MODEL DRIVEN DEVELOPMENT FOR MEDICAL DEVICES IN AADL/BLESS AND SPARK/ADA: PCA PUMP PROTOTYPE

by

Jakub Jedryszek

B.S., Wroclaw University of Technology, Poland, 2012

B.A., Wroclaw University of Economics, Poland, 2012

A THESIS

submitted in partial fulfillment of the
requirements for the degree

MASTER OF SCIENCE

Department of Computing and Information Sciences
College of Engineering

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2014

Approved by:

Major Professor
John Hatcliff

Copyright

Abstract

Ada programming language is targeted at embedded and real-time systems.

SPARK/Ada is designed for the development of safety and security critical systems. It contains properties, which allows to prove corectness of program and its entities.

AADL (Architecture Analysis & Design Language) is modeling language for representing hardware and software. It is used for real-time, safety critical and embedded systems.

BLESS (Behavior Language for Embedded Systems with Software) is AADL annex sub-language defining behavior of components. The goal of BLESS is automatically-checked correctness proofs of AADL models of embedded electronic systems with software.

Nowadays, we have trend to generate code from models. The ultimate goal of research, which this thesis if part of, is to create AADL/BLESS to SPARK/Ada traslator. Ultimatelly there will be standarized AADL/BLESS models, which will be generating code base for developers extensions (like sceleton code for some Web Framework).

Medical Devices are very important part of High-Assurance systems.

This thesis propose mapping from AADL/BLESS to SPARK/Ada. As an example of Medical Device, PCA Pump (Patient Controlled Analgesia) is used. The foundation for this work is System Requirements for "Integrated Clinical Environment Patient-Controlled Analgesia Infusion Pump System Requirements" (DRAFT 0.10.1) [Lar14] and AADL Models with BLESS annexes created by Brian Larson. Additionally, there was a contribution made in clarifying the requirements document and extending AADL models.

Table of Contents

List of Figures

List of Tables

Acknowledgments

Say thank you for everybody involved directly and indirectly.

Dedication

For my family, mentors and all people who inspired me directly or indirectly in things I am doing.

I also dedicate this thesis to everyone who have supported me throughout the process.

Chapter 1

Introduction

The tale about software safety: why important, software everywhere, human life, etc. (info from 890).

Software Engineering for Real-Time and Safety-Critical systems is very different than creating Desktop applications. In both types of software we want to ensure correctnes and security. In case of e.g. e-mail client software assurance is not crucial. When something happend, we just restart the app. However, in case of e.g. Airplane, software cannot just crash. If it crashes, then people dies. Behind these reasons, we need different properties of our programming language and its tools. For Web or Mobile apps our priority is Rapid Development. For Safety-Critical systems, security is crucial.

1.1 Motivation

There are many accidents where Medical Devices are involved. Very often, the reason is the lack of communication between different Medical Devices. [EXAMPLE ACCIDENT] The solution for such a problem is to create "Integrated Clinical Environment" (ICE). SAnToS Lab at Kansas State University is working on Medical Device Coordination Framework

(MDCF), which is prototype implementation of ICE.

Devices working under MDCF will need to satisfy some requirements. To make Developer's life easier, the requirements will be not only in documentation, but also in code. The code will be generated from models. Model Driven Development in this case means we will have some base models for medical devices development and developer will extend and customize them. The same like you do File > 'New Java project' in Eclipse, we want to be able to do the same in e.g. GNAT Programming Studio: File > 'New Medical device project'. Model as specification/requirements.

PCA Pump is as an example of Medical Device, which ultimately will work under Medical Device Coordination Framework (MDCF) developed by SAnToS Lab at Kansas State University. Summarizing, we want to be able to have MDCF, which coordinates Medical Devices. Additionally we want set of AADL/BLESS models, which can be automatically translated to SPARK/Ada. These models will be base for Medical Devices Developers, who can extend and adjust them to implement specific devices. Why AADL? Because it describes hardware and software. It allows to validate that the software will work on some device. Why SPARK? Because it is subset, which is easy to deal with it. In the future, when everything will be done (in case of proving perspective) in SPARK, it will (probably) be extended. Maybe finally, there will be no SPARK, but only Ada. Thus for now, SPARK is temporary subset of Ada for reasoning and corectness proving.

