Association for Computing Machinery

Advancing Computing as a Science & Profession

HILT 2014: HIGH INTEGRITY LANGUAGE TECHNOLOGY

ACM SIGAda's Annual International Conference

Co-Located with OOPSLA/SPLASH 2014

October 18–21, 2014 / Portland, Oregon / Final Program

High integrity software must not only meet correctness and performance criteria but also satisfy stringent safety and/or security demands, typically entailing certification against a relevant standard.

A significant factor affecting whether and how such requirements are met is the chosen language technology and its supporting tools: not just the programming language(s) but also languages for expressing specifications, program properties, domain models, and other attributes of the software or overall system.

HILT 2014 will provide a forum for experts from academia/research, industry, and government to present their latest findings in designing, implementing, and using language technology for high integrity software.

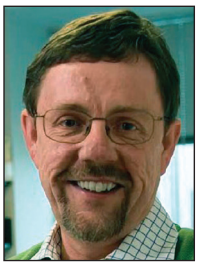
HILT attendees are invited to attend the SPLASH opening keynote address by Gary McGraw, CTO of Cigital, Inc. and author of *Software Security*.

Sponsored by SIGAda, ACM's Special Interest Group on the Ada Programming Language, in cooperation with SIGAPP, SIGBED, SIGCAS, SIGCSE, SIGPLAN, SIGSOFT, Ada-Europe, and the Ada Resource Association.

FEATURED SPEAKERS

Correctness via Compilation to Logic
THOMAS BALL
Microsoft Research

From Ada 9X to Spaceport America: Going Where No One Has Gone Before
CHRISTINE ANDERSON
Spaceport America



AADL and Model-Based Engineering
PETER FEILER
Software Engineering Institute/
Carnegie Mellon University

CORPORATE SPONSORS

PLATINUM LEVEL

AdaCore
The GNAT Pro Company

GOLD LEVEL

Microsoft Research

SILVER LEVEL

Ellidiss Software
TNI Europe Limited

BASIC LEVEL

MathWorks

CONTENTS

CONFERENCE TEAM

Conference Chair
Local Arrangements Chair
Academic Community Liaison
Michael B. Feldman, George Washington University (Ret.)
mfeldman@gwu.edu

Program Chair
Proceedings Chair
Tucker Taft, AdaCore
taft@adacore.com

Treasurer
Jeff Boleng, Software Engineering Institute
JLBoleng@SEI.CMU.edu

Workshops Chair
Tutorials Chair
John W. McCormick, University of Northern Iowa
mccormick@cs.uni.edu

Webmaster
Clyde Roby, Institute for Defense Analyses
clyderoby@acm.org

Exhibits and Sponsorships Chair
Greg Gicca, Verocel
gicca@verocel.com

Registration Chair
Thomas A. Panfil, U.S. Department of Defense (Ret.)
tapanfil@acm.org

Publicity Chair
Alok Srivastava, TASC Inc.
alok.srivastava@tasc.com

Logo Designer
Weston Pan, Raytheon Space and Airborne Systems

HILT 2014 CONFERENCE AT A GLANCE

Saturday, October 18, 2014: Conference Tutorials

8:00 AM–9:00 AM	Registration
9:00 AM–5:30 PM	Tutorials

Sunday, October 19, 2014: Conference Tutorials

8:00 AM–9:00 AM	Registration
9:00 AM–5:30 PM	Tutorials
7:00 PM–10:00 PM	SIGAda Business Meeting (Open to all)

Monday, October 20, 2014: Main Conference

8:00 AM–9:00 AM	Registration
9:00 AM–5:30 PM	Conference Program
10:30 AM–4:00 PM	Sponsor Exhibits
7:00 PM–10:00 PM	Dinner and Social Event

