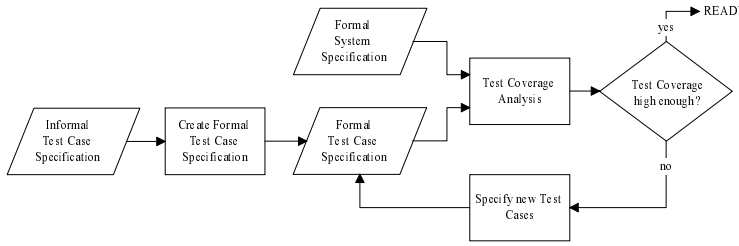
Formal Specification of a Voice Communication System Used in Air Traffic Control

An Industrial Application of Light-Weight Formal Methods Using VDM^{++}

Johann Hörl and Bernhard K. Aichernig

Technical University Graz, Institute for Software Technology (IST),
Münzgrabenstr. 11/II, A-8010 Graz, Austria
{jhoerl|aichernig}@ist.tu-graz.ac.at

A joint project of the Austrian company Frequentis[1] and the Technical University Graz demonstrates the applicability of executable formal models[2]. The formal method VDM^{++} has been applied to specify a safety critical voice communication system (VCS) for air-traffic control. Besides the expected improvement of the informal specification documents, 64 defects have been found, the efficiency of the system test-cases to cover the functionality of the VCS has been analyzed. In order to get a test-coverage measure, the formal specification has been animated with existing system test-cases using IFAD's VDMTools. A



main result of this work was the realization that only 80% of the system's radio functionality had been covered by the former existing test cases. Consequently, additional test cases have been derived from the formal specification. In addition, the specification high-lighted how much more economic test cases could be designed, in order to cover more system functionality in a single run. Furthermore, an existing change request has been chosen in order to investigate the role of an explicit model in the modification process. It turned out that the low abstraction level of an executable specification is certainly an advantage in analysing the impacts of change-requests: Since the object-oriented VDM^{++} model reflected the system's architecture, the impacts on the different components could be analyzed in the model. A further experience is that VDM's well-known refinement concepts, such as retrieve functions, are well suited to design the modifications.

[1] http://www.frequentis.co.at/

[2] See also ftp://www.ist.tu-graz.ac.at/pub/publications/IST-TEC-99-03.ps.gz

J. Wing, J. Woodcock, J. Davies (Eds.): FM'99, Vol. II, LNCS 1709, pp. 1868–1868, 1999.