# Michael W. Whalen

mike.whalen@gmail.com
http://www.cs.umn.edu/~whalen

**Work Address:**
200 Union St. 4-192
Minneapolis, MN 55455
(651) 422-8834

**Home Address:**
4709 Virginia Lane
Edina, Minnesota 55424
(952) 922-2792


## Research Interests:

Software plays an increasing role in the operation of critical systems. As these systems become more complex, ensuring software correctness becomes much more difficult. I am interested in automated formal techniques for precisely specifying, implementing, and verifying software. To support these activities, I have developed several translation and analysis tools to support formal reasoning and test case generation on a variety of commercial and research notations. I have significant experience in applying formal verification and auto-test generation techniques to production DO178B/C Level A and B avionics software development efforts.

## Areas of Experience:

Specification Languages: AADL, Simulink, StateFlow, Rhapsody, SCADE, Lustre, Esterel, Z, VDM, SCR, Statecharts

Programming Languages: Java, C/C++, Standard ML, OCaml, F#, XML/HTML, lisp, Prolog

Formal Analysis Tools: jkind, z3, CVC4, Isabelle/HOL, NuSMV/NuXMV, Prover, Kind, Dafny, ACL2, SAL, PVS

## Education:

Ph.D. Computer Science, University of Minnesota, Twin Cities, March 2005.
Thesis Topic: Trustworthy Translation of the Requirements State Machine Language without Events.

M.S. Computer Science, University of Minnesota, Twin Cities, April 2000.
Thesis Topic: A Formal Semantics for the Requirements State Machine Language without Events.

B.A. Computer Science with Honors, Luther College, May, 1994.

## PhD Students Graduated:

Tuan-Hung Pham, March, 2014. Thesis title: *Verification of Recursive Data Types using Abstractions*. Currently employed at Google Inc, Seattle, WA.

## Publications:

**Book Chapters:**

Michael W. Whalen, David Greve, Lucas Wagner, Steven P. Miller, Model Checking Information Flow. In *Design and Verification of Microprocessor Systems for High-Assurance Applications.* D. Hardin, Ed. Springer, 2010.

**Journal Publications:**

Tuan-Hung Pham, Andrew Gacek, and Michael W. Whalen, Reasoning about Algebraic Datatypes with Abstractions, *Journal of Automated Reasoning [Accepted – To Appear]*

Michael W. Whalen, Darren Cofer, and Andrew Gacek, Requirements and Architectures for Secure Vehicles, *IEEE Software – On Requirements Column*, Volume 33 (4), July-August, 2016.

Ajitha Rajan, Gregory Gay, Michael W. Whalen, Matt Staats, and Mats P.E. Heimdahl, The Effect of Program and Model Structure on the Effectiveness of MC/DC Test Adequacy Coverage, *ACM Transactions on Software Engineering and Methodology,* Volume 25 (3), July, 2016.

Gregory Gay, Matt Staats, Michael W. Whalen, and Mats P.E. Heimdahl, Automated Oracle Data Selection Support, *IEEE Transactions on Software Engineering ,* Volume 41, Number 11, November, 2015

Anitha Murugesan, Sanjai Rayadurgam, Michael W. Whalen, and Mats P.E. Heimdahl, Design Considerations for Modeling Modes in CPS, *IEEE Design & Test,* Volume 32, Number 5, October, 2015.

Gregory Gay, Matt Staats, Michael W. Whalen, and Mats P.E. Heimdahl, The Risks of Coverage-Directed Test Case Generation, *IEEE Transactions on Software Engineering,* Volume 41, Number 8, August, 2015.

Michael W. Whalen, Andrew Gacek, Darren Cofer, Anitha Murugesan, Mats Heimdahl, and Sanjai Rayadurgam. Your "What" Is My "How": Iteration and Hierarchy in System Design, *IEEE Software,* Volume 30 (2), March, 2013.

Willem Visser, Matthew B. Dwyer, and Michael W. Whalen, The Hidden Models of Model Checking. *Journal of Software and Systems Modeling*, Volume 11, Issue 4, October 2012.

Steven P. Miller, Michael W. Whalen, and Darren D. Cofer. Software Model Checking Takes Off. *Communications of the ACM*, February, 2010.

Steven P. Miller, Alan C. Tribble, Michael W. Whalen, and Mats P.E. Heimdahl. Proving the Shalls: Early Validation of Requirements through Formal Methods, *Journal of Software Tools for Technology Transfer*. Volume 8 Issue 4, August 2006.

Mats P.E. Heimdahl, Yunja Choi, and Michael W. Whalen. Deviation Analysis: A New Use for Model Checking, *Automated Software Engineering*, Volume 12, Number 3, July, 2005.

Jeffrey M. Thompson, Michael W. Whalen, and Mats P.E. Heimdahl. Requirements Capture and Evaluation in Nimbus: A Case Study. *Journal of Universal Computer Science*, Volume 6, Issue 7, July, 2000.