Tuesday, October 21, 2014: Main Conference

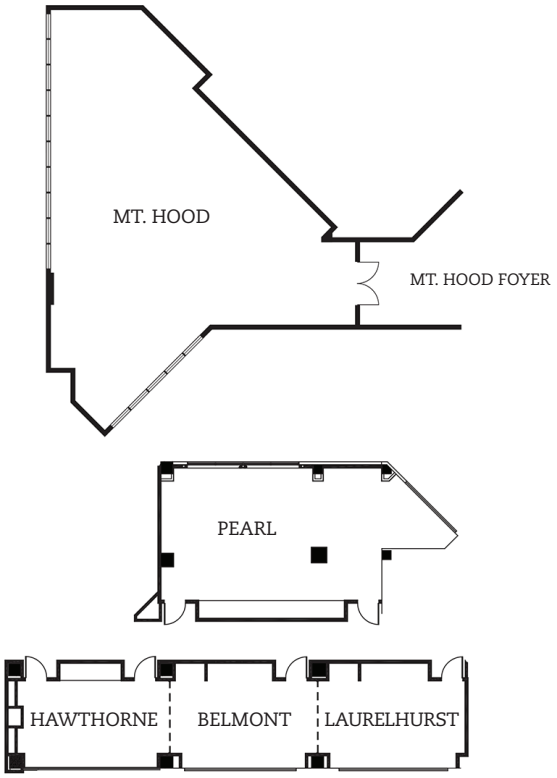
8:00 AM–8:30 AM	Registration
8:30 AM–6:00 PM	Conference Program
10:30 AM–4:00 PM	Sponsor Exhibits

Wednesday, October 22: SPLASH Keynote

8:30 AM–10:00 AM	SPLASH Keynote

CONFERENCE CENTER AND MEETING ROOM MAP

Portland Marriott Downtown Waterfront, Second Floor
1401 SW Naito Parkway, Portland, Oregon 97201
tel. 503.226.7600



Welcome to ACM SIGAda's Annual International Conference HIGH INTEGRITY LANGUAGE TECHNOLOGY — HILT 2014

Welcome to Portland and to HILT 2014, this year's annual international conference of the ACM Special Interest Group on the Ada Programming Language (SIGAda). This year we are pleased to be co-located with the SPLASH 2014 conference, enabling even more chances for interactions with colleagues in industry, academia, and government.

HILT 2014's top-quality technical program focuses on the issues associated with **high integrity software**—where a failure could cause loss of human life or have other unacceptable consequences—and on the solutions provided by **language technology**. "Language technology" here encompasses languages for programming, specifications, program properties, domain models, and other attributes of the software or the overall system.

HILT 2014 consists of two days of tutorials, and two days of conference sessions, covering a wide range of topics associated with **safe, secure and reliable software**: enhancing and evolving embedded systems languages for safety, behavioral modeling and code generation, practical use of assertions and formal methods in industry, and safe programming languages for the multicore era. You will learn the latest developments in model and program verification technologies, and hear industrial presentations from practitioners. The accompanying **exhibits** will give you the opportunity to meet our corporate sponsors and find out about their latest offerings.

At HILT 2014 you will have the chance to meet and talk with researchers and practitioners in industry, academia, and government, to ask them questions, and to explain your own work and interests. These renewed and new associations can be as valuable as the technical program at professional conferences, and their benefits will continue to reward you well after you return home.

HILT 2014 Conference Chair
MICHAEL FELDMAN
Professor, George Washington University (Retired)

HILT 2014 Program Chair
S. TUCKER TAFT
Director of Language Research, AdaCore

KEYNOTE TOPICS / FEATURED SPEAKERS

Monday, October 20, 2014 / 9:00 AM–10:30 AM

From Ada 9X to Spaceport America: Going Where No One Has Gone Before

CHRISTINE ANDERSON
Spaceport America

Bio sketch: www.sigada.org/conf/hilt2014/Christine-Anderson.html

ABSTRACT Ada 95, aka Ada9X at the time because we didn't know when we would be done, was a labor of love for most of us. A spectacular team was assembled from all over the world. I had the distinct pleasure and honor of being the Department of Defense Ada 9X Project Manager. The lessons I learned and the experience I gained allowed me to do many other things after Ada 95 was completed. I ran an Air Force space technology laboratory. I was responsible for building military satellites and launching them from the Cape. Currently, I am responsible for developing and operating the first purpose-built commercial spaceport. Looking back, the common thread through all of these endeavors is innovation, dedication, strong team work, and a passion for the job at hand. That can do spirit and boundless energy is a must for success and I have been fortunate to work on unprecedented projects with colleagues who possessed these qualities. Anecdotes from the Ada9X Project to today's emerging commercial space industry will be provided from my experiences and observations.

