Association for
Computing Machinery

Advancing Computing as a Science & Profession

HILT 2012: HIGH INTEGRITY LANGUAGE TECHNOLOGY

ACM SIGAda's Annual International Conference

November 10–14, 2013 / Pittsburgh, Pennsylvania / 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.

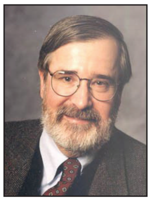
A significant factor affecting whether and how such requirements are met is the chosen language technology and its supporting tools: not just the programming language(s) but also languages for expressing specifications, program properties, domain models, and other attributes of the software or overall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

HILT 2013 provides a forum for the leading experts from academia/research, industry, and government to present their latest findings in designing, implementing, and using language technology for high integrity software.

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.

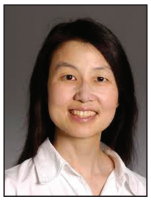
www.sigada.org/conf/hilt2013/

FEATURED SPEAKERS



Model Checking and the Curse of Dimensionality

EDMUND M. CLARKE
Carnegie Mellon University
Electrical and Computer Engineering (ECE)



Formal Methods: An Industrial Perspective

JEANNETTE WING
Microsoft Research

Building Confidence in System Behavior

JOHN GOODENOUGH
Carnegie Mellon University
Software Engineering Institute (SEI)

Up and Out: Scaling Formal Analysis Using Model-Based Development and Architecture Modeling