1.2 Contribution

Put all piecies together (SPARK, AADL, BLESS?, ICE, PCA Pump) and analyze current state of target technologies. Review PCA Pump Requirements document Implement PCA Pump based on document, by resolving ambiguities and analyzing different implementation possibilities. Then the implementation is sort of proof that, this document might be base for future Infusion Pumps and/or Medical Devices implementations. Analyzed and extended

PCA Pump AADL models, then based on available resource propose possible translation from AADL/BLESS to SPARK/Ada. Created AADL/BLESS to SPARK/Ada translator.

1.3 Organization

The thesis is organized in 6 chapters. Chapter 1 is the of the problem and summary of contribution which was made. Chapter 2 is Background that gives details about Model Driven Development, SPARK/Ada, AADL/BLESS, ICE and available tools for such environment. Chapter 3 describes the implementation of PCA Pump Prototype. Faced issues and design decisions made. Chapter 4 is about code generation from the model. Chapter 5 summarizes all work which has been done in this thesis. Chapter 6 is the future work that can be done on this topic.

Chapter 2

Background

This chapter is brief introduction of all technologies and tools used in this thesis. It is SPARK/Ada programming language and its tools (GNAT Programming Studio, Sireum Bakar, GNATprove), AADL modeling language, BLESS (AADL annex language). There is also overview of the context in which this work has been made: Integrated Clinical Environment standard (ICE) and PCA Pump (ICE compliant device). This is followed by main topic of the thesis: code generation from AADL and analysis of existing AADL translators (Ocarina, RAMSES).

2.1 Integrated Clinical Environment

Medical devices are safety-critical systems. http://santos.cis.ksu.edu/MDCF/doc/ICE-Motivation.pdf http://santos.cis.ksu.edu/MDCF/doc/MDCF-Tutorial-Overview.pdf MDCF conforms to ICE standards. Medical Devices, which are ICE compliant can be connected to MDCF. It enable many Medical Devices cooperation.

2.2 AADL

AADL stands for Architecture Analysis & Design Language. The aim of the AADL is to allow the description of Distributed Real-Time Embedded (DRE) systems by assembling separately developed blocks. Thus it focuses on the definition of clear block interfaces, and separates the implementations from those interfaces. AADL allows for the description of both software and hardware parts of a system [1].

AADL is a language for Model-Based Engineering [FG13].

2.2.1 Osate

OSATE is a set of plug-ins on top of the open-source Eclipse platform to provide a toolset for front-end processing of AADL models. It is developed mainly by SEI (Software Engineering Institute - CMU).

2.3 BLESS

How it fits into the picture. Why it was developed. Corectness prove in AADL + behavior [LCH13], from which we can generate SPARK/Ada code.

2.4 SPARK/Ada

First version of Ada programming language, Ada 83 was designed to meet the US Department of Defence Requirements formalized in "Steelman" document [2]. Since that time, Ada evolved. There were Ada 95, Ada 2005 and now we have Ada 2012 (released in December 10, 2012) [3]. Ada is activelly used in many Real-World projects, e.g. Aviation, Railway Transportation, Commercial Rockets, Satellites and even Banking [Fel12].

[1] http://penelope.enst.fr/aadl
[2] http://www.adahome.com/History/Steelman/steelman.htm
[3] http://www.ada2012.org

SPARK is a programming language and static verification technology designed specifically for the development of high integrity software. First designed over 20 years ago, SPARK has established a track record of use in embedded and critical systems across a diverse range of industrial domains where safety and security are paramount [Bar13].

SPARK provides a significant degree of automation in proving exception freedom [IEC+06]. SPARK excludes some Ada constructs to make static analysis feasible [IEC+06]. First version of SPARK was based on Ada 83. SPARK 2005 is based on Ada 2005. It includes annotation language that support flow analysis and formal verification. Annotations are encoded in Ada comments (via the prefix `--#`). It makes every SPARK 2005 programm, valid Ada 2005 program.

```
package Odometer
--# own Trip, Total : Integer;
is
   procedure Zero_Trip;
   --# global out Trip;
   --# derives Trip from ;
   --# post Trip = 0;

   function Read_Trip return Integer;
   --# global in Trip;

   function Read_Total return Integer;
   --# global in Total;

   procedure Inc;
   --# global in out Trip, Total;
   --# derives Trip from Trip & Total from Total;
   --# post Trip = Trip~ + 1 and Total = Total~ + 1;

end Odometer;
```

Listing 2.1: *SPARK 2005 code: Odometer [Bar13]*

SPARK 2014 [4] is based on Ada 2012 programming language targeted at safety- and security-critical applications [DEL+14]. Since Ada 2012 contains contracts, there is no need to use annotations like in SPARK 2005. Thus SPARK 2014 is subset of Ada 2012. It contains all features of Ada 2012 except:

- Access types (pointers)
- Exceptions
- Aliasing between variables
- Concurrency features of Ada (Tasking)
- Side effects in expressions and functions

The notion of executable contracts in Ada 2012, was inspired by SPARK.

