

Design and Verification of Medical System Control Software for Philips Medical Systems

Successful pilot leads to further deployment of ASD



The simple way to build
complex software
systems

Verum's Analytical Software Design (ASD) combines the practical application of software engineering mathematics and modelling with specification methods that avoid difficult mathematical notations and that remain understandable to all project stakeholders.

In a pilot project for Philips Medical Systems (PMS) ASD was applied to the design and verification of the controller software for a medical scanner. The purpose of the pilot project was to demonstrate the added value of ASD to the development of software for a typical PMS product. In particular PMS sought answers to the following two questions:

- **Are formal methods mature enough to be used in practice?**
- **Can PMS apply ASD on a large scale?**

The Project

The pilot was loosely based on the requirements for the controller of a new scanner under development in PMS. The pilot remit did not require the production of running code but did require code generation for key components.

The controller design was decomposed into 6 components of which 4 key components were fully designed and verified. The design was of moderate complexity, the components possessing a total of 75 states and 410 legal state transitions; 10 interfaces with 170 stimuli and responses. A change request was included in the pilot to assess ASD's flexibility. The generated code size was estimated to be about 16000 LOCs. The project lasted 10 weeks, the effort expended was 70 man days.

PHILIPS

Design and Verification of Medical System Control Software for Philips Medical Systems

Results and Conclusion

Verification of the design covered in excess of 1.5 million execution scenarios and the use of ASD resulted in the discovery of 44 defects of which 50% were considered serious design defects.

System Size and Complexity

- Designs for 4 components completed
- 10 interfaces specified - 6 external
- 170 Stimuli & Responses - 100 external
- Total 75 states & 410 legal transitions
- Code Size 16000 LOC (estimated)

Verification Results

- Verified over 1.5 million scenarios
- Discovery of 44 defects
- Removed defect density 3.5 / kLOC

Customer Findings

- | | | |
|----------------------------------|---|----|
| • Understandability of ASD Specs | ▶ | + |
| • Reliability | ▶ | ++ |
| • Incremental Development | ▶ | + |
| • Knowledge (Customer) | ▶ | = |

Customer Conclusion

"ASD is a powerful, promising and ready to use method in industry."

Questions Answered

In answer to the questions posed at the beginning of the pilot, the project reviewer, Daniela Dupré (Software Designer, PMS) concluded:

Are formal methods mature enough to be used in practice?

- Yes, ASD is quite a powerful and yet understandable tool

This case study is based on work completed in 2006. Since that time PMS has proceeded with a full-scale deployment of ASD.

For more information see: www.verum.com

Copyright © 2008 Verum