MICHAEL WHALEN
University of Minnesota

CORPORATE SPONSORS

PLATINUM LEVEL

AdaCore
The GNAT Pro Company

GOLD LEVEL

Microsoft Research

SILVER LEVEL

Ellidiss Software
TNI Europe Limited

VEROCEL
The Software Verification Company

BASIC LEVEL

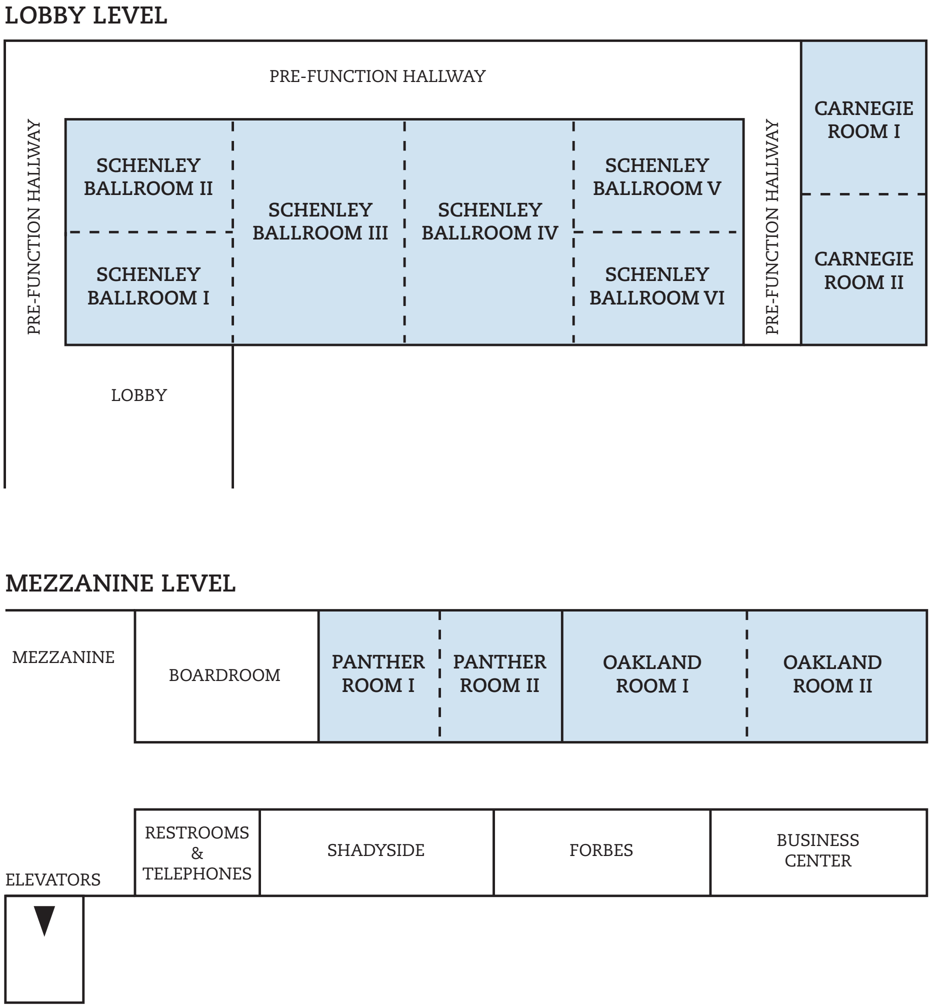
LDRA

MathWorks®

CONTENTS

CONFERENCE CENTER AND MEETING ROOM MAP

Wyndham Pittsburgh University Center, 100 Lytton Avenue, Pittsburgh, Pennsylvania 15213, tel. 412.682.6200



LOBBY LEVEL

MEZZANINE LEVEL

HILT 2013: HIGH INTEGRITY LANGUAGE TECHNOLOGY

Conference At A Glance

Sunday, November 10, 2013: Conference Tutorials

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

Monday, November 11, 2013: Conference Tutorials

8:00 AM–9:00 AM	Registration
9:00 AM–5:30 PM	Tutorials
7:00 PM–10:00 PM	SIGAda Extended Executive Committee (EEC) Meeting, open to all

Tuesday, November 12, 2013: 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
6:00 PM–10:00 PM	Evening Event: Dinner and Bowling at the PAA (Pittsburgh Athletic Association)

Wednesday, November 13, 2013: Main Conference

8:00 AM–9:00 AM	Registration
9:00 AM–5:30 PM	Conference Program
10:30 AM–2:00 PM	Sponsor Exhibits
7:00 PM–10:00 PM	Workshops / "Birds of a Feather" Sessions

Thursday, November 14, 2013: Main Conference

8:00 AM–9:00 AM	Registration
9:00 AM–12:00 PM	Conference Program
12:00 PM–12:30 PM	Closing Comments and Conference Adjournment

CONFERENCE COMMITTEE

Conference Chair /
Local Arrangements Chair
Jeff Boleng, Software Engineering Institute
jlboleng@SEI.CMU.EDU

Program Chair
Tucker Taft, AdaCore
taft@adacore.com

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

Treasurer
Ricky E. Sward, The MITRE Corporation
rsward@mitre.org

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

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

Registration Chair /
Academic Community Liaison
Michael B. Feldman, George
Washington University (Ret.)
mfeldman@gwu.edu

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

Logo Designer
Weston Pan, Raytheon Space
and Airborne Systems

Welcome to ACM SIGAda's Annual International Conference
High Integrity Language Technology – HILT 2013

Welcome to Pittsburgh and to HILT 2013, this year's annual international conference of the ACM Special Interest Group on the Ada Programming Language (SIGAda).

HILT 2013 features a top-quality technical program focused 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 not only programming languages but also languages for expressing specifications, program properties, domain models, and other attributes of the software or the overall system.

HILT 2013 consists of two days of tutorials, and three days of conference sessions. The **tutorials** cover a wide range of topics: Ada 2012, proving safety of parallel and multi-threaded programs, Formula 2.0: a language for formal specification and a tool for automated analysis, satisfiability modulo theories for high integrity development, practical specification and verification with code contracts, bounded model checking for high-integrity software, and service oriented architecture concepts and implementation.

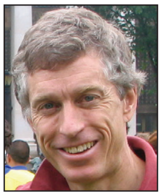
The conference program includes **keynote and invited presentations** from internationally recognized experts:

- **Edmund M. Clarke** (Carnegie Mellon University, 2007 Turing Award Winner), on Model Checking and the Curse of Dimensionality;
- **Jeannette Wing** (Microsoft Research), on Formal Methods: An Industrial Perspective;
- **John Goodenough** (Carnegie Mellon University Software Engineering Institute), on Building Confidence in System Behavior; and
- **Michael Whalen** (University of Minnesota), on Up and Out: Scaling Formal Analysis Using Model-Based Development and Architecture Modeling.