It is possible to mix SPARK 2014 with Ada 2012. However, only the part which is SPARK 2014 compliant will be verified.

The most popular IDE for SPARK/Ada is GNAT Programming Studio [5].

There is also plugin for Eclipse: GNATbench [6] created by AdaCore. Tools for corectness proving.

2.4.1 GNAT Programming Studio

IDE for SPARK/Ada programs development. Includes proving tools. E.g. Sireum Kiasan (developed by SAnToS lab) or GNAT Prove.

[4] http://www.spark-2014.org
[5] http://libre.adacore.com/tools/gps
[6] https://www.adacore.com/gnatpro/toolsuite/gnatbench/

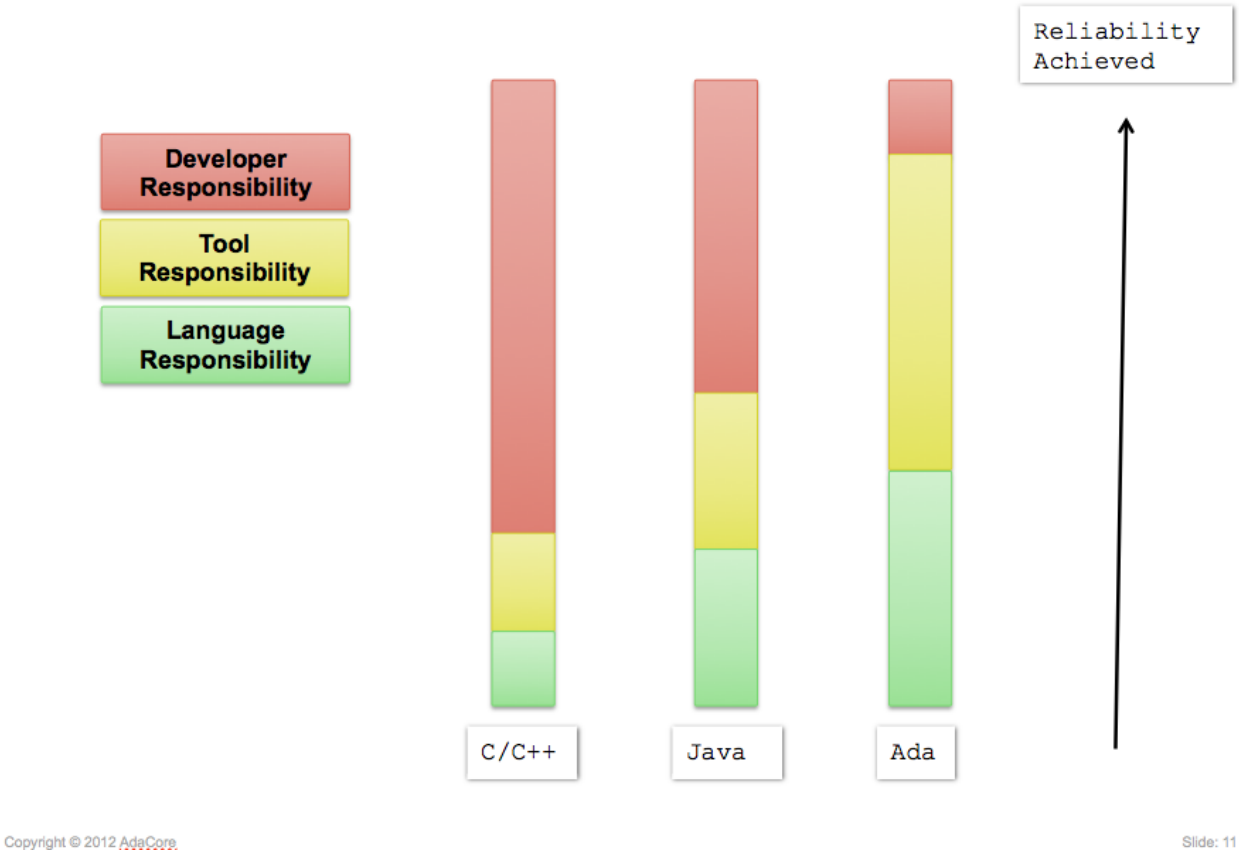

Figure 2.1: *Developer responsibility in Ada.*

2.4.2 Sireum Bakar

Overview: symbolic execution, Pilar, Kiasan and Alir [Thi11]. Sireum Kiasan [BHR+11] is a tool, which use symbolic execution for finding possible paths in program. Plugin for GNAT Programming Studio. Plugin for Eclipse (but only SPARK 2005).

