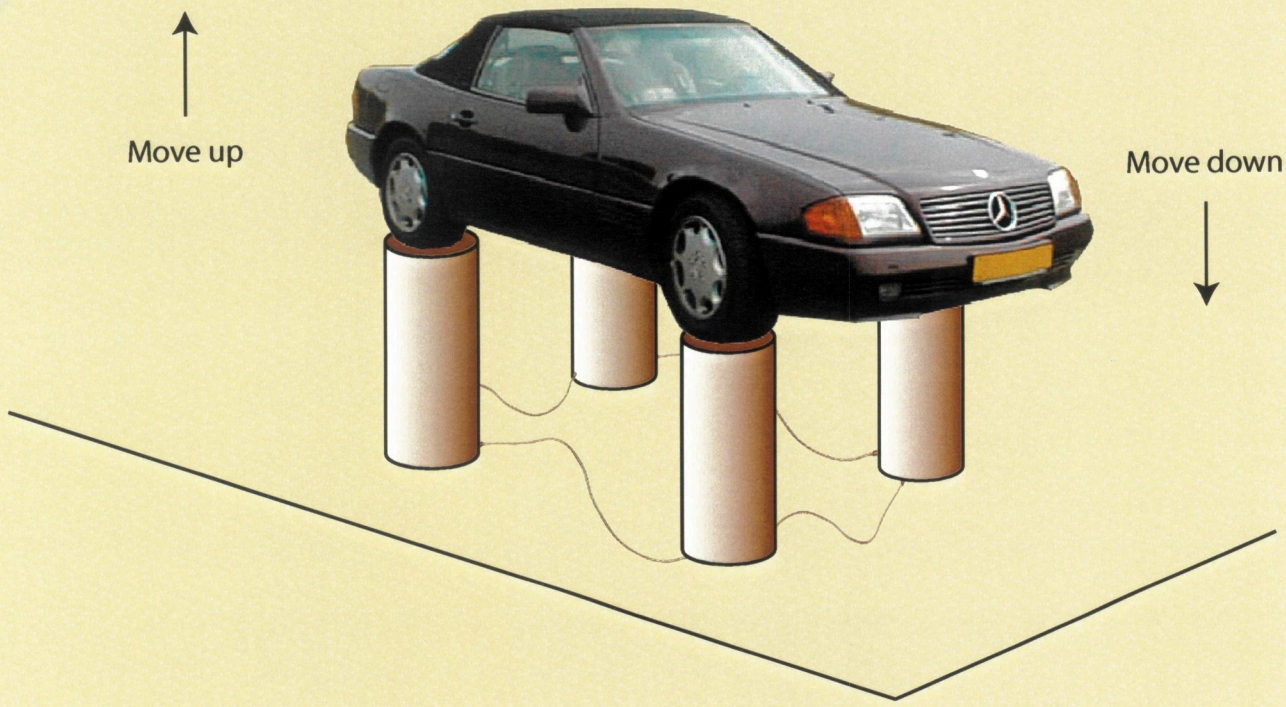
Centrum voor Wiskunde en Informatica

A Balancing Act: Analyzing a Distributed Lift System



Abstract

This paper reports on the analysis of a real-life system for lifting trucks. When testing the implementation the developers found three problems. They solved these problems in an ad hoc manner, although the causes of two of the three problems were unclear. Moreover, the developers were unsure that there were no other bugs hidden in the system. We specified the lift system in μCRL. Next, we analyzed the resulting specification with the μCRL tool set and the CÆSAR ALDÉBARAN DEVELOPMENT PACKAGE (CADP). The three known problems turned up in our specification. In addition we found a fourth error. This error was unknown and found its way into the implementation. We have analyzed the μCRL specification that results from the incorporation of the proposed solutions, showing that this specification meets the requirements by means of model checking.

Keywords

μCRL, distributed system, model checking, process algebra, specification and verification.

Conclusion

The presented case study demonstrates that by using formal specification and verification techniques, an improvement of such protocols and their implementations is possible.

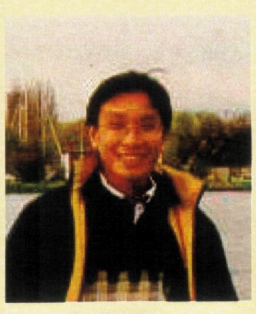
Website

http://www.cwi.nl/~mcrl/lift/

Participants

Prof.dr.ir. J.F. Groote[1]

Prof.dr. W.J. Fokkink[2]



Drs. J. Pang[2]

Dr. A.G. Wouters[2]

[1]Eindhoven University of Technology
[2]Center for Mathematics and Computer Science, Amsterdam

Note

This research is supported by the Dutch Technology Foundation STW under the project STW CES5008: Improving the quality of embedded systems by formal design and systematic testing.