**Refereed Conference and Workshop Publications:**

Elaheh Ghassabani, Andrew Gacek, and Michael W. Whalen. Efficient Generation of Inductive Validity Cores for Safety Properties. *FSE2016: ACM Sigsoft International Symposium on the Foundations of Software Engineering*, Seattle, WA, November 13-19, 2016. *[Accepted – To Appear]*

Michael W. Whalen, Anitha Murugesan, Elaheh Ghassabani, and Mats P.E. Heimdahl. *Complete Traceability for Requirements in Satisfaction Arguments.* 24th International Requirements Engineering Conference (RE@Next! Track), Beijing, China, September 12-16, 2016. *[Accepted – To Appear]*

John Backes, Michael W. Whalen, and Andrew Gacek. On Implementing Real-time Specification Patterns Using Observers. *NASA Formal Methods Conference,* Minneapolis, MN, June, 2016.

Andreas Katis, Michael W. Whalen, and Andrew Gacek. Towards Synthesis from Assume-Guarantee Contracts involving Infinite Theories: A Preliminary Report. *4th FME Workshop on Formal Methods in Software Engineering,* Austin, TX, May 15, 2016.

Dongjiang You, Sanjai Rayadurgam, Michael W. Whalen, Mats P.E. Heimdahl, and Gregory Gay. Efficient Observability-based Test Generation by Dynamic Symbolic Execution. *26th International Symposium on Software Reliability Engineering (ISSRE 2015)*, Gaithersburg, MD, November 2-5, 2015.

Michael W. Whalen, Sanjai Rayadurgam, Elaheh Ghassabani, Anitha Murugesan, Oleg Sokolsky, Mats Heimdahl, and Insup Lee. Hierarchical Multi-Formalism Proofs for Cyber-Physical Systems, *13th ACM-IEEE International Conference on Formal Methods and Models for System Design (MEMOCODE 2015),* Austin, Texas, September 21-23, 2015. [Short Paper]

Andreas Katis, Andrew Gacek, and Michael W. Whalen. Machine-Checked Proofs for Realizability Checking Algorithms, *7th Conference on Verified Software: Theories, Tools, and Experiments (VSTTE 2015)*, San Fransisco, CA, USA, July 18-19, 2015.

Michael W. Whalen, Suzette Person, Neha Rungta, Matt Staats, and Daniella Grijincu. A flexible and non-intrusive approach for computing complex structural coverage metrics, *International Conference on Software Engineering*, Florence, Italy, May, 2015.

Anitha Murugesan, Neha Runga, Oksana Tkachuck, Suzette Person, Michael W. Whalen, and Mats P.E. Heimdahl, Are We There Yet? Determining the Adequacy of Formalized Requirements and Test Suites, *NASA Formal Methods Conference,* Pasadena, CA, April 27-29, 2015.

John Backes, Darren Cofer, Steven Miller, and Michael W. Whalen, Requirements Analysis of a Quad-Redundant Flight Control System, *NASA Formal Methods Conference,* Pasadena, CA, April 27-29, 2015.

Andrew Gacek, Andreas Katis, Michael W. Whalen, and John Backes, Towards Realizability Checking of Contracts using Theories, *NASA Formal Methods Conference,* Pasadena, CA, April 27-29, 2015.

Andrew Gacek, John Backes, Darren Cofer, Konrad Slind, and Michael W. Whalen, Resolute: An Assurance Case Language for Architecture Models, *International Conference on High Integrity Languages and Tools,* Portland, Oregon, October 18-21, 2014.

Anitha Murugesan, Mats P.E. Heimdahl, Michael W. Whalen, Sanjai Rayadurgam, John Komp, Lian Duan, Baek-Gyu Kim, Oleg Sokolsky, and Insup Lee, From Requirements to Code: Model-Based Development of a Medical Cyber Physical System, *Symposium on Foundations of Health Information Engineering and Systems (FHIES) and the Software Engineering in Healthcare (SEHC) Workshop,* Washington DC, July 17-18, 2014.

Anitha Murugesan, Lu Feng, Mats P.E. Heimdahl, Sanjai Rayadurgam, Michael W. Whalen and Insup Lee, Exploring the Twin Peaks Using Probabilistic Verification Techniques, *4th International Workshop on the Twin Peaks of Requirements and Architecture*, Hyderabad, India, June 1, 2014.

Jason Biatek, Neha Rungta, Michael W. Whalen, and Oksana Tachuk, Helping System Engineers Bridge the Peaks, *4th International Workshop on the Twin Peaks of Requirements and Architecture*, Hyderabad, India, June 1, 2014.

Michael W. Whalen, Anitha Murugesan, Sanjai Rayadurgam, and Mats P.E. Heimdahl, Structuring Simulink Models for Verification and Reuse, *6th International Workshop on Modeling in Software Engineering,* Hyderabad, India, June 2-3, 2014.

Jason Biatek, Michael W. Whalen, Mats P.E. Heimdahl, Sanjai Rayadurgam, and Michael R. Lowry, Analysis and Testing of PLEXIL Plans, *2nd FME Workshop on Formal Methods in Software Engineering,* Hyderabad, India, June 3, 2014.

Gregory Gay, Michael W. Whalen, Mats P.E. Heimdahl, Matt Staats, Moving the Goalposts: Coverage Satisfaction is not Enough, *7th International Workshop on Search-Based Software Testing*, Hyderabad, India, June 2-3, 2014.

Anitha Murugesan, Oleg Sokolsky, Sanjai Rayadurgam, Michael Whalen, Mats Heimdahl, and Insup Lee. Linking Abstract Analysis to Concrete Design: A Hierarchical Approach to Verify Medical CPS Safety, *International Conference on Cyber-Physical Systems,* Berlin, Germany, April 14-17, 2014.

