

June 1, 2004

Career Background and Research Plans

Frederick T. Sheldon, Ph.D. (sheldon@acm.org | <http://www.csm.ornl.gov/~sheldon>)
U.S. DOE, Oak Ridge National Laboratory
PO Box 2008, MS 6085, 1 Bethel Valley Rd
Oak Ridge, TN 37831-6085
Office (865) 576-1339 | Fax: (865) 576-0003

Biography

Sheldon joined Oak Ridge National Laboratory in 2002 when he returned from a stint at DaimlerChrysler Research RIC/AS Stuttgart Germany, in system safety. Prior, he was an assistant professor at The Washington State University (School of EECS) and The University of Colorado (Computer Science) in Colorado Springs. In the aerospace industry he was a Software Design / Testability Engineer and Researcher in the areas of advanced avionics operational flight programs and diagnostics software at Lockheed Martin (Fort Worth) and Raytheon Systems (Dallas). He has participated in industrial R&D activities investigating formal methods used in software development and is currently focusing on solutions to the general problem of dependability and survivability of complex software and electronic systems.

Sheldon received his Ph.D. from The University of Texas at Arlington (UTA) in 1996 while supported by a fellowship ('93-95) from NASA Langley Research Center and an NRC Postdoc ('96). In 1997-98 he was an ASEE (summer) research fellow at Stanford University / NASA Ames Research Center. He received an M.S. in CS from UTA ('88) and a B.S. in CS from The University of Minnesota at Mpls./St. Paul ('83). He is a senior member of the IEEE Computer and Reliability Societies and a member of ACM, Tau Beta Pi and Upsilon Pi Epsilon. He received the Outstanding Research by a Ph.D. Student Award in CSE ('95-96) from the College of Engineering at UTA and the Outstanding Dissertation Award ('96-97) from the UTA Chapter of the Sigma Xi Scientific and Research Society.

In this brief document, I present in turn a research statement, then a teaching statement.

Research Plan

Background:

His experience can be broken down into *industrial* (TI [now Raytheon] and GD [now Lockheed Martin]), *applied research* (NASA, GD, DaimlerChrysler and ORNL) and *academic based research* (university projects). He has roughly thirteen years in engineering R&D with industry, plus five years associated with NASA and plus five years as a university professor/researcher. His background offers a unique combination of industrial/commercial, academic and government laboratory experience.

Completed and Ongoing Research Projects:

Establishing a center of excellence at ORNL based on practical approaches to the general problem of specification, modeling/analysis and verification/validation of software and systems related to critical infrastructure, system-of-systems reliability and survivability. This research was started in 2003 in the context of the relations on critical infrastructure protection related to potential funding from the departments of energy and of homeland security. For example, we have developed, in response to events such as the August 14, 2004 Blackout, an approach to critical energy infrastructure survivability, inherent limitations, obstacles and mitigation strategies.

References:

- **Sheldon, F.T.** Potok, T.E., Krings, A. and Oman, P., "Critical Energy Infrastructure Survivability, Inherent Limitations, Obstacles and Mitigation Strategies," *Int'l Jr. of Power and Energy Systems –Special Theme Blackout*, ACTA Press, Calgary Canada, 2004, a variation of this paper appeared in *IASTED Int'l Power Conf. - Special Theme Blackout*, New York NY, pp. 49-53, Dec. 10-12, 2003.