HILT 2013 **conference sessions** deal with a range of topics associated with **safe, secure and reliable software:** formal verification technologies and toolsets, high-integrity parallel programing, model-based integration and code generation, architecture level design languages and compositional verification, and approaches to software safety and security. You will learn the latest developments in software verification technologies, and hear industrial presentations from practitioners. The accompanying **exhibits** will give you the opportunity to meet vendors and find out about their latest offerings. Vendors include AdaCore (Platinum Level); Microsoft Research (Gold Level); Ellidiss, Verocel (Silver Level); and LDRA, MathWorks (Basic Level).

At HILT 2013 you will learn about both the challenges confronting high integrity software and the solutions available to address them. Perhaps just as important are the social interactions that you get at a live conference: 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.

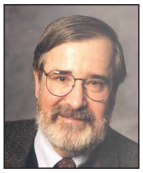
Jeff Boleng
HILT 2013
Conference Chair
Software Engineering
Institute



S. Tucker Taft
HILT 2013
Program Chair
AdaCore

KEYNOTE TOPICS / FEATURED SPEAKERS

Tuesday, November 12 / 9:00 AM–10:30 AM



Model Checking and the Curse of Dimensionality

EDMUND M. CLARKE
Carnegie Mellon University
Bio sketch: www.cs.cmu.edu/~emc/bio.html

Model Checking is an automatic verification technique for large state transition systems.

It was originally developed for reasoning about finite-state concurrent systems. The technique has been used successfully to debug complex computer hardware and communication protocols. Now, it is beginning to be used for software verification as well. The major disadvantage of the technique is a phenomenon called the State Explosion Problem. This problem is impossible to avoid in worst case. However, by using sophisticated data structures and clever search algorithms, it is now possible to verify state transition systems with astronomical numbers of states.

Wednesday, November 13 / 9:00 AM–10:30 AM

Up and Out: Scaling Formal Analysis Using Model-Based Development and Architecture Modeling

MICHAEL WHALEN
University of Minnesota
Bio sketch: www.sigada.org/conf/hilt2013/Michael-Whalen.html

Systems are naturally constructed in hierarchies in which design choices made at higher levels of abstraction levy requirements on system components at lower levels of abstraction. Thus, whether an aspect of the system is a design choice or a requirement depends largely on one's vantage point within the hierarchy of system components. Furthermore, systems are often constructed middle-out rather than top-down; compatibility with existing systems and architectures, or availability of specific components influences high-level requirements. We believe that requirements and architectural design should be more closely aligned: that requirements models must account for hierarchical system construction, and that architectural design notations must better support specification of requirements for system components.

In this presentation, I describe tools supporting iterative development of architecture and verification based on software models. We represent the hierarchical composition of the system in the Architecture Analysis & Design Language (AADL), and use an extension to the AADL language to describe requirements at different levels of abstraction for compositional verification. To describe and verify component-level behavior, we use Simulink and Stateflow and multiple analysis tools.

Above, left to right: Attendees at HILT 2012; HILT 2012 "Birds-of-a-Feather" Sessions. All conference photographs on pages 5–7 courtesy of Tom Panfil.

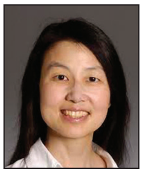
Wednesday, November 13 / 2:00 PM–3:30 PM

Building Confidence in System Behavior

JOHN GOODENOUGH
Carnegie Mellon University Software Engineering Institute
Bio sketch: www.sei.cmu.edu/about/people/profile.cfm?id=goodenough_12984

If the use of Ada (or SPARK or some other tool) increases our confidence in the behavior of high integrity software systems, why does it do so? What do we mean by confidence, and what is a justified basis for asserting some level of confidence? In this talk, I'll address some recent research on the potential value of thinking about confidence in terms of eliminative induction, assurance cases, and confidence maps.

