## University-based Researchers

### *Kendra Cooper*

Cooper's research addresses the challenge of achieving the precision and rigour of conventional formal specification notations, while retaining an English-like appearance. *www.cs.ubc.ca/spider/kcooper*

### *Nancy Day*

Day's research investigates the use of automated techniques for the analysis of system specifications given in multiple notations and at a high level of abstraction. *www.cs.ubc.ca/spider/day*

### *Michael Donat*

Donat's research focuses on using formal methods to automate portions of the test derivation process. *www.cs.ubc.ca/spider/donat*

### *Dr. Dan Hoffman*

Hoffman's research focuses on practical approaches to software documentation, inspection and automated testing. *www.csr.uvic.ca/~dhoffman*

### *Dr. Bruce Kapron*

Kapron is investigating the application of process algebra and temporal logic to modelling, verifying and testing reactive systems. *www.csc.uvic.ca/~bmkapron*

### *Georgi Kostadinov*

Kostadinov's research investigates model-checking techniques based on proof search, and implementing these techniques in Prolog.www.uvic.ca/~georgik

### *Jayakrishnan Nair*

Nair's research focuses on automated testing of software components. *www.csr.uvic.ca/~jk/*

### *Dr. Lee White*

White's research area is in Software Engineering, specifically in the area of theory and practice of software testing and reliability.

### *Ken Wong*

Wong's research concerns the safety verification of software-intensive systems. *www.cs.ubc.ca/spider/kwong*

## Selected Publications and Reports


M. Donat and J. Joyce, "Applying an Automated Test Description Tool to Testing Based on System Level Requirements", INCOSE '98, Vancouver, Canada, July 1998.

K. Cooper, "Advantages of Stimulus Response Requirement Specification Techniques for System Testing", INCOSE '98, Vancouver, Canada, July 1998.

R. Yates, J. Andrews and P. Gray , "Practical Experience Applying Formal Methods to Air Traffic Management Software", INCOSE '98, Vancouver, Canada, July 1998.

K. Wong, "Looking at Code with your Safety Goggles On", Ada Europe 98, Upsala, Sweden, June 1998.

D. Hoffman, J. Nair and P. Strooper, "Testing Generic Ada Packages with APE", in preparation, March 1998.

K. Cooper, J. Joyce and M. Ito, "Stimulus Response Requirements Specification Technique", UBC CICSR Technical Report, December 1997.

J. Andrews, N. Day and J. Joyce, "Using a Formal Description Technique to Model Aspects of a Global Air Traffic Telecommunications Network", FORTE/PSTV'97, Osaka, Japan, November, 1997.

N. Day, J. Joyce and G. Pelletier. "Formalization and Analysis of the Separation Minima for Aircraft in the North Atlantic Region". 4th NASA Langley Formal Methods Workshop, Hampton Virginia, USA, September, 1997.

M. Donat. "Automating formal specification-based testing." TAPSOFT '97, Lille, France, April 1997.


See www.cs.ubc.ca/formalWARE/publications.htm for a regularly updated list of formalWARE publications and reports as well as links to viewable/downloadable copies (if available).

*March 10, 1998*


# Applying Formal Methods to Critical Systems

*BC ASI sponsored industry/university research collaboration*

**www.cs.ubc.ca/formalWARE**

## Applying Formal Methods to Critical Systems

formal*WARE* is a two-year industry/university collaborative research project sponsored by the BC Advanced Systems Institute, Raytheon Systems Canada Ltd., and MacDonald Dettwiler.

## What do we do in formal*WARE*?

University researchers from the University of British Columbia and the University of Victoria have been brought together with industry-based researchers and engineers to investigate the use of "formal methods" in the development of software-intensive, critical systems.

Our research should be of interest to *systems software engineers* where we investigate potential applications of formal methods which address specific challenges in system/software engineering. Our research should also be of interest to *formal methods researchers* where we work on several different mathematical notations and formalisms.

## What are Formal Methods?

The term "formal methods" refers to a variety of techniques and tools which may be used to improve engineering processes to develop software-intensive systems. They are considered "formal" in the sense that they are based upon mathematical concepts such as formal logic, finite state machines and set theory.

WWW sites at Oxford University, www.comlab.ox.ac.uk/archive/formal-methods.html and at NASA, atb-www.larc.nasa.gov/fm.html, provide extensive information about formal methods research and industrial applications.

Several international industrial standards such as "IEC 1508: Functional Safety -- Safety Related Systems" refer specifically to the use of formal methods.

## Are you a software engineer?

At formal*WARE* we are investigating potential applications of formal methods in the following areas:

- requirements specification and validation,
- requirements-based, system level testing,
- software component engineering and,
- system safety engineering.

We have found a variety of ways to improve (i.e., "faster, cheaper and/or better") processes in the above areas. For example, one result of this project is a prototype software tool for automating aspects of the process for deriving test cases from functional requirements.

Although this project is strongly oriented towards industrial applications, the project also involves development of the underlying mathematical foundation required to support various elements of our notations, techniques and tools.

## Examples Anyone?

Taking advantage of domain expertise provided by industrial sponsors of formal*WARE*, we have developed several large "real-world" examples to demonstrate the application of new methods and techniques. One example is the formal specification and tool-based analysis of a "separation minima" for aircraft. You can browse through this formal specification and the analysis results by visiting www.cs.ubc.ca/formalWARE/examples/sepmin.htm

## Who benefits from formal*WARE*?

formal*WARE* benefits both universities and industry. New techniques and methodologies have already been introduced to the sponsoring companies as a direct result of this project. Students and faculty have acquired a better understanding of where to focus their research effort so that they address specific challenges in systems/software engineering which are of genuine interest to industry.

Following the completion of this project on 1 April 1998, a package of tools, techniques, concept papers, process descriptions and other deliverables will be "packaged" for public dissemination.

For BC industries developing critical software systems, local expertise in formal methods and software safety techniques may be an important asset when competing for business in global markets, especially in Europe. This local expertise will be provided by the soon-to graduate students of formal*WARE*.

## Return on ASI's support

$150K of funding from ASI's Strategic Research Program has resulted in:

- $300K of research funding provided to local universities plus well over $130K of "in-kind" support.
- in-depth, person-to-person research interaction between university-based researchers and industry-based researchers and practitioners.
- training of graduate students including first-hand experience with the transfer of research results from the "laboratory" into industrial practice.
- "spin-off" interactions between local industry and local universities, e.g., UBC Certificate in Software Engineering.

## Contact Information

formal*WARE* is directed by Dr. Jeffrey Joyce of Raytheon Systems Canada, Ltd. For information about this project please contact:

Christine Jensen, Assistant Project Director
Department of Computer Science, UBC,
201-2366 Main Mall, Vancouver, BC,
CANADA V6T 1Z4
tel: (604)822-0698, fax: (604)822-5485
email: cjensen@cs.ubc.ca