Universitè de Lorraine

Erasmus Mundus

Dependable Software Systems

Design Patterns in Event-B

Author:
Anders Olav
Candasamy

Supervisor:
Dominique Méry

April 12, 2016

1 Definitions

Machine ==¿ Hemodialysis machine

2 Variables

This section will detail various techniques that have been used to extract the required Event-B variables from the requirements.

2.1 Variable categories

In the case of the hemodialysis machine, there are a large amount of variables. This can be confirmed by reading the case study by in [x]. The variables required can be grouped into different categories. Categorising these variables can greatly help in improving our knowledge of the system. The concrete definition of the categories are left informal. We want our

Controlled are variables that the system has full control over

Monitored are variables that can only be observed and not directly modified.

User Input are monitored variables inserted by a nurse. Strictly $UserInput \subseteq Monitored$

Timed are monitored variables that have a dependency on time. Strictly $Timed \subseteq Monitored$

The two major categories of interest are the *controlled* and *monitored* variables. The User Input category is created to separate the internally monitored variables from the variables set by a nurse. This is done because the list of variables added by a nurse is such a large percentage of total variables. We have also decided to separate the monitored variables that include an element of time. As Event-B does not directly support time, we will extract them to their own category. These timed variables will be added at the very last machine refinement.

An example of a *controlled* variable is our blood pump. The software is in full control of what the state of the pump should be. An example of a monitored variable is the *blood flow direction*. Although we directly control

the pump, we do not control the blood flow direction. A *controlled* variable modifies the *environment* that again modifies the *monitored* variables. An argument could be made that the if the pump is on, it is guaranteed that the blood flows rotation is positive. This is however making assumptions about the system that we do not know. In any case, our paper will define *controlled variables* as the variables the system has full, and direct control over.

The idea of splitting variables into Controlled and Monitored came from reading [x]. Although Parnas presented this as a minor point in his paper, it is an interesting approach with regards to Event-B. This list is not an exhaustive list as other machines may require additional categories.