Due to a last minute conflict at the Spaceport, Christine will be joining us by video.

Monday, October 20, 2014 / 2:00 PM–3:30 PM

AADL and Model-Based Engineering

PETER FEILER
Software Engineering Institute/Carnegie Mellon University

Bio sketch: www.sigada.org/conf/hilt2014/Peter-Feiler.html

ABSTRACT Mission and safety critical software-reliant systems, aka Cyber-physical systems, face the increasing challenges of exponential increase in verification related software rework cost. Industry studies show that 70% of defects are introduced in requirements and architecture design, while 80% are discovered post-unit test. The Architecture Analysis & Design Language (AADL) standard was targeted to address these issues through virtual system integration to analytically discover these system level issues regarding operational system properties early in the life cycle.

After a summary of the challenges, the presentation highlights the expressive, analytical, and auto-generation capabilities of the AADL core language as well as several of its standardized extensions. The presentation then illustrates the importance of the analytical virtual system integration capabilities on several realistic industrial examples. In this context we discuss the benefit of well-defined semantics of nominal and fault behavior, timing, semantics of the model in AADL over other MBD notations.

The presentation concludes by outlining a four part improvement strategy: architecture-led requirement specification to improve the quality of requirements, architecture refinement and incremental virtual system integration to discover issues early, compositional verification through static analysis to address scalability, and incremental verification and testing throughout the life cycle as assurance evidence.

Tuesday, October 21, 2014 / 8:30 AM–10:00 AM

Correctness via Compilation to Logic

THOMAS BALL
Microsoft Research

Bio sketch: www.sigada.org/conf/hilt2014/Tom-Ball.html

ABSTRACT Advances in automated theorem provers over the last decade have led to a renaissance in software tools that compile problems of correctness to problems over logic formula. In this talk, I will review progress in automated theorem provers, such as Z3 from Microsoft Research, and consider a variety of program correctness tools that build upon Z3, such as automated test generators, automated safety/termination checkers, as well as interactive functional verifiers. I'll then describe a number of new projects that make use of the correctness via compilation to logic approach, including the design of new programming languages, ensuring the security of data centers, and safely programming gesture recognizers such as Kinect.

TUTORIALS Saturday, October 18, 2014

8:00 AM–9:00 AM	REGISTRATION IN MT. HOOD FOYER	
9:00 AM–10:30 AM	**BELMONT** **SAT_FD_1:** Object-Oriented Programming with Ada 2005 and Ada 2012 *Ed Colbert (Absolute Software)*	**HAWTHORNE** **SAT_FD_2:** Introduction to SPARK 2014 *Peter Chapin (Vermont Technical College) and John W. McCormick (University of Northern Iowa)*
10:30 AM–11:00 AM	MORNING BREAK	
11:00 AM–12:30 PM	**BELMONT** **SAT_FD_1, continued:** Object-Oriented Programming with Ada 2005 and Ada 2012	**HAWTHORNE** **SAT_FD_2, continued:** Introduction to SPARK 2014
12:30 PM–2:00 PM	LUNCH BREAK *(on your own)*	
2:00 PM–3:30 PM	**BELMONT** **SAT_FD_1, continued:** Object-Oriented Programming with Ada 2005 and Ada 2012	**HAWTHORNE** **SAT_FD_2, continued:** Introduction to SPARK 2014
3:30 PM–4:00 PM	AFTERNOON BREAK	
4:00 PM–5:30 PM	**BELMONT** **SAT_FD_1, continued:** Object-Oriented Programming with Ada 2005 and Ada 2012	**HAWTHORNE** **SAT_FD_2, continued:** Introduction to SPARK 2014