Tuan-Hung Pham and Michael W. Whalen. Parameterized Abstractions in Unrolling-Based Decision Procedure for Algebraic Data Types, *8th International Workshop on Constraints in Formal Verification*. San Jose, California, November 21, 2013.

Anitha Murugesan, Michael W. Whalen, Sanjai Rayadurgam, and Mats P.E. Heimdahl, Compositional Verification of a Medical Device System, *Proceedings of the 2nd Conference on High Integrity Languages and Tools.* Pittsburgh, PA, November 13-15, 2013. **Best Paper of HILT 2013**

Tuan-Hung Pham and Michael W. Whalen. RADA: A Tool for Reasoning about Algebraic Data Types with Abstractions, *Proceedings of the 9th Joint Meeting of the European Software Engineering Conference and the Symposium on Foundations of Software Engineering.* St. Petersburg, Russia, August 18-26, 2013. [Tool Paper]

Michael W. Whalen, Gregory Gay, Dongjiang You, Matt Staats, and Mats P.E. Heimdahl. Observable Modified Condition / Decision Coverage. *35rd International Conference on Software Engineering,* San Francisco, CA, May 21-28, 2013.

Tuan-Hung Pham and Michael W. Whalen. An Improved Unrolling-Based Decision Procedure for Algebraic Data Types, *Verified Software: Theories, Tools, and Experiments (VSTTE 2013).* Atherton, CA, May 17-19, 2013.

David Hardin, Konrad Slind, Michael W. Whalen, and Tuan-Hung Pham. The Guardol Environment, *First Conference on High-Integrity Languages and Tools (HILT 2012),* Boston, MA, Dec. 2 – 6, 2012.

Daniel Balasubramanian, Corina S. Pasareanu, Jason Biatek, Michael W. Whalen, Gabor Karsai, Michael Lowry. Improving Symbolic Execution for Statecharts Formalisms. *9th Workshop on Model Design, Verification and Validation,* September 30, 2012.

Michael W. Whalen, Mats Heimdahl, and Anitha Murugesan, Your What is My How: Why Requirements and Architectural Design Should Be Iterative, *Proceedings of the TwinPeaks Workshop 2012*, Chicago, Illinois, September 25, 2012.

Darren Cofer, Andrew Gacek, Steven Miller, Michael W. Whalen, Brian LaValley, and Lui Sha. Compositional Verification of Architectural Models. *Proceedings of the Fourth NASA Formal Methods Symposium,* Norfolk, VA, April 3-5, 2012

Temesghen Kahsai, Pierre-Loic Garoche, Cesare Tinelli, and Michael W. Whalen. Incremental Verification with Mode Machine Invariants in State Machines. *Proceedings of the Fourth NASA Formal Methods Symposium,* Norfolk, VA, April 3-5, 2012

Daniel Balasubramanian, Corina S. Pasareanu, Jason Biatek, Michael W. Whalen, Gabor Karsai, Michael Lowry. Integrating Statecharts Components in Polyglot. *Proceedings of the Fourth NASA Formal Methods Symposium,* Norfolk, VA, April 3-5, 2012

David Hardin, Konrad Slind, Michael W. Whalen, and Tuan-Hung Pham. The Guardol Language and Verification System, *18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS),* Tallinn, Estonia, March 24 – April 1, 2012.

Gregory Gay, Matt Staats, Michael W. Whalen, and Mats P.E. Heimdahl. On the Danger of Coverage Directed Test Case Generation, *15th International Conference on Fundamental Approaches to Software Engineering (FASE),* Tallinn, Estonia, March 24- April 1, 2012.

David Hardin, Konrad Slind, Michael W. Whalen, and Tuan-Hung Pham. Introduction to the Guardol Language and Verification System, *4th Annual Layered Assurance Workshop,* Orlando, Florida, December 5-6, 2011.

Daniel Balasubramanian, Corina S. Pasareanu, Michael W. Whalen, Gabor Karsai, Michael Lowry. Polyglot: Modeling and Analysis for Multiple Statechart Formalisms, *Proceedings of the International Symposium on Software Testing and Analysis (ISSTA),* Toronto, Ontario, Canada, July 17-21, 2011.

Matt Staats, Michael W. Whalen, and Mats P.E. Heimdahl. Better Testing Through Oracle Selection. *New Ideas and Emerging Results Track, 33rd International Conference on Software Engineering,* Honolulu, Hawaii, May 21-28, 2011.

Matt Staats, Michael W. Whalen, and Mats P.E. Heimdahl. Programs, Tests, and Oracles: The Foundations of Testing Revisited. *33rd International Conference on Software Engineering,* Honolulu, Hawaii, May 21-28, 2011. **ICSE 2011 Distinguished Paper**

Michael W. Whalen, Patrice Godefroid, Leonardo Mariani, Andrea Polini, Nikolai Tillman, and Willem Visser. FITE: Future Integrated Testing Environment. *Workshop on the Future of Software Engineering Research 2010 (FoSER),* Santa Fe, New Mexico, November 7-8, 2010.

Matt Staats, Michael W.Whalen, Ajitha Rajan, and Mats P.E. Heimdahl. Coverage Metrics for Requirements-Based Testing: Evaluation of Effectiveness. *Proceedings of the Second NASA Formal Methods Symposium.* Washington, D.C., April 13-15, 2010.

