Association for Computing Machinery

Advancing Computing as a Science & Profession

HILT 2012: HIGH INTEGRITY LANGUAGE TECHNOLOGY

ACM SIGAda's Annual International Conference

December 2–6, 2012 / Boston, Massachusetts / 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 2012 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 SIGCSE, SIGPLAN, SIGSOFT, SIGBED, Ada-Europe, and the Ada Resource Association.

www.sigada.org/conf/hilt2012/

KEYNOTE TOPICS / FEATURED SPEAKERS

High-Assurance Cyber Military Systems (HACMS): High-Assurance Vehicles

KATHLEEN FISHER
DARPA Information Innovation Office

Challenges for Safety-Critical Software

NANCY LEVESON
Massachusetts Institute of Technology
Department of Aeronautics and Astronautics
Engineering Systems Division

Programming the Turing Machine

BARBARA LISKOV
Massachusetts Institute of Technology
Department of Electrical Engineering and Computer Science

Hardening Legacy C/C++ Code

GREG MORRISETT
Harvard University
School of Engineering and Applied Sciences

Programming Language Life Cycles

GUY L. STEELE, JR.
Oracle Labs

CORPORATE SPONSORS

PLATINUM LEVEL

AdaCore
The GNAT Pro Company

SILVER LEVEL

Ellidiss Software
TNI Europe Limited

LDRA

TASC

Microsoft Research

BASIC LEVEL

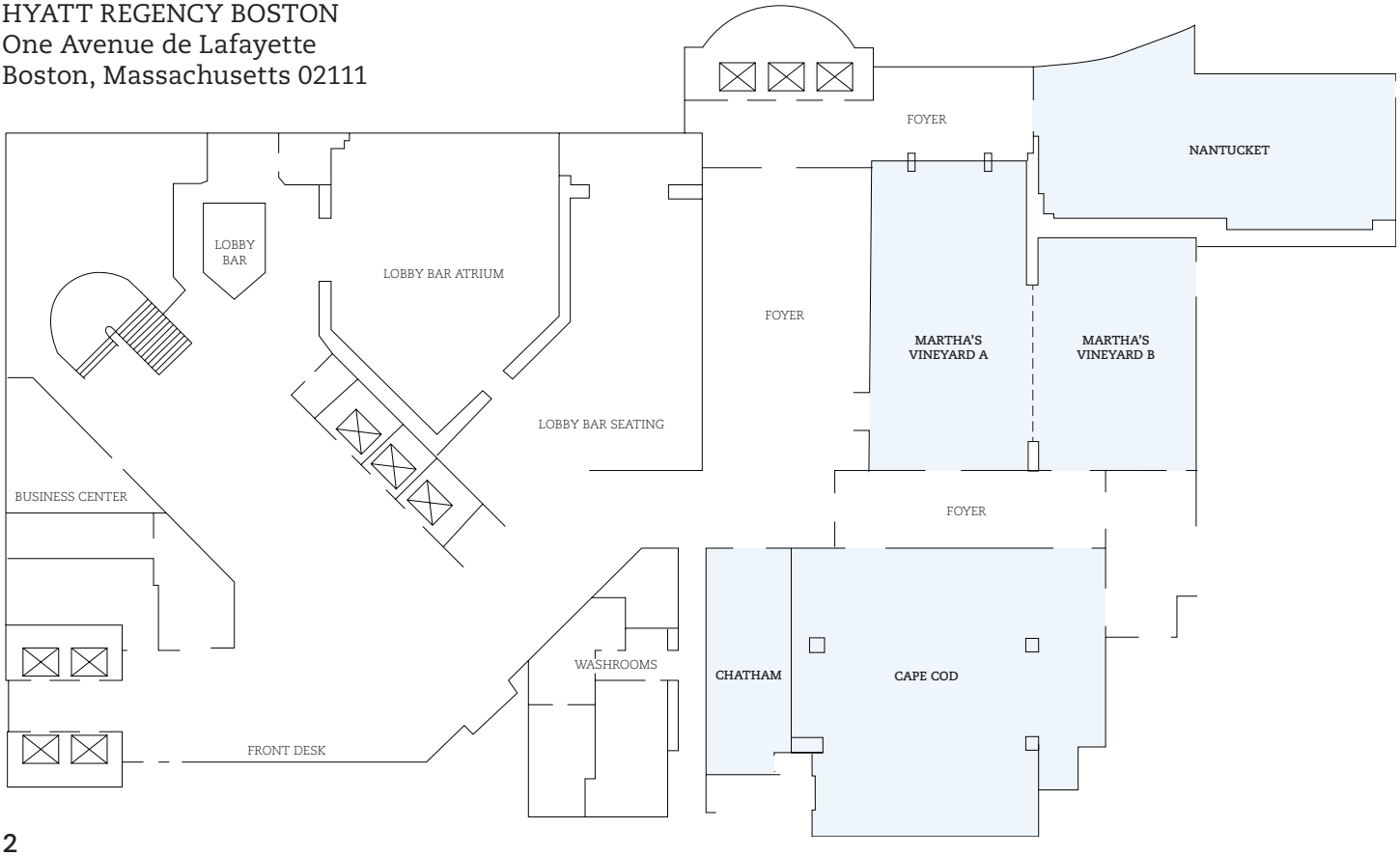
MathWorks

VECTOR software

CONTENTS

CONFERENCE CENTER AND MEETING ROOM MAP

HYATT REGENCY BOSTON
One Avenue de Lafayette
Boston, Massachusetts 02111



HILT 2012: HIGH INTEGRITY LANGUAGE TECHNOLOGY
Conference At A Glance

Sunday, December 2, 2012: Conference Tutorials

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

Monday, December 3, 2012: 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, December 4, 2012: 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
6:30 PM–7:30 PM	Old Town Trolley Tour of Boston
7:30 PM–9:30 PM	Dinner: Legal Sea Foods (Copley Place)

Wednesday, December 5, 2012: 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
8:00 PM–9:30 PM	Evening “Birds of a Feather” Session

Thursday, December 6, 2012: Main Conference

8:00 AM–9:00 AM	Registration
9:00 AM–1:00 PM	Conference Program
1:00 PM	Closing Comments and Conference Adjournment

CONFERENCE COMMITTEE

Conference Chair / Local Arrangements Chair
Ben Brosgol, AdaCore
brosgol@adacore.com