- **Sheldon, F.T.** Potok, T.E. and Kavi, K.M., "Multi-Agent System Case Studies in Command and Control, Information Fusion and Data Management," *Informatica Int'l Journal, Ljubljana, Slovenia, 2004.*
- **Sheldon, F.T.**, Potok, T.E., Loebl, A., Krings, A. and Oman, P., "Managing Secure Survivable Critical Infrastructures To Avoid Vulnerabilities," *Eighth IEEE Int'l Symp. on High Assurance Systems Engineering, Tampa Florida, pp. 293-96, Mar. 25-6, 2004.*
- Potok, T.E., Phillips, L., Pollock, R., Loebl, A. and **Sheldon, F.T.**, "Suitability of Agent-Based Systems for Command and Control in Fault-tolerant, Safety-critical Responsive Decision Networks," *ISCA 16th Int'l Conf. on Parallel and Distributed Computer Systems (PDCS), Reno NV, pp. 283-90, Aug. 13-25, 2003.*
- Potok, T., Elmore, M., Reed, J. and **Sheldon, F.T.**, "VIPAR: Advanced Information Agents Discovering Knowledge in an Open and Changing Environment," *Proc. World Multiconference on Systemics, Cybernetics and Informatics, Session on Agent-Based Computing, Orlando, pp. 28-33, July 27-30, 2003.*

Funding: *Computational Science and Engineering ORNL*

Software Requirements Specification, Analysis, Design Methods and Metrics. This research project was started in 2000 when Professor Hong Chung (Keimyung Univ. Korea) was invited as a visiting scholar at the SEDS Laboratory. Later that same year, by Professor Young-Jik Kwon (Taegu Univ. Korea) also joined our group. Together we have conducted a Case Study: *B2B E-Commerce System Specification and Implementation Employing Use-Case Diagrams, Digital Signatures and XML* and the development of a *Web Based Auction System using UML and Components*. We have also investigated the work of Chidamber and Kemerer and Li involved in *Software Maintenance Metrics*. We have extended their work to apply specifically to the maintenance of a class inheritance hierarchy. In doing so, we suggest new metrics for understandability and modifiability of a class inheritance hierarchy. The main contribution includes the various comparisons that we have been made and the advantages over CK's metrics and Henderson-Sellers's metrics in the context of maintaining class inheritance hierarchies. More work is needed to validate the claims that these metrics provide a more effective measure.

References:

- **Sheldon, F.T.** and Kim, H.Y., "Testing Software Requirements with Z and Statecharts Applied to an Embedded Control System," *Software Quality Jr.*, Kluwer, Vol. 12, Issue 3, 2004.
- Kim, H.Y, Jerath, K. and **Sheldon, F.T.**, "Assessment of High Integrity Components for Completeness, Consistency, Fault-Tolerance and Reliability," in Component-Based Software Quality: Methods and Techniques, a book edited by Alejandra Cechich, Mario Piattini, and Antonio Vallecillo, *Springer LNCS Vol. 2693, Heidelberg*, pp. 259-86, 2003.
- **Sheldon, F.T.**, Kwon, Y-J., Chung, H., Kim, W-H. and Jerath, K., "Case Study: B2B E-Commerce System Specification and Implementation Employing Use-Case Diagrams, Digital Signatures and XML," Submitted October 2001 5th IEEE Int'l Symp. On Object-oriented Real-time Distributed Computing [ISORC'2002], Wash. DC Apr. 29 – May 1, 2002.
- **Sheldon, F.T.**, Jerath, Kshamta and Chung, Hong, "Metrics for Maintainability of Class Inheritance Hierarchies," To appear Jr. of Software Maintenance and Evolution, John Wiley and Sons, London, Summer 2002.
- **Sheldon, F.T.**, Kwon, Y-J., and Jerath, K., "Implementing a Web Based Auction System using UML and Components," Submitted January 2002 Proc. Int'l. Annual Computer Software and Applications Conference [COMPSAC 2002], Oxford England, Aug. 26-29, 2002.
- **Sheldon, F.T.**, Xie, Gaoyan, Pilskalns, Orest and Zhou, Zhihe, "Survey of Rigorous Software Specification and Design Tools," To appear Software Focus Jr., John Wiley and Sons, London, Spr. 2002.

