical, transportation and process control. However, in these critical systems, minor errors in the system may cause serious risk or harm to hardware, human health, or environments. Hence, the most unambiguity, correct and complete requirements should be captured to produce a system specification in order to reduce the risk to hardware damage, human, or environments.

This paper aim to propose a tool for capturing the safety properties from the requirement specifications. The specification describes the system operations in terms of the input parameters and the output results. For safety-critical systems, a collection of safety-related function needs to be identified. A safety-related function is a function that may result in occupational illness, death, injury; cause harm to the environment or equipment damage. Each safety-related function consist of functional

---

1. Email Address: azma@ump.edu.my