Program Co-Chair / Proceedings Chair
Jeff Boleng, Software Engineering Institute
jlboleng@SEI.CMU.EDU

Program Co-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
Alok Srivastava, TASC Inc.
alok.srivastava@tasc.com

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

Publicity Chair
Greg Gicca, AdaCore
gicca@adacore.com

Logo Designer
Weston Pan, Raytheon Space and Airborne Systems

Final Program Designer
Abigail Coyle

Welcome to ACM SIGAda's Annual International Conference
High Integrity Language Technology – HILT 2012

Welcome to Boston and to HILT 2012, this year's annual international conference of the ACM Special Interest Group on the Ada Programming Language (SIGAda).

HILT 2012 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.

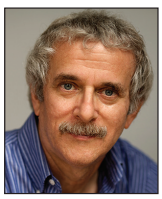
HILT 2012 consists of two days of tutorials, and three days of conference sessions. The **tutorials** cover a wide range of topics: designing for multitasking and multicore environments; leading-edge Ada verification technologies; contract-based programming and object-oriented programming in Ada 2012; safety of embedded software; Microsoft Research's Dafny automatic program verifier; Service-Oriented Architecture; and safety-critical Java.

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

- **KATHLEEN FISHER** (DARPA Information Innovation Office), on High-Assurance Cyber Military Systems (HACMS) / High-Assurance Vehicles;
- **NANCY LEVESON** (MIT), on Challenges for Safety-Critical Software;
- **BARBARA LISKOV** (MIT), on Programming the Turing Machine;
- **GREG MORRISETT** (Harvard University), on Hardening Legacy C/C++ Code; and
- **GUY L. STEELE, JR.** (Oracle Labs), on Programming Language Life Cycles.

HILT 2012 **conference sessions** deal with a range of topics associated with **safe, secure and reliable software:** analyzing and proving programs (program verification at compile time, advancing compilation technology); security and safety; real-time systems; and designing and implementing languages (compiler certification issues). 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); Ellidiss, LDRA, Microsoft Research, and TASC (Silver Level); and MathWorks and Vector Software (Basic Level).

At HILT 2012 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.