Funding: *Dept. of Comp. Engineering, Keimyung Univ. Korea, and Sch. of Comp and Comm., Taegu Univ. Korea*

Software Engineering for Dependable Systems (SEDS) Laboratory Infrastructure. The SEDS research laboratory, part of the School of EECS on the computer science side, was initiated as a center of excellence and to complement the SRES (Secure Reliable Embedded Systems) housed in the computer engineering side. The group had numerous graduate students including two visiting professors from Korea. The SEDS group has the goal of developing and validating methods and supporting tools for the creation of safe and correct software. This goal is designed to offer

not one but a set of approaches and tools useful in the specification, analysis and design of complex software systems. We are developing such methods/ tools and conducting case studies with the goal of designing in quality (cheaper, faster and better). This goal enriched our ability to offer curriculum that use state-of-the-practice facilities for undergraduate/ graduate education in software engineering. Students investigate and experiment with popular methods and tools within a classroom laboratory context working on pertinent problems from the industrial domain (e.g., embedded systems used in avionics, aerospace, transportation systems) contributed by way of industrial partnerships. These methods and tools offer a baseline state-of-the-practice approach to sharing and solving complex, yet academic sized, software-engineering challenges. In the end, our research and project oriented Software Engineering Curriculum endeavored to establish innovative constructive approaches with formal rigorous foundations to software design and evolution.

References:

- *Software Tool: Integrating Message Sequence Charts (MSC) formalism into the Mobius Framework*, developed by Zhihe “Bill” Zhou (for MS Thesis), and Frederick Sheldon at the Washington State Univ. (planned release Ver. 1.0 in Spr. 2002).
- **Sheldon, F.T.** and Wang, S., "A Translation Tool (PCX) from PROMELA/Spin to C-Based Stochastic Petri Net Language (CSPL)," Fifth Int'l Workshop on Performability Modeling of Computer and Communication Systems [PMCCS 2001], Erlangen, Sept. 2001.
- Wang, Shuren, "PCX A Tool for Translating PROMELA Specified Models into SPNs," Masters Thesis, Sch. of EECS, Washington State University, May 2001.
- **Sheldon, F.T.** and Kim, H.Y., "Software Requirements Specification and Analysis Using Zed and Statecharts," *IEEE 3rd Wkshp on Formal Descriptions and Software Reliability*, San Jose, CA, Oct. 7, 2000.
- **Sheldon, F.T.** and Dugan, D., "Stochastic Petri Nets and Discrete Event Simulation: A Comparative Study of Two Formal Description Methods," *IEEE 3rd Wkshp on Formal Descriptions and Software Reliability*, San Jose, CA, Oct. 7, 2000.

Funding: *Intel, Microsoft and the School of EECS Startup*

Brake-Safe: Embedded System Stochastic Analysis. In this study we focused on the specification and assessment of Stochastic Petri net (SPN) models to evaluate the design of an embedded system for reliability and availability. The system provides dynamic driving regulation (DDR) to improve vehicle derivability (anti-skid, -slip and steering assist). A functional SPN abstraction was developed for each of three subsystems that incorporate mechanics, failure modes/effects and model parameters. The models are solved in terms of the subsystem and overall system reliability and availability. Four sets of models were developed. The first three sets include subsystem representations for the TC (Traction Control), AB (Antilock Braking) and ESA (Electronic Steering Assistance) systems. The last set combines these systems into one large model. This general approach used empirical data to parameterize the Petri net graphs. The reliability estimates were used to evaluate the design of the DDR in parts and as a whole.

References:

- **Sheldon, F.T.** and Jerath, Kshamta, "Assessing the Effect of Failure Severity, Coincident Failures and Usage-Profiles on the Reliability of Embedded Control Systems," *ACM Symposium on Applied Computing, Nicosia Cyprus*, pp. 826-33, Mar. 14-17 2004.
- **Sheldon, F.T.**, Jerath, K., and Greiner, S.A., "Examining Coincident Failures and Usage-Profiles in Reliability Analysis of an Embedded Vehicle Sub-System," *Proc Ninth Int'l Conference on Analytical and Stochastic Modeling Techniques [ASMT 2002]*, Darmstadt Germany, pp. 558-563, June 3-5, 2002.
- **Sheldon, F.T.** and Jerath, K., "Reliability Analysis of an Anti-lock Braking System Using Stochastic Petri Nets," Fifth Int'l Workshop on Performability Modeling of Computer and Communication Systems [PMCCS 2001], Erlangen, Sept. 2001.
- **Sheldon, F.T.** Greiner, S.A., and Benzinger, M., "Specification, Safety and Reliability Analysis Using Stochastic Petri Net Models," *ACM Proc. Tenth Int'l Wkshp on Software Specification and Design*, pp. 123-132 Nov. 5-7 2000.