Thursday, November 14 / 9:00 AM–10:30 AM



Formal Methods: An Industrial Perspective

JEANNETTE WING
Microsoft Research
Bio sketch: research.microsoft.com/en-us/press/jeannette-wing.aspx

Formal methods research has made tremendous progress since the 1980s when a proof using a theorem prover was worthy of a Ph.D. thesis and a bug in a VLSI textbook was found using a model checker. Now, with advances in theorem proving, model checking, satisfiability modulo theories (SMT) solvers, and program analysis, the engines of formal methods are more sophisticated and are applicable and scalable: to a wide range of domains, from biology to mathematics; to a wide range of systems, from asynchronous systems to spreadsheets; and for a wide range of properties, from security to program termination. In this talk, I will present a few Microsoft Research stories of advances in formal methods and their application to Microsoft products and services. Formal methods use, however, is not routine—yet—in industrial practice. So, I will close with outstanding challenges and new directions for research in formal methods.

Clockwise from top left: SIGAda 2011 tutorial; SIGAda 2011 dinner; SIGAda 2011 EEC meeting.

TUTORIALS Sunday, November 10, 2013

8:00 AM–9:00 AM	REGISTRATION IN PRE-FUNCTION HALLWAY	
9:00 AM–10:30 AM	**PANTHER I, II** **SA1:** Object Oriented Programming in Ada 2012 Part 1 *Ed Colbert (Absolute Software)*	**OAKLAND I, II** **SA2:** Proving Safety of Parallel/ Multi-Threaded Programs *Tucker Taft (AdaCore)*
10:30 AM–11:00 AM	MORNING BREAK	
11:00 AM–12:30 PM	**PANTHER I, II** **SA1:** Object Oriented Programming in Ada 2012 Part 1 *(continued)*	**OAKLAND I, II** **SA2:** Proving Safety of Parallel/ Multi-Threaded Programs *(continued)*
12:30 PM–2:00 PM	LUNCH BREAK *(on your own)*	
2:00 PM–3:30 PM	**PANTHER I, II** **SP1:** Object Oriented Programming in Ada 2012 Part 2 *Ed Colbert (Absolute Software)*	**OAKLAND I, II** **SP2:** Engineering Domain-Specific Languages with FORMULA 2.0 *Ethan K. Jackson (Microsoft Research)*
3:30 PM–4:00 PM	AFTERNOON BREAK	
4:00 PM–5:30 PM	**PANTHER I, II** **SP1:** Object Oriented Programming in Ada 2012 Part 2 *(continued)*	**OAKLAND I, II** **SP2:** Engineering Domain-Specific Languages with FORMULA 2.0 *(continued)*

Clockwise from top left: SIGAda 2010 registration; SIGAda 2009 keynote address; SIGAda 2008 dinner; SIGAda 2009 morning break.

TUTORIALS Monday, November 11, 2013

8:00 AM–9:00 AM	REGISTRATION IN PRE-FUNCTION HALLWAY	
9:00 AM–10:30 AM	**PANTHER I, II** **MA1:** Satisfiability Modulo Theories for High Integrity Development *Nikolaj Bjorner (Microsoft Research)*	**OAKLAND I, II** **MA2:** Practical Specification and Verification with CodeContracts *Francesco Logozzo (Microsoft Research)*
10:30 AM–11:00 AM	MORNING BREAK	
11:00 AM–12:30 PM	**PANTHER I, II** **MA1:** Satisfiability Modulo Theories for High Integrity Development *(continued)*	**OAKLAND I, II** **MA2:** Practical Specification and Verification with CodeContracts *(continued)*
12:30 PM–2:00 PM	LUNCH BREAK *(on your own)*	
2:00 PM–3:30 PM	**PANTHER I, II** **MP1:** Bounded Model Checking for High-Integrity Software *Sagar Chaki (CMU/SEI)*	**OAKLAND I, II** **MP2:** Service-Oriented Architecture (SOA) Concepts and Implements *Ricky Sward (The MITRE Corporation) and Jeff Boleng (CMU/SEI)*
3:30 PM–4:00 PM	AFTERNOON BREAK	
4:00 PM–5:30 PM	**PANTHER I, II** **MP1:** Bounded Model Checking for High-Integrity Software *(continued)*	**OAKLAND I, II** **MP2:** Service-Oriented Architecture (SOA) Concepts and Implements *(continued)*
5:30 PM–7:00 PM	DINNER BREAK *(on your own)*	
7:00 PM–10:00 PM	**PANTHER I, II** SIGAda Extended Executive Committee (EEC) Meeting *(open to all)*	

