Summary of Research and Collaboration Agreement between FDA and MathWorks

Either party may release this summary page to the public without further consultation or permission.

TITLE OF RCA Project:	Research on Applying Model-Based Design and Formal Verification Techniques to Medical Device Software Development
FDA Office/Center:	Center for Devices and Radiological Health
FDA Principal Investigator:	Mr. Paul Jones
Collaborator Organization:	MathWorks
Collaborator Principal Investigator:	Arvind Ananthan
TERM OF RCA:	Five (5) years from the effective date

Abstract of the Research Plan

Software has become ubiquitous in medical devices; a pacemaker contains upward of 80,000 lines of code while an MRI machine contains over 7 million lines of code. Software accounts for approximately 24% of adverse events recorded in FDA's Maude data base.

The primary goal of this research plan is to explore model-based design and formal verification techniques as applied to medical device design. These design techniques have been in use in other high-integrity industries such as aerospace and automotive for many years now. Only recently, in large part due to the efforts of CDRH/OSEL/DESE research and collaborations, such as with MathWorks, has the medical device industry has been looking at adopting these approaches to improve their software development process while achieving the desired quality and time-to-market goals for a high integrity safety critical applications.

The activities planned as part of this research collaboration fall into two primary categories:

1. Investigation of Model-Based Design/ Model-Based Engineering (MBD/MBE) approaches to design, verify, and validate medical device software. This includes formal analysis of the designs at the model level to facilitate analysis of the design for properties of completeness and consistency.
2. Exploration of formal verification techniques to prove presence or absence of errors, and provide a framework to verify software quality throughout the software development and maintenance/evolution process. Artifacts of these engineering processes can be used as measures of device (software) quality as well as methods by which to continuously improve software quality. They may also serve as a basis for certification schemes.

Research envisioned under this plan is broadly applicable to any medical device that contains software. It is expected to provide actionable guidance to engineers on specific techniques that can improve various aspects of the device design process. It is particularly relevant to (CDRH) regulators in that it describes a new scalable approach using graphical models to assist in reviewing portions of design submissions and is expected to provide measures of device quality that a reviewer can assess in both a pre-market and post-market context to help establish confidence that a device will perform as intended.

Research issues to be explored, based upon resource availability, include abstracting design requirements as executable (graphical) models, simulation of designs to explore dependability and robustness, connectivity between model elements and requirements, functional and formal verification of the model, property proving using formal methods to prove/disprove safety requirements, automatic implementation of models into code, verification of design implementations on target hardware, static analysis, automatic report generation for evidence of standard(s)/regulation(s) compliance, closed-loop physiological systems, real-time design and performance issues, and (safety) assurance cases.

MathWorks®
Accelerating the pace of engineering and science

mathworks.com