- Brake-Safe Analysis Final Report: Safety and Reliability Analysis Using Stochastic Petri Nets (Author: **F.T. Sheldon**, *DaimlerChrysler FT3/AS Final Report which included the CSPL Specified Models Software Toolkit*, June 2000).

Funding: *DaimlerChrysler, Research and Technology/ System Safety (FT3/AS)*

Composing, Analyzing and Validating Software Models. Formal specifications provide good support for designing a functionally correct system, however they are weak at incorporating non-functional performance requirements (like reliability). Techniques which utilize stochastic Petri nets (SPNs) are good for evaluating the performance and reliability for a system, but they may be too abstract and cumbersome from the standpoint of specifying and evaluating functional behavior. Therefore, one major objective of this research is to provide an integrated approach to assist the user in specifying both functionality (qualitative: mutual exclusion and synchronization) and performance requirements (quantitative: reliability and execution deadlines). In this way, the merits of a powerful modeling technique for performability analysis (using SPNs) can be combined with a well-defined formal specification language. In doing so, we can come closer to providing a formal approach to designing a functionally correct system that meets reliability and performance goals.

References:

- **Sheldon, F.T.** and Greiner, S.A., "Composing, Analyzing and Validating Software Models to Assess the Performability of Competing Design Candidates," *Annals of Software Engineering –Special Volume on Software Reliability, Testing and Maturity*, Vol. 8, 49 pages, 1999.
- **Sheldon, F.T.**, Composing, Analyzing and Validating Software Models, *NASA ARC / Stanford – ASEE Final Report which included the CSPN Software Toolkit*, August 1998).

Funding: *NASA Ames Research Center*

Specification Based Stochastic Analysis. This research was conducted at the Computational Sciences Division of the Information Sciences Directorate at Ames Research Center. The primary goal was to identify suitable applications (i.e., safety/cost critical hardware and software systems) for analysis of their stochastic properties based on the structural characteristics of a specification model. Two main example applications have been investigated. The *first* includes the Gerard Kuiper Airborne Observatory (KAO) which considered the questions: (1) What empirical information exists to help parameterize the estimates of failure rates for subsystems? (2) Ascertain the composition and structure of subsystems that are most sensitive to shaping its operational behavior, (3) What failures can be identified including frequency of occurrence (e.g., Mechanical, Timing, Communications, Design) for a diagnostics based model? The *second* application is based on a SPIN model of the DS1 Executive with 2 (or more) tasks. The DS1 executive has correctness requirements in both realms of timing and logic. A PROMELA model was investigated and found to be unsuitable for stochastic analysis due to a lack design documentation.

References:

- **Sheldon, F.T.**, Specification Based Stochastic Analysis and Diagnostics of Concurrent Embedded Systems, *NASA ARC / Stanford – ASEE Final Report*, August 1997.

Funding: *NASA Ames Research Center*

Changing the Learning Paradigm through Technology. This project developed two courses (in the ECE and CS departments) based on currently available off-the-shelf distance learning technologies (e.g., Web enabled, portable, and distributed). The project focused on curriculum development in support of the following goals: (1) Emphasize project based learning in engineering education, (2) enhance the learning experience through an information/technology rich environment (3) better allocate access to limited resources and thereby improve the return on investment for both the student and the institution, (4) reduce the need for students to travel to the on-campus delivery site, and (5) utilize a strategy that facilitates asynchronous learning (i.e., learning-at-your-own-pace).