Ben Brosgol
Conference Chair
AdaCore

Jeff Boleng
Program Co-Chair
Software Engineering Institute

S. Tucker Taft
Program Co-Chair
AdaCore

KEYNOTE TOPICS / FEATURED SPEAKERS

Tuesday, December 4 / 9:00 AM–10:30 AM

Programming the Turing Machine

BARBARA LISKOV
Massachusetts Institute of Technology
Department of Electrical Engineering and Computer Science
Bio sketch: sigada.org/conf/hilt2012/Barbara-Liskov.html

Turing provided the basis for modern computer science. However there is a huge gap between a Turing machine and the kinds of applications we use today. This gap is bridged by software, and designing and implementing large programs is a difficult task. The main way we have of keeping the complexity of software under control is to make use of abstraction and modularity. This talk will discuss how abstraction and modularity are used in the design of large programs, and how these concepts are supported in modern programming languages. It will also discuss what support is needed going forward.

Tuesday, December 4 / 2:00 PM–3:30 PM

Hardening Legacy C/C++ Code

GREG MORRISETT
Harvard University
School of Engineering and Applied Sciences
Bio sketch: sigada.org/conf/hilt2012/Greg-Morrisett.html

Much of our computing infrastructure (e.g., your operating system, database, networking stack, web browser) is still built using C and C++, in spite of the overwhelming language-level errors (e.g., buffer overruns, integer overflows, double-frees, etc.) that easily lead to security exploits. For both technical and economic reasons, we can't afford to rewrite this code in a type-safe language like Java, though doing so would stop a broad class of attacks.

I will discuss a range of compiler-oriented techniques that researchers have explored to try and harden C/C++ code. In one corner of the space, we have ad hoc techniques such as stack cookies and address space layout randomization that are already deployed, and have essentially no overhead, but leave gaping holes. In another corner, we have techniques such as Software Fault Isolation (SFI) and Control Flow Isolation (CFI) that have low overhead, and guarantee to enforce a particular security policy.

However, the SFI and CFI policies are relatively coarse-grained compared to type-safety, and as such forfeit some security. In yet another corner of the space is the Secure Virtual Architecture (SVA) which enforces a fine-grained, object-level integrity policy comparable to type safety.

However, SVA and related techniques can have high overhead for some code, and will generally break more programs than SFI or CFI.

All of these techniques depend upon compiler transformations, optimizations, and/or analyses, that could lead to a large trusted computing base (TCB). So I will also discuss recent research that helps to minimize the TCB via machine-checked proofs of correctness.

Wednesday, December 5 / 9:00 AM–10:30 AM

High-Assurance Cyber Military Systems (HACMS): High-Assurance Vehicles

KATHLEEN FISHER
DARPA Information Innovation Office and Tufts University
Bio sketch: sigada.org/conf/hilt2012/Kathleen-Fisher.html

Embedded systems form a ubiquitous, networked, computing substrate that underlies much of modern technological society. Such systems range from large supervisory control and data acquisition (SCADA) systems that manage physical infrastructure to medical devices such as pacemakers and insulin pumps, to computer peripherals such as printers and routers, to communication devices such as cell phones and radios, to vehicles such as airplanes and satellites. Such devices have been networked for a variety of reasons, including the ability to conveniently access diagnostic information, perform software updates, provide innovative features, lower costs, and improve ease of use.

Researchers and hackers have shown that these kinds of networked embedded systems are vulnerable to remote attack, and such attacks can cause physical damage while hiding the effects from monitors.

The goal of the HACMS program is to create technology for the construction of high-assurance cyber-physical systems, where high assurance is defined to mean functionally correct and satisfying appropriate safety and security properties. Achieving this goal requires a fundamentally different approach from what the software community has taken to date. Consequently, HACMS will adopt a clean-slate, formal methods-based approach to enable semi-automated code synthesis from executable, formal specifications. In addition to generating code, HACMS seeks a synthesizer capable of producing machine-checkable proof that the generated code satisfies functional specifications as well as security and safety policies. A key technical challenge is the development of techniques to ensure that such proofs are composable, allowing the construction of high-assurance systems out of high-assurance components.

