Will This Be Formal?

Steven P. Miller*

Advanced Technology Center, Rockwell Collins,
400 Collins Rd NE, Cedar Rapids, Iowa 52498
spmiller@rockwellcollins.com

Abstract. While adding formal methods to traditional software development processes can provide very high levels of assurance and reduce costs by finding errors earlier in the development cycle, there are at least four criteria that should be considered before introducing formal methods into a project. This paper describes five successful examples of the use of formal methods in the development of high integrity systems and discusses how each project satisfied these criteria.

Keywords: Formal methods, model checking, theorem proving, avionics.

1 Introduction

Adding formal methods to traditional software development processes can provide very high levels of assurance and reduce costs by finding errors earlier in the development cycle. However, to be successful there are at least four criteria that should be considered before introducing formal methods into a project. This paper describes five successful examples of the use of formal methods in industry and discusses how each of the five projects satisfied these criteria.

2 Examples of the Successful Use of Formal Methods

This section describes five successful examples of the use of formal methods in the development of high integrity systems. In three projects model checking was used to verify the functional correctness of Simulink® models. In two projects theorem proving was used to verify security properties of microcode and source code.

2.1 FCS 5000 Flight Control System

One of the first applications of model checking at Rockwell Collins was to the mode logic of the FCS 5000 Flight Control System [1]. The FCS 5000 is a family of Flight Control Systems for use in business and regional jet aircraft. The mode logic determines

---

* This work was supported in part by the NASA Langley Research Center under contract NCC-01001 of the Aviation Safety Program (AvSP), the Air Force Research Lab under contract FA8650-05-C-3564 of the Certification Technologies for Advanced Flight Control Systems program (CerTA FCS) and the Air Force Research Lab under the EISTS program Delivery Order 4.
which lateral and vertical flight modes are armed and active at any time. While inherently complex, the mode logic consists almost entirely of Boolean and enumerated types and is written in Simulink. The mode logic analyzed consisted of five inter-related mode transition diagrams with a total of 36 modes, 172 events, and 488 transitions.

Desired properties of the mode logic were formally verified using the NuSMV model checker. To accomplish this, the Simulink models were automatically translated into NuSMV using a translation framework developed by Rockwell Collins and the University of Minnesota. This same translation framework also optimized the models for efficient analysis by the NuSMV BDD-based model checker.

Analysis of an early specification of the mode logic found 26 errors, seventeen of which were found by the model checker. Of these 17 errors, 13 were classified by the FCS 5000 engineers as being possible to miss by traditional verification techniques such as testing and inspections. One was classified as being unlikely to be found by traditional verification techniques.

2.2 ADGS-2100 Adaptive Display and Guidance System

One of the most complete examples of model checking at Rockwell Collins was the analysis of the Window Manager logic in the ADGS-2100 Adaptive Display and Guidance System [2]. The ADGS-2100 is a Rockwell Collins product that provides the display management software for next-generation commercial aircraft. The Window Manager (WM) is a component of the ADGS-2100 that ensures that data from different applications is routed to the correct display panel, even in the event of physical failure of one or more components.

Like the FCS 5000 mode logic, the WM is specified in Simulink and was verified by translating it into NuSMV and applying the NuSMV model checker. While the WM contains only Booleans and enumerated types, it is still quite complex. It is divided into five main components that contain a total of 16,117 primitive Simulink blocks that are grouped into 4,295 instances of Simulink subsystems. The reachable state space of the five components ranges from $9.8 \times 10^9$ to $1.5 \times 10^{37}$ states.

Ultimately, 593 properties about the WM were developed and checked, and 98 errors were found and corrected in early versions of the model. As with the FCS 5000 mode logic, this verification was done early in the design process while the design was still changing. While the verification was initially performed by formal methods experts, by the end of the project, the WM developers themselves were doing virtually all the model checking.

2.3 Lockheed Martin Operational Flight Program

The Air Force Research Labs (AFRL) sponsored Rockwell Collins to apply model checking to the Operational Flight Program (OFP) of an Unmanned Aerial Vehicle developed by Lockheed Martin Aerospace as part of the CerTA FCS project [3]. The OFP is an adaptive flight control system that modifies its behavior in response to flight conditions. Phase I of the project concentrated on applying model checking to portions of the OFP, specifically the Redundancy Management (RM) logic, which were well suited to analysis with the NuSMV model checker. While relatively small (the RM logic consisted of three components containing a total of 169 primitive