2.4.3 GNAT Prove

GNATprove [7] is a formal verification tool for SPARK/Ada programs. It interprets SPARK/Ada annotations exactly like they are interpreted at run time during tests.

[7] http://www.open-do.org/projects/hi-lite/gnatprove/

2.4.4 AUnit

Overview AUnit tutorials [Fal14] AUnit Cookbook [Ada14]

2.5 PCA Pump

http://www.santoslab.org/pub/paper/LarsonEtAl13-PCA-Requirements-SEHC-preprint.pdf

2.6 AADL/BLESS to SPARK/Ada code generation(maybe translation is better word?)

The ultimate goal of long term research, this thesis is part of. AADLto Ada BLESS to SPARK contracts + (eventually) behavior

2.6.1 Ocarina

Ocarina [LZPH09, LZPH09] generates code from an AADL architecture model to an Ada application running on top of PolyORB framework. In this context, PolyORB acts as both the distribution middleware and execution runtime on all targets supported by PolyORB. It generate Ada 2005 and C code. Since mid-2009, Telecom ParisTech is no longer involved in Ocarina, and is developping another AADL toolchain, based on Eclipse, codenamed RAMSES [Hug13].

2.6.2 Ramses

RAMSES is a model transformation framework dedicated to the refinement of AADL models.

Chapter 3

PCA Pump Prototype

Overview of PCA Pump and issues, which MDCF/ICE will solve.

3.1 PCA Pump Requirements Document

Selected use cases for implementation?

3.2 PCA Pump AADL/BLESS Models

Selected modules for implementation. Pictures etc.

3.3 BeagleBoard-XM

First step was create PCA Pump prototype on BeagleBoard-xM.

BeagleBoard-xM is Embedded device with AM37x 1GHz ARM processor (Cortex-A8 compatible). It has 512 MB RAM, 4 USB 2.0 ports, HDMI port, 28 General-purpose input/output (GPIO) ports and Linux Operating System (on microSD card). All these properties makes this device good candidate for prototyping PCA Pump.

There is no existing SPARK/Ada compiler running on ARM system. Hence, to compile SPARK/Ada program for ARM device, we need to perform cross-compilation on other machine. There is GNAT compiler [Hor09] created by AdaCore, but there was no cross-compiler for ARM. However AdaCore was working on it. They had working version in 2013, but tested only on their target, Android-based device. BeagleBoard-xM is coming with Linux Angstrom Operating System. There is possibility to install Android on BeagleBoard-xM, but still not warranty everything will be working. Cooperation with AdaCore allowed to cross-compile SPARK/Ada program for BeagleBoard-xM.

Include source of simple program? GNAT cross-compiler only for Linux Platform (cross-compilation has to be done on Linux).

3.4 PCA Pump Prototype Implementation

Currently SPARK 2014 does not support tasking [AL14]. For SPARK 2005, GNAT compiler provides Ravenscar Profile [Tea10]. It provides a subset of the tasking facilities of Ada95 and Ada 2005 suitable for the construction of high-integrity concurrent programs.

Issues: Ravenscar Profile, how to deal with different boluses (look at UMinn requirements and annotations for our doc). Look at annotated PCA Pump Req document.

Chapter 4

AADL/BLESS to SPARK/Ada translation

First step was to create mock (based on doc, aadl models and implemented PCA Pump). Prototyping Embedded Systems using AADL lasts for a few years [CB09].

4.1 Extention of exisitng PCA Pump AADL models

I added Subprograms etc. How I did it. Code examples.

4.2 AADL/BLESS to SPARK/Ada mapping

Mapping is driven by Ocarina and "Architecture analysis & Design Language (AADL) V2 Programming Language Annex Document" [SCD13]. Only high level mapping is done. No implementation (thread interactions) like Ocarina does.

Table, how specific constructs (subset) in AADL/BLESS are translated to SPARK/Ada.