David Hardin, T. Douglas Hiratzka, D. Randolph Johnson, Lucas Wagner, and Michael Whalen. Development of Security Software: A High-Assurance Methodology. *Proceedings of the 11th International Conference of Formal Engineering Methods (ICFEM 2009)*, Rio de Janeiro, Brazil, December, 2009.

Ajitha Rajan, Michael W Whalen, Matt Staats, and Mats P.E. Heimdahl. Requirements Coverage as an Adequacy Measure for Conformance Testing. *Proceedings of the 10th International Conference on Formal Engineering Methods (ICFEM 2008)*, Kitakyushu City, Japan, October, 2008.

Michael W. Whalen, Mats P.E. Heimdahl, Ajitha Rajan, and Matt Staats. On MC/DC and Implementation Structure: An Empirical Study. Proceedings of the 27th Digital Avionics Systems Conference (DASC'08). St. Paul, MN, October 2008. **Best Paper of DASC Software Design Session**

Darren Cofer, Michael W. Whalen, Steven P Miller. Software Model Checking for Avionics Systems. Proceedings of the 27th Digital Avionics Systems Conference (DASC'08). St Paul, MN, October 2008

Ajitha Rajan, Michael W. Whalen, and Mats P.E. Heimdahl. The Effect of Program and Model Structure on MC/DC Test Adequacy Coverage. *Proceedings of the 30th International Conference on Software Engineering (ICSE 2008),* Leipzig, Germany, May, 2008. **ICSE 2008 Distinguished Paper**

Michael W. Whalen, Darren Cofer, Steven Miller, Bruce Krogh, and Walter Storm. Integration of Formal Analysis into a Model-Based Software Development Process. *12th International Workshop on Industrial Critical Systems (FMICS 2007),* Berlin, Germany, July, 2007.

Jimin Gao, Michael W. Whalen, and Eric Van Wyk. Extending Lustre with Timeout Automata. *Synchronous Languages, Applications, and Programming (SLA++P) 2007,* Braga, Portugal, March, 2007.

Michael W. Whalen, Ajitha Rajan, and Mats P.E. Heimdahl. Coverage Metrics for Requirements-Based Testing. *Proceedings of the International Symposium on Software Testing and Analysis (ISSTA) 2006,* Portland, Maine, July, 2006.

Michael W. Whalen. Certificate Management: A Practitioner's Perspective, *Workshop on Software Certificate Management (SoftCeMent '05)*, November, 2005.

Anjali Joshi, Steven P. Miller, Michael W. Whalen, and Mats P. E. Heimdahl. A Proposal for Model-Based Safety Analysis. In *Proceedings of the 24th Digital Avionics Systems Conference (DASC'05),* Washington, D.C., October, 2005. **Best Paper of the DASC Open Systems Architecture track**

Johann Schumann, Bernd Fischer, Michael W. Whalen, Jon Whittle. Certification Support for Automatically Generated Programs. In *Proc. HICSS'36: Hawaiian Int'l Conf. on System Sciences,* Big Island, HI, January 2003.

Mats P.E. Heimdahl, Yunja Choi, and Michael W. Whalen. Deviation Analysis Through Model Checking. *Proceedings of the 17th IEEE International Conference on Automated Software Engineering,* Edinburgh, UK, September, 2002. **ASE 2002 Distinguished Paper**

Michael W. Whalen, Bernd Fischer, and Johann Schumann. Certifying Synthesized Code. *Proceedings of Formal Methods Europe 2002,* Copenhagen, Denmark, July 2002

Michael W. Whalen, Bernd Fischer, and Johann Schumann. AutoBayes/CC – Combining Program Synthesis with Automatic Code Certification. *Proceedings of Conference on Automated Deduction 18,* Copenhagen, Denmark, July 2002.

Michael W. Whalen. High Assurance Code Generation for State-Based Formalisms (for Doctoral Symposium). *Proceedings of the 22nd International Conference on Software Engineering,* Limerick, Ireland, June 2000.

Michael W. Whalen and Mats P.E. Heimdahl. On the Requirements on High Integrity Code Generation. *Proceedings of the Fourth IEEE High Assurance in Systems Engineering Workshop*, Washington DC, November, 1999.

Michael W. Whalen and Mats P.E. Heimdahl. An Approach to Automatic Code Generation for Safety-Critical Systems. Short Paper in *Proceedings of the 14th IEEE International Conference on Automated Software Engineering*, Orlando, FL, October, 1999.

Mats P.E. Heimdahl, Jeffrey M. Thompson, and Michael W. Whalen. On the Effectiveness of Slicing Hierarchical State Machines: A Case Study. In *Proceedings of the Twenty-fourth EUROMICRO Conference*, volume 1, 1998.

Mats P.E. Heimdahl and Michael W. Whalen. Reduction and Slicing of Hierarchical State Machines. *Proceedings of the Fifth ACM SIGSOFT Symposium on the Foundations of Software Engineering*, September, 1997.

**Other Publications:**

Kerianne Gross, Matthew Clark, Jonathan Hoffman, Aaron Fifarek, Kuldip Rattan, Eric Swenson, Michael W. Whalen, Lucas Wagner. Formally Verified Run Time Assurance Architecture of a 6U CubeSat Attitude Control System. *AIAA SciTech Conference.* San Diego, CA, January, 2016.