Pittsburgh. Photographs courtesy of commons.wikimedia.org/wiki/Pittsburgh. Clockwise from top left: Heinz Field by Bernard Gagnon (User:bgag); Smithfield Bridge by Chuck Szmurlo (User:Cszmurlo); Duquesne Incline by Derek Cashman (User:Derek.cashman); Point State Park by John Marino (User:Weatherman1126).

TECHNICAL PROGRAM Tuesday, November 12, 2013

Technology for Program Verification

8:00 AM–9:00 AM	REGISTRATION IN PRE-FUNCTION HALLWAY
9:00 AM–10:30 AM	**SCHENLEY BALLROOM I, II, III** **Greetings** *SIGAda and Conference Officers*
	SCHENLEY BALLROOM I, II, III **Keynote Address: Model Checking and the Curse of Dimensionality** *Edmund M. Clarke (CMU/ECE)*
10:30 AM–11:00 AM	MORNING BREAK / EXHIBITS IN SCHENLEY BALLROOM IV, V, VI
11:00 AM–12:30 PM	**SCHENLEY BALLROOM I, II, III** **Session: Underlying Formal Verification Technologies**
	Panel on Underlying Formal Verification Technologies *Moderator: Tucker Taft (AdaCore)* Coq-based proofs *(Prof. Robby, Kansas State University)*; SMT Solvers *(Nikolaj Bjorner, Microsoft Research)*; Inferring contracts with Abstract Interpretation *(Francesco Logozzo, Microsoft Research)*; Bounded Model Checking *(Sagar Chaki, CMU/SEI)*
	Sponsor Presentation: AdaCore *(Albert Lee, AdaCore)*
12:30 PM–2:00 PM	LUNCH BREAK / EXHIBITS IN SCHENLEY BALLROOM IV, V, VI
2:00 PM–3:30 PM	**SCHENLEY BALLROOM I, II, III** **Session: Formal Verification Toolsets** *Session Chair: David Cook (Stephen F. Austin State University)*
	SAW: The Software Analysis Workbench *Joe Hendrix (Galois)*
	Optimizing Development and Verification Effort with SPARK 2014 *Andrew Hawthorn (ALTRAN)*
	Towards the Formalization of SPARK 2014 Semantics with Explicit Run-time Checks Using Coq *Zhi Zhang (Kansas State University)*
3:30 PM–4:00 PM	AFTERNOON BREAK / EXHIBITS IN SCHENLEY BALLROOM IV, V, VI
4:00 PM–5:30 PM	**SCHENLEY BALLROOM I, II, III** **Session: High-Integrity Parallel Programming**
	Panel on Safe, Efficient Parallel Programming *Moderator: Clyde Roby (Institute for Defense Analyses)* Real-Time Programming on Accelerator Many-Core Processors *(Steven Michell, Maurya Software)*; Bringing Parallel Programming to the SPARK Verifiable Subset of Ada *(Tucker Taft, AdaCore)*
	Sponsor Presentation
5:30 PM–6:00 PM	BREAK
6:00 PM–10:00 PM	**Evening Social Event: Dinner and Bowling at the Pittsburgh Athletic Association**

SOCIAL EVENT: DINNER AND BOWLING AT THE PAA Tuesday, November 12

This year's social event will be our Tuesday evening dinner at the Pittsburgh Athletic Association across from the conference hotel in Pittsburgh. Reception is from about 6:00–6:30 PM, dinner will be about 6:30–7:45 PM or so, and bowling will then be from about 8:00–10:00 PM.