TUTORIALS Sunday, October 19, 2014

8:00 AM–9:00 AM	REGISTRATION IN MT. HOOD FOYER	
9:00 AM–10:30 AM	**BELMONT** **SUN_AM_1:** High-Integrity Object-Oriented Programming with Ada 2012 *Ben Brosgol (AdaCore)*	
10:30 AM–11:00 AM	MORNING BREAK	
11:00 AM–12:30 PM	**BELMONT** **SUN_AM_1, continued:** High-Integrity Object-Oriented Programming with Ada 2012	
12:30 PM–2:00 PM	LUNCH BREAK *(on your own)*	
2:00 PM–3:30 PM	**BELMONT** **SUN_PM_1:** AADLv2, an Architecture Description Language for the Analysis and Generation of Embedded Systems *Jérôme Hugues (Institute for Space and Aeronautics Engineering) and Frank Singhoff (Université de Bretagne Occidentale)*	**HAWTHORNE** **SUN_PM_2:** Rust—Zero-Cost Safety *Niko Matsakis (Mozilla Research)*
3:30 PM–4:00 PM	AFTERNOON BREAK	
4:00 PM–5:30 PM	**BELMONT** **SUN_PM_1, continued:** AADLv2, an Architecture Description Language for the Analysis and Generation of Embedded Systems	**HAWTHORNE** **SUN_PM_2, continued:** Rust—Zero-Cost Safety

SIGAda Business Meeting Sunday, October 19, 2014

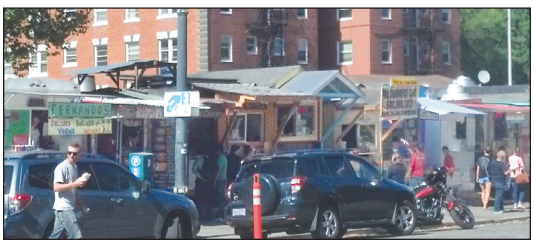
7:00 PM–10:00 PM	**BELMONT** SIGAda Business Meeting *(open to all)*

TECHNICAL PROGRAM Monday, October 20, 2014

8:00 AM–9:00 AM	**REGISTRATION IN MT. HOOD FOYER**
9:00 AM–10:30 AM	**MT. HOOD** **Plenary Session** **Greetings** *SIGAda and Conference Officers* **Plenary Session** *Chair: John Barnes (John Barnes Informatics)*
	Keynote Address: From Ada9X to Spaceport America: Going Where No One Has Gone Before *Christine Anderson (Spaceport America) Due to a last minute conflict at the Spaceport, Christine will be joining us by video*
10:30 AM–11:00 AM	**MORNING BREAK / EXHIBITS IN PEARL**
11:00 AM–12:30 PM	**MT. HOOD** **Session: Enhancing and Evolving Embedded Systems Languages for Safety** *Chair: Jack Wileden (University of Massachusetts, Amherst)*
	Ada83 to Ada2012—Lessons Learned Over 30 Years of Language Design *John Barnes (John Barnes Informatics) and Tucker Taft (AdaCore)*
	Can C++ Be Made as Safe as SPARK? *David Crocker (Escher Technologies Ltd., UK)*
	mbeddr—Extensible Languages for Embedded Software Development *Tamas Szabo (itemis AG, Germany)*
	AdaCore Sponsor Presentation *Ben Brosgol (AdaCore)*
12:30 PM–2:00 PM	**LUNCH BREAK / EXHIBITS IN PEARL**
2:00 PM–3:30 PM	**MT. HOOD** **Session: Model-Based Engineering** *Chair: Julien Delange (Carnegie Mellon University Software Engineering Institue (SEI))*
	Invited Address: AADL and Model-Based Engineering *Peter Feiler (Software Engineering Institue / Carnegie Mellon University)*
	Resolute: An Assurance Case Language for Architecture Models *John Backes (Rockwell Collins)*
3:30 PM–4:00 PM	**AFTERNOON BREAK / EXHIBITS IN PEARL**
4:00 PM–5:30 PM	**MT. HOOD** **Session: Behavioral Modeling and Code Generation** *Chair: John W. McCormick (University of Northern Iowa)*
	Hybrid Annex: An AADL Extension for Continuous Behavior and Cyber-Physical Interaction Modeling *Stephen Barrett (Kansas State University)*
	Leveraging Ada 2012 and SPARK 2014 for Assessing Generated Code from AADL Models *Jérôme Hugues (Institute for Space and Aeronautics Engineering (ISAE), Toulouse, France)*
	Session: Industrial Presentations
	Formal Semantics for the PACEMAKER System Specification *Brian Larson (Kansas State University)*
	UML with Meaning: Executable Modeling in Foundational UML and the Alf Action Language *Ed Seidewitz (Model Driven Solutions)*
	Panel: Executable and Behavioral Modeling Languages *Moderator: John W. McCormick (University of Northern Iowa)* Continuous AADL for Cyber-Physical Modeling *(Stephen Barrett, Kansas State University)*; Assessing AADL Code Generation Using SPARK *(Jérôme Hugues, Institute for Space and Aeronautics Engineering (ISAE), Toulouse, France)*; PACEMAKER Specification Using Behavioral AADL *(Brian Larson, Kansas State University)*; Adding Meaning to UML with the Alf Action Language *(Ed Seidewitz, Model Driven Solutions)*
5:30 PM–7:00 PM	**BREAK**
7:00 PM–10:00 PM	**Dinner and Social Event: Portland Food Cart World Tour**