Andrew Gacek, Andreas Katis, Michael W. Whalen, and Darren Cofer. Hierarchical Circular Compositional Reasoning, UMN Tech Report 2014-1, www.umsec.umn.edu/publications

David Hardin, T. Douglas Hiratzka, D. Randolph Johnson, Lucas Wagner, and Michael Whalen. A High-Assurance Methodology for the Development of Security Software. *The Next Wave*, National Security Agency, October, 2011.

Michael W. Whalen, A Parametric Semantics for Statecharts, UMN Tech Report 2010-1, www.umsec.umn.edu/publications

Darren Cofer, Michael W. Whalen, and Steven P. Miller, Model-Checking of Safety-Critical Software for Avionics, *European Research Consortium for Infomatics and Mathematics (ERCIM) News*, Number 75, October, 2008.

Anjali Joshi, Michael W. Whalen, and Mats P.E. Heimdahl, Model-Based Safety Analysis Final Report, *NASA Contractor Report NASA/CR-2006-213953*, February 2006.

Michael W. Whalen, Lucas G. Wagner, John D. Innis, and Steven P. Miller, ADGS-2100 Adaptive Display & Guidance System Window Manager Analysis Final Report, *NASA Contractor Report NASA/CR-2006-213952*, February 2006.

Steven P Miller, Michael W. Whalen, Daniel O'Brien, Mats P.E. Heimdahl, and Anjali Joshi, A Methodology for the Design and Verification of Globally Asynchronous/Locally Synchronous Architectures. *NASA Contractor Report NASA/CR-2005-213912*, November 2005.

Steven P Miller, Elise A. Anderson, Lucas G. Wagner, Michael W. Whalen, and Mats P.E. Heimdahl. Formal Verification of Flight Critical Software, in *Proceedings of the AIAA Guidance, Navigation, and Control Conference and Exhibit*, San Francisco, August 15-18, 2005.

Michael W. Whalen and Mats P.E. Heimdahl. Representing the Unknown in Specification Languages. *Technical Report TR 00-024,* University of Minnesota, Department of Computer Science and Engineering, Minneapolis, MN 2000.

Mats P.E. Heimdahl, Jeffrey M. Thompson, and Michael W. Whalen. Executing State-based Specifications in a Heterogeneous Environment. *Technical Report TR 98-029*, University of Minnesota, Department of Computer Science and Engineering, Minneapolis, MN, 1998.

## Invited and Plenary/Keynote Talks:

*Rigorous Testing Approaches using Symbolic Search,* Invited talk at The Mathworks, March, 2016.

*Up and Out: Scaling Formal Analysis Using Model-Based Development and Architecture Modeling,* **Keynote address** at the 6th Working Conference on Verified Software: Theories, Tools and Experiments, Vienna, Austria, July, 2014.

*Engineering Support for Virtual Integration,* **Keynote address** at the International Workshop on the Twin Peaks of Requirements and Architecture, Hyderabad, India, June, 2014.

*Multi-Level Requirements, Architecture, and Verification: the Good, the Bad, and the Ugly*, IFIP Working Group on Requirements, February, 2014.

*Up and Out: Scaling Formal Analysis Using Model-Based Development and Architecture Modeling.* Invited talk at High Integrity Languages and Tools Conference (HILT) 2103, November, 2013.

*Scaling Software Verification and Validation.* Invited talk at the GE Controls Seminar, September, 2013.

*Why We Model: Using MBD Effectively in Critical Domains.* **Keynote address** at the Modeling in Software Engineering Workshop (MiSE) 2013, May, 2013.

*Observable Modified Condition Decision Coverage.* University of Western Ontario, February, 2013.

*The Future of Software V&V,* Lockheed Martin/IEEE Computer Society Webinar, January, 2013.

*Scaling Up and Out: Formal Requirements at Different Levels of Abstraction*, **Keynote address** at the Analytical Virtual Integration of Cyber-Physical Systems (AVICPS) Workshop, December, 2012.

*Building a Compliant Verification & Validation Program: Knowing the Ropes,* OPAL Medical Device Summit, Bloomington, MN, September, 2012.

*Model-Based Development: Benefits and Pitfalls in Practice,* Webinar with GE Research, August, 2012.

*Reasoning Challenges for Guard Applications,* EPFL School of Computer and Communication Sciences Summer Research Institute, Lausanne, Switzerland, June, 2012.

*Scaling Up and Out: Formal Requirements at Different Levels of Abstraction*, IFIP Working Group on Requirements, February, 2012

*Proving the Shalls in Practice: Experience with Industrial Formal Analysis*, **Keynote address** at the 19th Annual Requirements Engineering Conference, August, 2011

*The Future of Software Testing:* Medtronic Technical Forum, June, 2011

*The Future of Software Engineering:* (with Mats Heimdahl) Medtronic Technical Forum, April, 2011

*Next-Generation V&V Techniques for Medical Devices,* OPAL Medical Device Summit, March, 2011

*Proving the Shalls in Practice: Experience with Industrial Formal Analysis*, IFIP Working Group on Requirements, February, 2011

*The Future of Software Testing:* CodeFreeze 2011 **Keynote Talk**, January, 2011.

*Analysis Engines:* UMN Invited Colloquium Talk, December, 2010

*Security and Software Engineering:* TwinSPIN, December, 2010

*Model Checking:* Midwest Verification Day **Keynote Talk**, September, 2010.