Wednesday, December 5 / 2:00 PM–3:30 PM

Challenges for Safety-Critical Software

NANCY LEVESON
Massachusetts Institute of Technology
Department of Aeronautics and Astronautics, Engineering Systems Division
Bio sketch: sigada.org/conf/hilt2012/Nancy-Leveson.html

Much of our focus on safety-critical software has been on ensuring that the software implements the requirements. Is this enough? In the talk I will suggest some other goals that we need to consider for our software in order to avoid losses, and some potential approaches for achieving them.

Thursday, December 6 / 9:00 AM–10:30 AM

Programming Language Life Cycles

GUY L. STEELE, JR.
Oracle Labs
Bio sketch: sigada.org/conf/hilt2012/Guy-Steele.html

New programming languages keep getting invented, and (most) old languages eventually die. Many languages are eventually reduced to, if anything, a single surviving slogan or idea. (Examples: COBOL = programs look like English; SNOBOL = pattern matching on strings.) How do ideas about what programmers want or need to do drive decisions made by language designers? We'll look at some of these ideas, and also at the origin, evolution, and possible destinations of certain ideas pursued during the development of the Fortress programming language, speculating on the forces that drive these life cycles.

TUTORIALS Sunday, December 2, 2012

9:00 AM–10:30 AM	**MARTHA'S VINEYARD B** **SF1:** Design of Multitask Software: The Entity-Life Modeling Approach *Bo I. Sandén (Colorado Technical University)*	
	MARTHA'S VINEYARD A **SA1:** Leading-Edge Ada Verification Technologies: Highly Automated Ada Contract Checking Using Bakar Kiasan *Jason Belt, Patrice Chalin, John Hatcliff, and Robby (Kansas State University)*	**NANTUCKET** **SA2:** Ada 2012 Contracts and Aspects *Ed Colbert (Absolute Software)*
10:30 AM–11:00 AM	MORNING BREAK	
11:00 AM–12:30 PM	**MARTHA'S VINEYARD B** **SF1:** Design of Multitask Software *(continued)*	
	MARTHA'S VINEYARD A **SA1:** Highly Automated Ada Contract Checking Using Bakar Kiasan *(continued)*	**NANTUCKET** **SA2:** Ada 2012 Contracts and Aspects *(continued)*
12:30 PM–2:00 PM	LUNCH BREAK *(on your own)*	
2:00 PM–3:30 PM	**MARTHA'S VINEYARD B** **SF1:** Design of Multitask Software *(continued)*	
	MARTHA'S VINEYARD A **SP1:** Leading-Edge Ada Verification Technologies: Combining Testing and Verification with GNATTest and GNATProve—The Hi-Lite Project *Johannes Kanig (AdaCore)*	**NANTUCKET** **SP2:** Object-Oriented Programming with Ada 2005 and 2012 *Ed Colbert (Absolute Software)*
3:30 PM–4:00 PM	AFTERNOON BREAK	
4:00 PM–5:30 PM	**MARTHA'S VINEYARD B** **SF1:** Design of Multitask Software *(continued)*	
	MARTHA'S VINEYARD A **SP1:** Combining Testing and Verification with GNATTest and GNATProve—The Hi-Lite Project *(continued)*	**NANTUCKET** **SP2:** Object-Oriented Programming with Ada 2005 and 2012 *(continued)*

This page, left: Massachusetts State House (photo by Abigail Coyle); right: Leonard P. Zakim Bridge (photo by Todd Van Hoosear).
Next page, left: Hyatt Regency Boston (www.regencyboston.hyatt.com); right: the old and new John Hancock buildings (photo by Abigail Coyle).