Pittsburgh Athletic Association
4215 Fifth Avenue
Pittsburgh, Pennsylvania 15213
Tel. 412.621.2400

TECHNICAL PROGRAM Wednesday, November 13, 2013

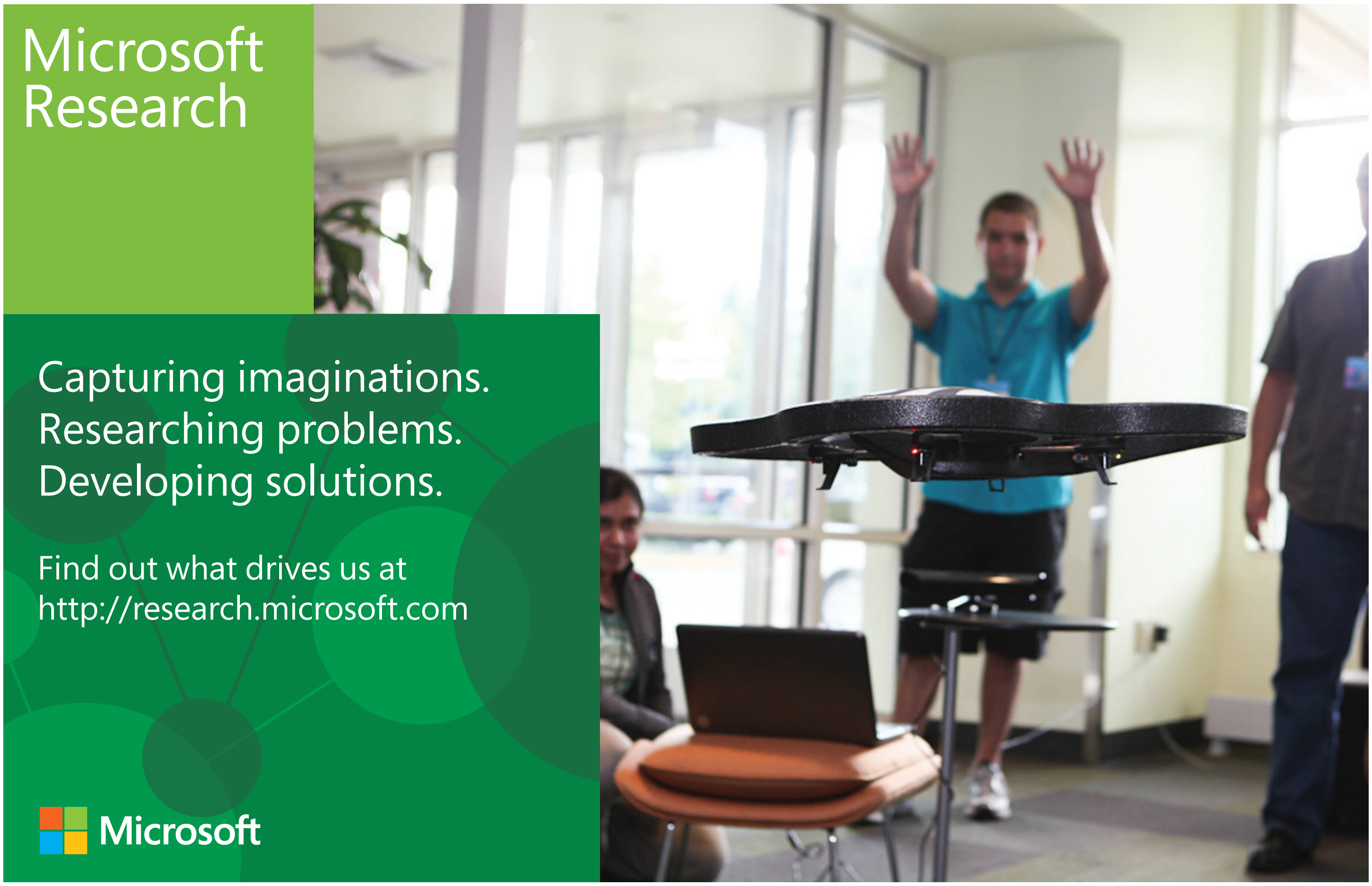
Model-Based Engineering and Verification