References:

- **Sheldon, F.T.**, Alspector, J. and Haefner, J. "Technical Education over Drive-able Distances using a Portable Classroom and Variable Bandwidth Communication Networks," *IEEE Proc. Int'l Symp. On Internet Technology*, Apr. 29 - May 1, 1998.

Funding: Univ. of Colorado Presidents Learning Paradigm Initiative

A Novel Approach to Model Based Validation of Fault Tolerant Systems. Project addresses the limitations and issues for modeling methods and tools developed specifically for stochastic analysis, performability evaluation, and solution methods suited to systems with low latency requirements and rare events (e.g., single independent and multiple coincident failures). Goal: develop a methodology and toolset for specification and stochastic and performability analysis of vital DoD systems

References:

- Wei, Wen, "Adaptation and Implementation and Integration of Graph Layout Algorithms for a Petri Net Graphical Editor," Masters Thesis, Sch. of EECS, Washington State University, May 2001.
- Owens, D.A., and **Sheldon, F.T.**, "A Tool-based Approach to Distributed Database Design," *ACM Symposium on Applied Computing (SAC'99)*, 10 refs., 18 pages, February 1999.
- **F.T. Sheldon**, "Final Report: A Novel Approach to Model Based Validation of Fault Tolerant Systems," *DARPA SBIR Final Report*: May 1997).

Funding: DARPA

Simulation-Based Analysis for Real-Time Systems Development This research project was multifaceted and extended over a three (plus) year time frame. The project was funded through the NASA Graduate Student Researchers Fellowship Program, funded by Langley Research Center. This research was conducted both at the Univ. of Texas at Arlington, NASA LaRC in Virginia and Duke University. The proposal was originally funded based on research ongoing by Prof. Sung-Min Yang at UTA and myself at General Dynamics FWD. However, Yang left the project and Prof. Krishna Kavi took over as my Ph.D. advisor.

References:

- Kavi, K.M., **Sheldon, F.T.** and Reed, S.C., "Specification and Analysis of Real-Time Systems Using CSP and Petri Nets," *Int'l Journal of Software Engineering and Knowledge Engineering –Special Issue on Software Engineering Practices and Tools for Real-Time Systems*, 24 Refs., June 1996.
- **Sheldon, F.T.**, "Specification and Analysis of Stochastic Properties for Concurrent Systems Expressed Using CSP," Ph.D. Dissertation, *Computer Science and Engineering Dept., Univ. of TX at Arlington*, 260 Refs., May 1996 (Sigma Xi Scientific Research Society Outstanding Ph.D. Dissertation Award).
- Kavi, K.M., and **Sheldon, F.T.**, "Specification and Analysis of Real-Time Systems Using CSP and Petri Nets," *IIT Proceedings 1st Conf. on Fault-Tolerant Systems (FTS'95)*, Madras, India, Dec. 20-22, 1995.
- **Sheldon, F.T.**, and Kavi, K.M., "Linking Software Failure Behavior to Specification Characteristics II," *IEEE Proceedings Fourth International Workshop on Evaluation Techniques for Dependable Systems*, San Antonio, TX, 27 Refs., Oct. 1995.
- **Sheldon, F.T.**, Kavi, K.M., and Kamangar, F.A., "Reliability Analysis of CSP Specifications: A New Method Using Petri Nets," *AIAA Proc. Computing in Aerospace 10*, pp. 317-326, 16 Refs., March 1995.
- Kavi, K.M., **Sheldon, F.T.**, Shirazi, B. and Hurson, Ali R., "Reliability Analysis of CSP Specifications Using Petri Nets and Markov Processes," *IEEE Proc. Hawaii Int'l Conf. on Systems and Sciences*, 10 Refs., Jan. 1995.
- Kavi, K.M., and **Sheldon, F.T.**, "Specification of Stochastic Properties with CSP," *IEEE Proceedings Int'l Conference on Parallel and Distributed Systems*, Taiwan, ROC, pp. 288 - 293, 12 Refs., December 1994.
- **Sheldon, F.T.**, and Kavi, K.M., "Position Statement: Linking Software Failure Behavior to Specification Characteristics I," *IEEE Proceedings Third International Workshop on Integrating Error Models with Fault Injection*, Annapolis, MD, pp. 35-39, 19 Refs., April 1994.