TUTORIALS Monday, December 3, 2012

9:00 AM–10:30 AM	**MARTHA'S VINEYARD A** **MF1:** Safety of Embedded Software *Nancy Leveson, Cody Fleming, and John Thomas (MIT)*	
	MARTHA'S VINEYARD B **MA1:** Developing Verified Programs with Dafny *K. Rustan M. Leino (Microsoft Research)*	**NANTUCKET** **MA2:** Service-Oriented Architecture (SOA) Concepts and Implementations *Ricky E. Sward (The MITRE Corporation), Jeff Boleng (Software Engineering Institute)*
10:30 AM–11:00 AM	MORNING BREAK	
11:00 AM–12:30 PM	**MARTHA'S VINEYARD A** **MF1:** Safety of Embedded Software *(continued)*	
	MARTHA'S VINEYARD B **MA1:** Developing Verified Programs with Dafny *(continued)*	**NANTUCKET** **MA2:** Service-Oriented Architecture (SOA) Concepts and Implementations *(continued)*
12:30 PM–2:00 PM	LUNCH BREAK *(on your own)*	
2:00 PM–3:30 PM	**MARTHA'S VINEYARD A** **MF1:** Safety of Embedded Software *(continued)*	
	MARTHA'S VINEYARD B **MP1:** Multicore Programming Using Divide-and-Conquer and Work Stealing *Tucker Taft (AdaCore)*	**NANTUCKET** **MP2:** Understanding Dynamic Memory Management in Safety Critical Java *Kelvin Nilsen (Atego)*
3:30 PM–4:00 PM	AFTERNOON BREAK	
4:00 PM–5:30 PM	**MARTHA'S VINEYARD A** **MF1:** Safety of Embedded Software *(continued)*	
	MARTHA'S VINEYARD B **MP1:** Multicore Programming Using Divide-and-Conquer and Work Stealing *(continued)*	**NANTUCKET** **MP2:** Understanding Dynamic Memory Management in Safety Critical Java *(continued)*
5:30 PM–7:00 PM	DINNER BREAK *(on your own)*	
7:00 PM–10:00 PM	**NANTUCKET** SIGAda Extended Executive Committee (EEC) Meeting *(open to all)*	

CONFERENCE SESSIONS Tuesday, December 4, 2012

Analyzing and Proving Programs

8:00 AM–9:00 AM	REGISTRATION
9:00 AM–10:30 AM	**MARTHA'S VINEYARD A** **Welcome and Conference Introduction** *Ben Brosgol (HILT 2012 Conference Chair) and Ricky Sward (SIGAda Chair)*
	MARTHA'S VINEYARD A Keynote Address: Programming the Turing Machine *Barbara Liskov (MIT)*
10:30 AM–11:00 AM	MORNING BREAK / EXHIBITS IN THE CAPE COD ROOM
11:00 AM–12:30 PM	**MARTHA'S VINEYARD A** **Session: Program Verification at Compile-Time**
	Program Proving Using Intermediate Verification Languages (IVLs) like Boogie and Why3 *K. Rustan M. Leino (Microsoft Research)*
	Hi-Lite: The Convergence of Compiler Technology and Program Verification *Claire Dross, Johannes Kanig, and Edmond Schonberg (AdaCore)*
12:30 PM–2:00 PM	LUNCH BREAK / EXHIBITS IN THE CAPE COD ROOM
2:00 PM–3:30 PM	**MARTHA'S VINEYARD A** Keynote Address: Hardening Legacy C/C++ Code *Greg Morrisett (Harvard University)*
3:30 PM–4:00 PM	AFTERNOON BREAK / EXHIBITS IN THE CAPE COD ROOM
4:00 PM–5:30 PM	**MARTHA'S VINEYARD A** **Session: Advancing Compiler Technology**
	The Implementation of Compile-Time Dimensionality Checking *Vincent Pucci and Edmond Schonberg (AdaCore)*
	A Robust Implementation of Ada's Finalizable Controlled Types *Hristian Kirtchev (AdaCore)*
5:30 PM–6:30 PM	BREAK
6:30 PM–9:30 PM	Evening Social Event: Old Town Trolley Tour and Legal Sea Foods dinner

This page, left: SIGAda 2009, Tampa/St. Petersburg, Florida; center: lunch at SIGAda 2010, Fairfax, Virginia; right: SIGAda 2011, Denver, Colorado (photos by Tom Panfil).