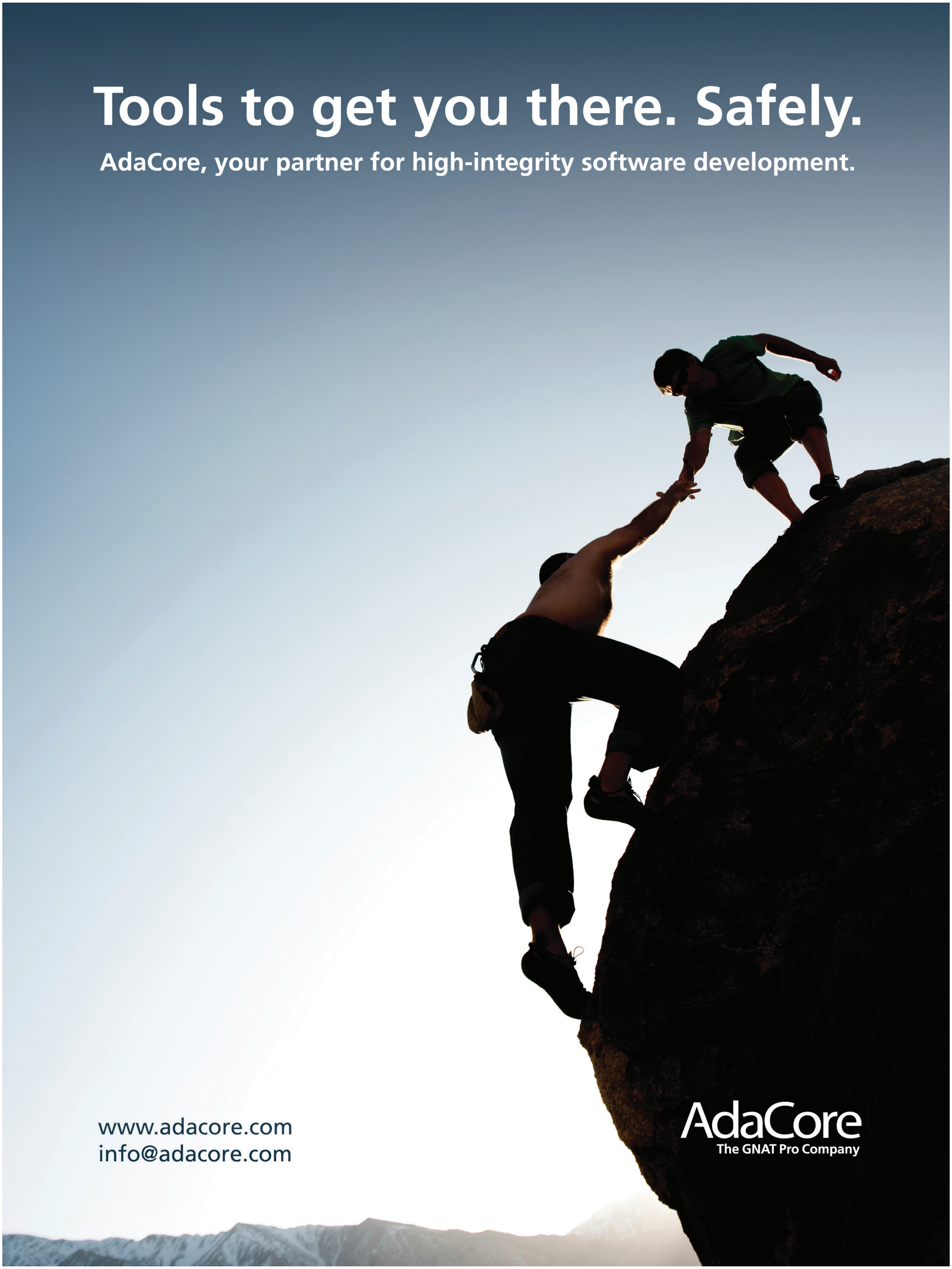
8:00 AM–9:00 AM	REGISTRATION IN PRE-FUNCTION HALLWAY
9:00 AM–10:30 AM	**SCHENLEY BALLROOM I, II, III** **Announcements; SIGAda Awards** *Ricky E. Sward (Past SIGAda Chair)* **Overall Introduction to Model-Based Engineering and Verification Day** *General Session Chair: Julien Delange (CMU/SEI)*
	SCHENLEY BALLROOM I, II, III **Invited Talk: Up and Out: Scaling Formal Analysis Using Model-Based Development and Architecture Modeling** *Michael Whalen (University of Minnesota)*
10:30 AM–11:00 AM	MORNING BREAK / EXHIBITS IN SCHENLEY BALLROOM IV, V, VI
11:00 AM–12:30 PM	**SCHENLEY BALLROOM I, II, III** **Session: Model-Based Integration and Code Generation** *Session Chair: Dirk Craeynest (KU Leuven)*
	An Approach to Integration of Complex Systems: The SAVI Virtual Integration Process (industrial presentation) *David Redman (Aerospace Vehicle Systems Institute, Texas A&M)*
	Reddo - A Model Driven Engineering Toolset for Embedded Software Development (industrial presentation) *Steven Doran (Northrop Grumman)*
	Sponsor Presentation
12:30 PM–2:00 PM	LUNCH BREAK / EXHIBITS IN SCHENLEY BALLROOM IV, V, VI *(exhibits close at 2:00 PM)*
2:00 PM–3:30 PM	**SCHENLEY BALLROOM I, II, III** **Keynote Address: Building Confidence in System Behavior** *John Goodenough (CMU/SEI)*
3:30 PM–4:00 PM	AFTERNOON BREAK
4:00 PM–5:30 PM	**SCHENLEY BALLROOM I, II, III** **Session: Architecture-Level Design Languages and Compositional Verification** *Session Chair: Michael Feldman (GWU)*
	Compositional Verification of a Medical Device System *Sanjai Rayadurgam (University of Minnesota)*
	Illustrating the AADL Error Modeling Annex (v. 2) Using a Simple Safety-Critical Medical Device *Brian Larson (Kansas State University)*
	Sponsor Presentation
5:30 PM–7:00 PM	DINNER BREAK *(on your own)*
7:00 PM–10:00 PM	**SCHENLEY BALLROOM I, II, III** **Workshops / “Birds-of-a-Feather” Sessions**