Table 4.1: *AADL to SPARK mapping.*

AADL/BLESS	SPARK/Ada

subprogram sp
features
  e : **in parameter** T;
  s : **out parameter** T;
end sp;
	procedure sp(e : **in** T; s : **out** T) **is**
	begin
	  null;
	end sp;

data Flow_Rate --dose rate
  properties
  BLESS::Typed=>"integer";
  Data_Model::Base_Type => (
  classifier(Base_Types::Integer_16));
  Data_Model::Measurement_Unit => "ml
  /hr";
end Flow_Rate;
	subtype Flow_Rate **is** Integer **range** 0 ..
	  Integer'Last;

Table 4.2: *BLESS to SPARK contractsmapping.*

AADL/BLESS	SPARK/Ada
BLESS::Assertion=>"<<VP()>>"	--# pre VP; --# post VP;
<<Pre()>>Action()<<Post()>>	**procedure** Action; --# pre Pre; --# post Post;

4.3 "DeusEx" translator

AADL/BLESS to SPARK/Ada translator in Scala. Main idea. Maybe at least create base: AADL to AST covertion?

Chapter 5

Summary

What I have done.

Chapter 6

Future work

What has to be done now.

The semantics of BLESS contain notions of time that make translation to SPARK difficult.

Bibliography

[Ada14] AdaCore. Aunit cookbook. URL: http://docs.adacore.com/aunit-docs/aunit.html, Mars 2014.

[AL14] AdaCore and Altran UK Ltd. Spark 2014 reference manual. URL: http://docs.adacore.com/spark2014-docs/html/lrm, 2011-2014.

[Bar13] John Barnes. *SPARK - The Proven Approach to High Integrity Software*. Altran, 2013.

[BHR+11] Jason Belt, John Hatcliff, Robby, Patrice Chalin, David Hardin, and Xianghua Deng. Bakar kiasan: Flexibe contract checking for critical systems using symbolic execution. In *NASA Formal Methods*, pages 58–72. Springer Berlin Heidelberg, 2011.

[CB09] Mohamed Yassin Chkouri and Marius Bozga. Prototypying of distributed embedded systems using aadl. In *ACESMB 2009, Second International Workshop on Model Based Architecting and Construction of Embedded Systems*, pages 65–79. Springer Berlin Heidelberg, 2009.

[DEL+14] Claire Dross, Pavlos Efstathopoulos, David Lesens, David Mentre, and Yannick Moy. Rail, space security: Three case studies for spark 2014. In *ERTS 2014: Embedded Real Time Software and Systems*, 2014.

[Fal14] Ed Falis. Aunit tutorials. URL: http://libre.adacore.com/tools/aunit, Mars 2014.

[Fel12] Michael B. Feldman. Who's using ada? real-world projects powered by the ada programming language. URL: http://www.seas.gwu.edu/~mfeldman/ada-project-summary.html, 2012.

[FG13] Peter H. Feiler and David P. Gluch. *Model-Based Engineering with AADL*. Addison-Wesley, 2013.

[Hor09] Bartłomiej Horn. Ada'05 compiler for arm based systems. thesis, Technical University of Lodz, Poland, 2009.

[Hug13] Jérôme Hugues. About ocarina. URL: http://www.openaadl.org/ocarina.html, 2013.

[IEC+06] Andrew Ireland, Bill J. Ellis, Andrew Cook, Roderick Chapman, and Janet Barnes. An integrated approach to high integrity software verification. *Journal of Automated Reasoning*, 36(4):379–410, Avril 2006.

[Lar14] Brian R. Larson. Integrated clinical environment patient-controlled analgesia infusion pump system requirements draft 0.10.1, Février 2014.

[LCH13] Brian R. Larson, Patrice Chalin, and John Hatcliff. Bless: Formal specification and verification of behaviors for embedded systems with software. In *NASA Formal Methods*, pages 276–290. Springer Berlin Heidelberg, 2013.

[LZPH09] Gilles Lasnier, Bechir Zalila, Laurent Pautet, and Jérôme Hugues. Ocarina : An environment for aadl models analysis and automatic code generation for high integrity applications. In *Reliable Software Technologies – Ada-Europe 2009*, pages 237–250. Springer Berlin Heidelberg, 2009.

[SCD13] SAE AS-2C Architecture Description Language Subcommittee, Embedded Computing Systems Committee, and Aerospace Avionics Systems Division. Aerospace

standard - architecture analysis & design language (aadl) v2 programming language annex document, 2013.

[Tea10] SPARK Team. The spark ravenscar profile. URL: http://docs.adacore.com/sparkdocs-docs/Examiner_Ravenscar.htm, 2010.

[Thi11] Hariharan Thiagarajan. Dependence analysis for inferring information flow properties in spark ada programs. thesis, Kansas State University, 2011.

Appendix A

Title for This Appendix

Content of this appendix.

Appendix B

Title for This Appendix