Submission to ISSRE'99 – Fast Track Session

Reliability Assessment through Certification Activities

A.Kornecki, S.Khajenoori, W.Thabet, H. Li, J. Chapman
Embry Riddle Aeronautical University
Daytona Beach, FL
<korn@db.erau.edu>

Introduction

It is imperative for the safety critical software to go through a rigorous verification and validation process. In addition, depending on the specific industry regulations, most of the safety critical software needs to be certified. The research activity mentioned in this paper deals with issues of software verification, validation, and certification as a means of insuring the software reliability. The paper describes various certification methodologies identified and researched in the lab and outlines the technologies identified to certify safety critical software.

The Viewpoint

According to IEEE standard 982, the reliability of a software component is the probability that a failure which causes deviation from the required output by more than specified tolerance, in a specified environment, under specified conditions, does not occur during the a specified exposure period. Our viewpoint on software reliability, then is 1) to achieve high reliability one must implement the reliability requirements, 2) to implement the reliability requirements, one must specify and document them, 3) to insure that the requirements are implemented properly, one must verify, validate and certify both the product and the process by which the product was developed.

The research reported in this short paper is related to the recent departmental activities. The cooperation between ERAU and Guidant Corporation, a leading maker of medical cardiac equipment: pacemakers and defibrilators, led to establishing a unique laboratory. The safety critical nature of the operational firmware installed in these cardiac devices, as well as the software in the associated programming devices installed in physician offices requires use of best practices in the design and implementation. It requires also an advanced testing techniques as well as development of effective processes for verification, validation and certification.

In this laboratory the ERAU faculty and students have engaged in exploration of the industrial partner hardware and software artifacts, developing expertise in the application domain and design and development of safety critical systems and serving as a solution provider and technology transfer agent to the industry partner. The work has focused on a disciplined approach to engineering safety critical system by identifying the best practices and the effective software processes. The industrial partner provides financial support and by close collaboration and continued participation in the lab activities they attract qualified potential employees familiar with the company culture, processes, and products.

Certification Issues

In the civilian sector two leading industries requiring highly reliable software are aviation and health services. Both industries developed ways of certifying software products. In general there are three distinct approaches to certifying the quality of software: assessing the "goodness" of software (product certification), certifying the process of the development organization, and

certifying personnel. Product evaluation techniques are underpinned by techniques for software verification and validation (V&V). Some techniques used for product evaluation and certification are static analysis, dynamic analysis, use of checklists, and formal verifications. These techniques are used to verify the functionality, integrity, reliability, efficiency, portability and maintainability of the software. Another idea is to give the certificate to the software only if an adequate methodology has been used for its development. This certifying approach relies on the premise that good processes will result in good software. This premise has also lead to government regulatory standards for software certification in avionics, medical devices, and electric power generation. There is a recent hypothesis, among the software engineering community, that certified personnel equates to higher quality of software. There are many ways that a person can be certified such as professional licensing examinations, practical experience evaluation and earned degrees. The rigor with which the personnel are certified depends on the criticality of the services that the person offers. Certifying personnel can help the customer identify who is qualified.

Certification in Aviation and Medical Industry

With increasing reliability of hardware, alternate methods were developed for flight critical avionics replacing the classical statistical approach. The methods analyze based systems is not viable [do we have any reference for this?]. Alternate knowledge and methods were necessary to establish equivalent system integrity as the software design and implementation issue rather than the statistical component failures. In addition to the conventional testing, verification and validation became necessary activities. Verification provides the proof that a system is built in a way to meet stated specific requirements. Validation is an activity designed to establish that the requirements were complete and correct, thus making system working as "expected". DO-178B standard was developed to assure the avionics software integrity. The standard and associated guidelines were created to identify and document the "best known" software practices supporting the certification of software-based equipment and systems, thus proving a basis for software certification approval.

Food and Drug Administration (FDA) established procedures for medical software regulation. FDA regulates the industry which includes the software in the medical devices. It focus on the systems with the highest risks to the patients. A thorough evaluation of medical software products includes the evaluation of the system structure (interface, algorithms, and behavior), its function and its impact. The involvement of medical professionals is of critical importance.

Closing remarks

It was pointed out that effective testing of safety critical software system is difficult or impossible, when the size of the software is meaningful. The difficulties include such issues:

- 100 % test coverage requires far too many resources.
- Black box testing can not possibly find all errors.
- The user can (in principle) sue the producer for insufficient testing of its software.

Considering the drawbacks, to effectively insure high reliability in safety critical systems, one has to rely on verification, validation and certification of not only the software product, but also the software processes and personnel. Best practices for developing safety critical systems must be identified, developed and researched on and software processes must be clearly defined to effectively organize and improve upon the uses of the best practices.