TECHNICAL PROGRAM Thursday, November 14, 2013

Applying Formal Methods to the Real World

8:00 AM–9:00 AM	REGISTRATION IN PRE-FUNCTION HALLWAY
9:00 AM–10:30 AM	SCHENLEY BALLROOM I, II, III **Announcements; Best Paper and Student Paper Awards** *Tucker Taft (HILT 2013 Program Chair)*
	SCHENLEY BALLROOM I, II, III **Keynote Address: Formal Methods: An Industrial Perspective** *Jeannette Wing (Microsoft Research)*
10:30 AM–11:00 AM	MORNING BREAK
11:00 AM–12:00 PM	SCHENLEY BALLROOM I, II, III **Session: Approaches to Software Safety and Security** *Session Chair: Alok Srivastava (TASC)*
	Panel on Approaches to Software Safety and Security *Moderator: Alok Srivastava (TASC)* Secure Coding *(Robert Seacord, SEI/CERT)*; Use of Domain-Specific Languages *(Ethan K. Jackson, Microsoft Research)*; Integrating Technologies for Verification *(Joe Hendrix, Galois)*; Using contract-based programming tools *(Francesco Logozzo, Microsoft Research)*; Automatic vs. Interactive Program Verification *(Suad Alagic, University of Southern Maine)*
12:00 PM–12:30 PM	SCHENLEY BALLROOM I, II, III **Ada-Europe 2014 and SIGAda 2014 Conference Announcements** *Tucker Taft (SIGAda Vice Chair)*
12:30 PM	**Closing Remarks and Conference Adjournment**




Tools to get you there. Safely.
AdaCore, your partner for high-integrity software development.
www.adacore.com
info@adacore.com
AdaCore
The GNAT Pro Company