CONFERENCE SESSIONS Wednesday, December 5, 2012
Security and Safety

8:00 AM–9:00 AM	REGISTRATION	
9:00 AM–10:30 AM	**MARTHA'S VINEYARD A** **Announcements** **SIGAda Awards** *John McCormick (Chair, SIGAda Awards Committee)*	
	MARTHA'S VINEYARD A Keynote Address: HACMS: High-Assurance Vehicles *Kathleen Fisher (DARPA)*	
10:30 AM–11:00 AM	MORNING BREAK / EXHIBITS IN THE CAPE COD ROOM	
11:00 AM–12:30 PM	**MARTHA'S VINEYARD A** **Session: Languages and Security**	
	Formal Verification of the seL4 Microkernel *Michael Norrish (NICTA (Australia))*	
	DSL for Cross-Domain Security *D. S. Hardin (Rockwell Collins)*	
	AdaCore Sponsor Presentation *Greg Gicca (AdaCore)*	
12:30 PM–2:00 PM	LUNCH BREAK / EXHIBITS IN THE CAPE COD ROOM *(exhibits close at 2pm)*	
2:00 PM–3:30 PM	**MARTHA'S VINEYARD A** Keynote Address: Challenges for Safety-Critical Software *Nancy Leveson (MIT)*	
3:30 PM–4:00 PM	AFTERNOON BREAK	
4:00 PM–5:30 PM	**Session: Languages and Safety**	
	MARTHA'S VINEYARD A **TRACK 1: Industrial Session on Safety**	**MARTHA'S VINEYARD B** **TRACK 2: Real Time Systems**
	Real-Time Java in the Modernization of the Aegis Weapon System *Kelvin Nilsen (Atego)*	Synchronization Cannot Be a Library *Geert Bosch (AdaCore)*
	Software for FAA's Automatic Data Comm Between Air Traffic Controller and Pilot *J. O'Leary (Federal Aviation Administration)*	Applicability of RT Schedulability Analysis on a Software Radio Protocol *Shuai Li (Lab-STICC/UMR), Frank Singhoff (University of Brest, France), Michel Bourdellès (THALES Communications & Security)*
	LDRA Sponsor Presentation: Managing and Migrating Existing Applications to the DO-178B Standard *Jay Thomas (LDRA)*	Ellidiss Sponsor Presentation *Tony Elliston (Ellidiss (TNI Europe))*
5:30 PM–8:00 PM	DINNER BREAK *(on your own)*	
8:00 PM–9:30 PM	**MARTHA'S VINEYARD A** GNAT "Birds-of-a-Feather" Session *Greg Gicca (AdaCore)*	

CONFERENCE SESSIONS Thursday, December 6, 2012
Designing and Implementing Languages

8:00 AM–9:00 AM	REGISTRATION
9:00 AM–10:30 AM	**MARTHA'S VINEYARD A** **Announcements** **Best Paper and Student Paper Awards** *Jeff Boleng (HILT 2012 Program Co-Chair)*
	MARTHA'S VINEYARD A Keynote Address: Programming Language Life Cycles *Guy L. Steele, Jr. (Oracle Labs)*
10:30 AM–11:00 AM	MORNING BREAK
11:00 AM–1:00 PM	**MARTHA'S VINEYARD A** **Session: Compiler Certification Issues**
	Adapting ACATS for Use with Run-Time Checks Suppressed *Dan Eilers (Irvine Complier Corp.), Tero Koskinen (Tampere, Finland)*
	Panel on Compiler Certification: Should You Trust Your Compiler? *Tucker Taft (AdaCore), Lennart Berringer (Princeton), Randy Brukardt (RR Software), Tom Plum (Plum Hall)*
	MARTHA'S VINEYARD A **Ada-Europe 2013 Conference Announcement** *Erhard Ploedereder (Ada-Europe)* **HILT 2013 Conference Announcement** *Alok Srivastava (SIGAda Vice Chair for Meetings and Conferences)*
1:00 PM	**MARTHA'S VINEYARD A** **Closing Comments and Conference Adjournment**

SOCIAL EVENT AT LEGAL SEA FOODS Tuesday, December 4, 2012

The conference social event is a trolley tour of Boston followed by a dinner at Legal Sea Foods, a well-known and highly rated restaurant that is a local institution/tradition (photo, left, courtesy of www.legalseafoods.com).

Our dinner will be at their Copley Place location. We will leave the hotel at 6:30 PM on the Old Town Trolley for a tour of Boston, arriving at the restaurant ataround 7:30 for a sit-down dinner. Fish, as you might expect, is their specialty, but the menu will also include meat and vegetarian selections. Afterwards, around 9:30 PM, we'll return to the hotel. The trolley will be available for transportation, or you can choose to walk. The distance is around amile, which should take about twenty minutes up Boylston Street and past the Public Garden and Boston Common.