Analysis of manual using formal method

Shuhei Akiyama (1010002)

School of Information Science,
Japan Advanced Institute of Science and Technology

February 6, 2013

Keywords: Formal method, Manual, Human error, Accident, Verification.

Several accidents occur in medical service. For example a medical mistake damages a patient. Such accidents are often caused by human error such as lack of necessary works. It is expected to prevent accidents by removing human error. But, it is difficult to remove all human error. Hence, we need to analyze human error which leads to accident. RCA (Root Cause Analysis) and FMEA (Failure Mode and Effects Analysis) are used to analyze relationship of human errors and accidents. RCA can be applied to an accident when it is happened. FMEA requires experience and knowledge of service.

In this study, We propose a method to analyze service by using formal method. We create model of manual based on contents of service. One can analyze it without experience and knowledge before services are performed. Our method is as follow : (1) We create model of manual as state-transition system by OTS/CafeOBJ. (2) We verify whether the model of manual achieve purpose of services. (3) We create models by adding human error to the model of manual. (4) We verify whether such models achieves purpose of service.

We focus on works and objects used them. Such objects are called as work factor. We define states as sets of work factors and transitions as works. purposes of services and accidents can be represented by work factors. Our method to create model of manual from manual as follow :

(1)we make list of works from manuals. (2)We extract works which alter work factors from the list. In this study, we create a model of manual for laboratory test. We verify accidents donot occur by using manual model. We define purpose of service as a property. We semi automatically verify such a property on CafeOBJ system by creating proof score. If one cannot verify manual model achieves purpose of service, the model have an risk that accident occurs.

Next, we add human error to manual model. We show Human error by unfastening transition rule and adding transition. In this study, we add confusion of work factor or lack of work to manual model. We verify model including human error achieves purpose. In this study, We verify whether three models achive purpoes of laboratory test. In model including lack of work, we verify it achieves the purpose. In model including confusion of work factor, We verify it achieves the purpose. In model including lack of work and confusion of work factor, We can not verify it achieves the purpose. If we verify model including human error achieves purpose of service, the human error does not lead to accident. In contrast, if we can not model including human error achieves purpose of service, the human error have risk that accident occur.