*Semantics of Statecharts.* CMU CMACS Lecture Series, Pittsburgh, PA, April, 2010.

*Formal Methods for Avionics.* The Mathworks, Natick, MA, March, 2010.

*Understanding Software Requirements and Conducting Effective V&V Within Challenging Development Schedules,* OPAL Medical Devices Summit Panel, March, 2010.
*Semantics of Statecharts.* NASA Ames, Sunnyvale, CA, February, 2010.
*Beyond Static Code Analysis.* UMSEC Summer Software Symposium: Static Code Analysis and Complex Medical Devices, Minneapolis, MN, July, 2009.
*Formal Verification of Numerically Intensive Avionics Models.* Workshop on Numerical Software Verification (NSV) **Keynote talk**, San Francisco, CA, April, 2009.
*Formal Methods for Critical Systems.* Digital Avionics Systems Conference (DASC) **Plenary talk**, St. Paul, MN, October, 2008.
*Formal Tools for Mixed Criticality Architectures*. Cyber-Physical Systems Week, St. Louis, MO, April, 2008.
*Integration of Formal Analysis into a Model-Based Development Process.* Boston Scientific Corporation, January, 2008.
*Formal Verification of Avionics Software in a Model-Based Development Process.* 1st International Workshop on Aerospace Software Engineering (AeroSE 2007), Minneapolis, MN, May, 2007.
*Getting it Really Right – Software Development for Highly Critical Systems*. Twin Cities Software Process Improvement Network (TwinSPIN), January 2006.
*Affordable High-Assurance Systems*. Guidant Corporation, November 2005.
*Proving the Shalls*. University of Minnesota Software Engineering Center, October 2005.
*The NIMBUS RSML-e Simulator:* Automated Software Engineering Conference (ASE) 2002, October, 2002
*Using Java in Embedded Devices*. Datacard Corporation, March 1998.

## Tutorials:

*Compositional Verification using AADL and the Assume Guarantee Reasoning Environment (AGREE).* Full-day tutorial at the Formal Methods Conference, Limassol, Cyprus, November 2016
*Model-Based Development: Benefits and Pitfalls in Practice*. Half-day tutorial at the Summer Software Symposium, July, 2011
*Software Model Checking.* Lockheed Martin Inc., August 2006
*From Research to Industry: The Role of Software Engineering Standards*. Associated with Automated Software Engineering (ASE) 2002, October, 2002.

## Teaching:

*Csci8802: Advanced Software Engineering.* University of Minnesota, Spring Semester 2015
*SEng 5861: Software Architecture.* University of Minnesota, Fall Semester 2014, 2013, 2012, 2011, 2010
*SEng 5841: Model-Based Software Development and Analysis.* University of Minnesota, Spring Semester 2007

## Employment:

University of Minnesota, Computer Science Department. Minneapolis, Minnesota.

**Director, University of Minnesota Software Engineering Center** 7/2015 to present

**Management:** Managing research center with > $1M annual budget and 3 full-time employees as well as graduate students, post-docs, adjunct faculty, and other long term temporary employees.

**Masters of Science in Software Engineering (MSSE) Program:** Responsible for managing program, recruiting students, and acting as Director of Graduate Studies (DGS) role for MSSE program. MSSE program provides a thorough grounding in software engineering principals and technical leadership for working developers.

**Research:** Automated checking of *realizability* of Assume/Guarantee contracts involving safety properties over infinite theories, and *synthesis:* derivation of witness implementations for contracts involving infinite theories. Generation of *Inductive Validity Cores* to provide traceability for inductive proofs. Real-time specification patterns for assume/guarantee reasoning. Continuation of research from program director position (see below).

**Program Management:**
[Under submission] 2016 PI: Snow Crash project (ONR): $300k PoP 6/2017 – 6/2020
2016 PI: Systems of Systems Integration Technology and Experimentation Phase 2 project (DARPA): $500k PoP 11/2016 – 11/2019
2016 PI: HACMS TACMS project (DARPA) $30k
2016 PI: Advanced Modeling and Safety Engineering (AMASE) project (NASA): $210k PoP 7/2016-6/2019
2015 Co-I: CFAR project (DARPA): $203k

**Program Director, University of Minnesota Software Engineering Center** 11/2009 to 7/2015

**Research:** Investigating coverage metrics for testing that are invariant to simple manipulations of code structure (Observable MCDC), and metrics for requirements-based testing. Extended existing decision procedures for reasoning about algebraic datatypes with abstractions to support combinations of abstractions (associative catamorphisms), and created the RADA tool for analysis of verification conditions involving algebraic datatypes. Created new foundations and tools for compositional reasoning of architectural models with colleagues at Rockwell Collins (AGREE) along with algorithms for checking *realizability* of contracts. Created techniques for efficient measurement of source-level MCDC on multicore processors and symbolic analysis. Co-inventor of Guardol domain-specific language for Guard (firewall) applications.

**Masters of Science in Software Engineering (MSSE) Program:** Assisting with management, recruiting, and Director of Graduate Studies (DGS) roles for MSSE program. MSSE program provides a thorough grounding in software engineering principals and technical leadership for working developers.