DINNER AND SOCIAL EVENT: PORTLAND FOOD CART WORLD TOUR Monday, October 20, 2014

On Monday evening, October 20, the Marriott exhibition hall will be transformed for HILT 2014 registrants, into a Portland Food Cart World Tour, featuring a variety of cuisines and nationalities. Was CNN's judgement correct? Does Portland have the world's best street food? Come taste for yourself.



TECHNICAL PROGRAM Tuesday, October 21, 2014

8:00 AM–8:30 AM	REGISTRATION IN MT. HOOD FOYER
8:30 AM–10:00 AM	**MT. HOOD** **Plenary Session** **Announcements** **SIGAda Awards** *David Cook (Chair of SIGAda)* **Plenary Session** *Chair: Judith Bishop (Microsoft Research)*
	Keynote Address: Correctness via Compilation to Logic *Thomas Ball (Microsoft Research)*
	Microsoft Research Sponsor Presentation
10:00 AM–10:30 AM	MORNING BREAK / EXHIBITS IN PEARL
10:30 AM–12:30 PM	**MT. HOOD** **Session: Applying Formal Methods** *Chair: Tucker Taft (AdaCore)*
	A Framework for Model Checking UDP Network Programs with Java Pathfinder *William Rathje (University of Puget Sound)*
	Specification of Generic APIs—or; Why Algebraic May Be Better Than Pre/Post *Magne Haveraaen (University of Bergen, Norway)*
	Ellidiss Sponsor Presentation *Tony Ellison (Ellidiss (TNI Europe)*
12:30 PM–2:00 PM	LUNCH BREAK / EXHIBITS IN PEARL
2:00 PM–3:30 PM	**MT. HOOD** **Session: Safe Programming Languages for the Multicore Era (I)** *Chair: Brad Moore (General Dynamics)*
	Safe Parallel Programming in Ada with Language Extenstions *Tucker Taft (AdaCore)*
	Spot: A Programming Language for Verified Flight Software *Robert Bocchino (Jet Propulsion Laboratory)*
	The Rust Language *Niko Matsakis (Mozilla Research)*
3:30 PM–4:00 PM	AFTERNOON BREAK / EXHIBITS IN PEARL
4:00 PM–5:30 PM	**MT. HOOD** **Session: Safe Programming Languages for the Multicore Era (II)** *Session Chair: Clyde Roby (Institute for Defense Analyses)*
	Panel: Finding Safety in Numbers—New Languages for Safe Multicore Programming and Modeling *Moderator: Clyde Roby (Institute for Defense Analysis)* Spot for Verified Flight Software *(Robert Bocchino, Jet Propulsion Laboratory)*; The Rust Language *(Niko Matsakis, Mozilla Research)*; ParaSail for Pointer-Free Parallelism *(Tucker Taft, AdaCore)*; BLESS: Behavioral AADL *(Brian Larson, Kansas State University)*; Alf: Action Language for Foundational UML *(Ed Seidewitz, Model Driven Solutions)*
5:30 PM–6:00 PM	**Plenary Session** **Ada-Europe 2015 Conference Announcement** **Future SIGAda Conferences** *Tucker Taft (AdaCore)*

SPLASH KEYNOTE Wednesday, October 22, 2014 *HILT registrants are invited to attend this talk*

8:30 AM–10:00 AM	**SALON E+F** **Plenary Session**
	Keynote Address: Software Security—A Study in Technology Transfer *Gary McGraw (Cigital, Inc.)*