SOFTWARE SAFETY IN MEDICAL APPLICATIONS

John C. Knight, Kevin G. Wika

Department of Computer Science
University of Virginia
Charlottesville, VA 22903
knight@Virginia.EDU
wika@Guidant.COM

Abstract

The use of software in safety-critical medical applications permits sophisticated functionality that would otherwise not be achievable. However, it is very difficult to ensure that software in these systems is dependable. In particular all software development techniques have limitations and none can provide any guarantee of overall software dependability. Given this shortcoming, the approach that we have taken is to develop techniques that emphasize the verification of properties that are important to overall software dependability. In this paper we describe two techniques that support the implementation and verification of dependable software for an experimental neurosurgical device and safety-critical applications in general.

The first technique involves the assurance of critical safety properties by a relatively simple software component known as a safety kernel. Situated between the application software and the application devices, the safety kernel enforces rules that govern the safe operation of the devices. The simplicity of the safety kernel facilitates its implementation and verification.

In most cases, it is not possible to rely upon testing to provide the necessary verification of the software in a safety-critical application. However, testing can perform an appropriate and vital role in the demonstration of safety properties. The second technique takes this approach utilizing automated testing and selected test cases to demonstrate useful system properties.

Keywords: Software dependability, software testing, software verification, dependability assessment, software fault tolerance, safety kernel

This document is protected by copyright that is held by the publishers of the Journal of Image Guided Surgery.

The document can be obtained from the journal.