**Program Management:**
2014 Co-I: Systems of Systems Integration Technology and Experimentation (DARPA): $305k
2013 Co-I: Verification and Validation in Planning Systems (NASA): $417k
2013 PI: Compositional Verification of Flight-Critical Systems (NASA Contract # NNA13AA21C, PO 4504982612) $335k
2012 Co-I: Generating Tests to Satisfy Complex Test Adequacy Coverage of Models and Source Code with Java Pathfinder (NASA – Extended Scope): $80k
2012 PI: Application of Guardol Technology III (NSA): $73k
2012 PI: HACMS (DARPA Agreement # FA8750-12-9-0179) : $850K
2011 PI: Application of Guardol Technology II (NSA): $21k
2010 PI: Application of Guardol Technology (NSA): $64k
2010 PI: META II – Formal Analysis of Architecture Design Patterns (DARPA): $116K
2010 Co-I: SI2-SSE: Software Infrastructure For Partitioning Sparse Graphs on Existing and Emerging Computer Architectures (NSF): $499K
2010 Co-I: NSF grant CNS-1035715: Assuring the safety, security, and reliability of medical device cyber physical systems (NSF) $1.45M

Rockwell Collins, Inc. Advanced Technology Center, Minneapolis, Minnesota

**Sr. Software Engineer** 6/2003 to 11/2009

**Research:** Created approach for automatically generating test cases from formal requirements written in temporal logic. Created optimizations for efficient translation of Simulink and StateFlow into formal analysis tools. Researched approaches for representing and reasoning about asynchrony and GALS architectures using synchronous languages. Investigated the effect on fault-finding of MC/DC adequate test cases given different functionally-equivalent models with different syntactic properties. Created an accurate and efficient approach for information-flow (non-interference) analysis using model checking.

**Development:** Created the *Gryphon* tool suite, which translates Simulink/StateFlow and SCADE models into a variety of back-end analysis tools, including NuSMV, PVS, ACL2, SAL, BAT, Prover, and Kind, and programming languages: Java, C, and Ada. Gryphon supports functional verification, automated verification of runtime safety properties, test-case generation, and simulation. Used Gryphon to lead large analysis efforts:

- The ADGS-2100 Display Window Manager, a commercial DO178B Level A avionics system containing over 16000 Simulink blocks and 4000 subsystems. Proved 573 requirements and found 98 errors over the course of the analysis.
- CerTA FCS Redundancy Manager. Compared model checking to test on UAV redundancy management software. On same model with same requirements, model checking required 50% less effort than traditional test and found 12 errors vs. 0 errors in test.
- High Speed Crypto Controller: Proved the correctness of high-speed crypto controller implemented in Simulink from formal requirements in Z.

**Program Management:** Led CerTA FCS and CerTA CPI programs (total: $750K) AFRL-funded projects using Gryphon to demonstrate applicability of model checking to UAV models from Lockheed Martin Aerospace. Finished both projects on time and on budget with excellent reviews.

University of Minnesota, Computer Science Department. Minneapolis, Minnesota.

**Adjunct Faculty** 1/2007 to 6/2007

**Teaching:** Co-taught the *Model-Based Software Development and Analysis* class for the Masters of Software Engineering program at the University of Minnesota. Developed syllabus, gathered class materials, defined class projects, and lectured on topics related to model-based development.

Research Institute for Advanced Computer Science at NASA Ames. Sunnyvale, California.

**Research Assistant** 6/2001 to 9/2001

**Research:** Researched techniques for combining program synthesis with code certification (proof-carrying code). This approach allows automatic verification of complex safety properties on autogenerated programs, and is both more scalable and capable than existing approaches.

University of Minnesota, Computer Science Department. Minneapolis, Minnesota.

**Research Assistant** 1/1997 to 6/2003

**Research:** Participated in research of several aspects of safety-critical reactive systems. With Professor Mats Heimdahl, wrote the formal semantics of the RSML$^{-e}$ language using the Z specification language. Investigated strengths and weaknesses of several formal specification techniques for embedded systems including Z, B, Statecharts, Modecharts, and VDM.

**Development:** Helped create the *NIMBUS* development toolset, allowing simulation, static analysis, and code-generation of specifications written in the RSML$^{-e}$ language. The toolset is multi-threaded and allows asynchronous input from several sources: COM components, data files, and Win32 clocks. Although the toolset is large (>100,000 lines of code), it is organized around a small, straightforward set of classes, and is designed for extension. System simulation can occur between multiple copies of the toolset, VBA applications (e.g. Access, Excel, etc.), and hardware (e.g. National Instruments DAQ products). The toolset utilizes several OO design patterns including Visitor, Command, Observer/Observable, and Bridge.

**Teaching Assistant** 9/1996 to 1/1997

Assisted with introductory FORTRAN course, giving recitations, grading, holding office hours for student questions, and maintaining the course web site.

West Group, IS Department. Eagan, Minnesota.

**Senior Software Engineer** 7/1994 to 9/1996, 6/1997 to 9/1997

Worked on several aspects of an in-house multi-platform transaction monitor (WIPC), including porting WIPC from Unix to Windows NT, designing a C++ WIPC API, and implementing a WIPC proxy server that allowed Windows 3.1 clients to access WIPC services. Used Netscape Commerce Server to build prototype e-commerce web sites, using Java and CORBA (Orbix Transaction Server).

## Affiliations and Activities:

NSF Panelist, IEEE, ACM, IFIP 2-9 Working Group.

**Chair of Conference or Workshop**

Finance Chair, NASA Formal Methods Conference 2016
Chair, CodeFreeze Workshop, 2016, 2015, 2014, 2013, 2012
Program Committee co-chair, Automated Software Engineering (ASE) 2015
Student Research Competition co-chair, ICSE 2015
Doctoral Symposium co-chair, Automated Software Engineering 2014
Industrial and Experience Track co-chair, ICSE 2012
Finance Chair, Requirements Engineering Conference 2012
Co-chair, Midwest Verification Day Workshop 2011

**Journal Reviewer for:**

IEEE Transactions on Software Engineering (TSE) 2016, 2015, 2014, 2013, 2012, 2011, 2010, 2006
ACM Transactions on Embedded Systems 2015, 2014
Science of Computer Programming (SCP) 2015, 2014, 2013
Software and Systems Modeling (SOSYM) 2015
Requirements Engineering Journal 2014
Journal of Software and Systems Modeling 2014, 2013
ACM Transactions on Software Engineering (TOSEM) 2012, 2011, 2010, 2006, 2005
ACM Computing Surveys 2011
Journal of Empirical Software Engineering (ESE) 2013, 2012
International Journal on Software Tools for Technology Transfer (STTT) 2006, 2005
Journal of Automated Software Engineering (ASE) 2005, 2004

**Program Committee Member / Program Board Member of**:

Formal Techniques for Safety-Critical Systems (FTSCS) 2016, 2015, 2014, 2013
Formal Methods conference (FM) 2016, 2015, 2012
Verified Software: Theories, Tools, and Experiments (VSTTE) 2016
Automated Software Engineering (ASE) 2016, 2014, 2012, 2011, 2009
Models conference (MODELS) 2016, 2014, 2013
Workshop on Modeling in Software Engineering (MiSE) 2016
International Conference on Information Technology for Organizations Development (IT4OD) 2016
International Conference on Software Engineering (ICSE) 2016, 2014
ICSE Student Research Competition (ICSE SRC) 2016, 2014
Runtime Verification (RV) 2016, 2014
NASA Formal Methods (NFM) 2015, 2014, 2013, 2012, 2011, 2010, 2009
International Conference on Software Testing (ICST) 2015, 2014, 2013
International Conference on Model-Driven Engineering and Software Development (MODELSWARD) 2015
Analysis of Model Transformations Workshop (AMT) 2015, 2013, 2012
Conference on Software Language Engineering (SLE) 2014, 2008
International Workshop on Requirements Engineering and Testing (RET) 2014
Formal Integrated Development Workshop (F-IDE) 2014
Requirements Engineering (RE) 2014
Workshop on the Twin Peaks of Requirements and Architecture (TwinPeaks) 2014, 2013
SPIN 2014
Embedded Software (EMSOFT) 2013
ICST Tools Track 2013
Analytic Virtual Integration of Cyber Physical Systems Workshop (AVICPS) 2013, 2012
Formal Techniques for Distributed Systems (FMOODS/FORTE) 2012
Evaluation of Novel Software Approaches to Software Engineering (ENASE) 2012
International Symposium on Software Testing and Analysis (ISSTA) 2012
ASE Tools Forum 2012
Systems Software Verification Workshop (SSV) 2011
International Conference on Software Engineering (ICSE) Tools Workshop 2009
Formal Methods for Aerospace (FMA) 2009
Automated Formal Methods workshop (AFM) 2008, 2007
High Assurance Systems Engineering Conference (HASE) 2008

Conference on Software Language Engineering (SLE) 2008
Innovative Techniques for Certification of Embedded Systems (ITCES) 2006
Principles and Practice of Declarative Programming (PPDP) 2005

**Committee Member of:**
Automated Software Engineering Conference Steering Committee (2015-present)
IFIP 2.9 Working Group on Requirements (2014-present)
RTCA SC-205 DO178C Civil Avionics Software Standards Working Group (2005-2007) (Committee that created DO-178C software standard).

**PhD Committees**
Mohammad Hassan (External Reviewer at University of Western Ontario)
John Backes (UMN EE Dept.)
Ted Kaminski (UMN CS Dept.)
Deveraj George (UMN CS Dept)
Anjali Joshi (UMN CS Dept)
Ajitha Rajan (UMN CS Dept)
Matt Staats (UMN CS Dept)

## Miscellaneous Awards and Honors:

2016 Featured Faculty Member on the University of Minnesota "Driven To Discover" Campaign
2015 Dagstuhl Seminar Participant: *Qualification of Formal Methods Tools*
2014 Shonan Seminar Participant: *Integration of Formal Methods and Testing for Model-Based Systems Engineering*
2014 Inducted to IFIP 2.9 Working Group on Requirements
2013 MODELS Conference Best Reviewer Award
2012 Requirements Engineering Conference *Ready-Set-Transfer* contest winner
2012 Dagstuhl Seminar Participant: *Architecture-Driven Semantic Analysis of Embedded Systems*
2012 Senior Member IEEE
2010 Dagstuhl Seminar Participant: *Practical Software Testing*
2007 Rockwell Collins Engineer of the Year - Automated Analysis Group
RIACS 2001 Summer Student Research Program Participant
ICSE 2000 Doctoral Symposium Participant
National Merit Scholarship, Luther College
Weston Noble Scholarship, Luther College
Regents Scholarship, Luther College

## References:

Available upon request