- **Sheldon, F.T.**, Mei, Hsing, and Yang, S.M., "Reliability Prediction of Distributed Embedded Fault-Tolerant Systems," *IEEE Proc. 4th Int'l Symp. On Software Reliability Engineering*, pp. 92-102, 27 Refs., Nov. 1993.
- Yang, S.M., Yoo, S.M., Kim, Y.S., Song, Y.J., and **Sheldon, F.T.**, "UTARK: An Object-Based Real-Time Kernel for Distributed Embedded Systems," *IEEE Proc. CompEuro93 (Paris)*, pp. 392-399, May 1993.
- **Sheldon, F.T.**, Yang, S.M., and Bornejko, T.L., "Simulation-Based Analysis for Real-Time Systems Development," *IEEE Proc. Automatic Testing Conf. (AutoTestCon92)*, pp. 361-366, 15 Refs., Sept. 1992.

Funding: NASA Langley Research Center

Generic Integrated Maintenance Diagnostics Systems. Eighteen month project to define a generic Integrated Diagnostics (ID) Software Development Process to address problems associated with functional deficiencies of avionics software and software maturation using as a basis, the Software Development Integrity Program Mil-Std-1803 (plus Mil-Std-2167A, 2168, 1815 and 800-xx Series). We developed a software engineering process model (to specify, develop and verify diagnostic software) and recommendations to the USAF for Mil-Std-1814 updates. We provided a report on new and formal methods used in software development as they may be applied to software diagnostics and diagnostics (involving testability) for software.

References:

- GIMADS Task 29 Four Final Reports for Subtasks 1-4, Defense Technical Information Center (www.dtic.mil)

Funding: USAF Wright Patterson SPO

Research Interests

My research interests can be classified into three broad categories:

- Theoretical Foundations of Software Engineering. Formal and systematic methods (e.g., Zed, CSP, Petri nets, Statecharts, etc.) used in specification, modeling, analysis and verification (e.g., model checking) of important properties (e.g., safety, completeness, consistency). Specification and programming language semantics and interoperability (among logical and stochastic formalisms).*
- Engineering Aspects of Software Engineering. Structural and architectural characterizations including: reuse, process modeling, product line engineering (simulation and design), domain engineering, and component based development (e.g., embedded real-time).*
- Managerial Aspects of Software Engineering. Software metrics, performance, reliability, dependability and extensibility including both analytical and empirical approaches to software metrics.*

Research Prospects

We are currently working on, and preparing for, a number of research projects, some of which are discussed below.

Title: Characterizing the Logical and Stochastic Properties of Network Software Systems. The correctness, safety and robustness of a critical system specification are generally assessed through a combination of rigorous specification capture and inspection; formal modeling and analysis of the specification; and execution and/or simulation of the specification (or possibly a model of such) and naturally testing. Such activities are conducted to ensure the confidence and quality of certain key attributes (i.e., correctness, reliability, availability, safety, security and timeliness). The long-term goal for this effort is to develop and validate methods and tools for the creation of correct and dependable software based systems by investigating mechanisms to assess those key attributes. This goal is apparent in the name Software Engineering for Dependable Systems (SEDS) which targets application domains that can benefit from the use of formal and rigorous methods and technology.

Funding: Samsung and Korean Government

Collaborators: Prof. Hyunseung Choo (Sungkyunkwan Univ., Korea)

Integrating the Message Sequence Charts (MSC) Formalism into Mobius Framework for Performability Analysis. Message Sequence Chart (MSC) is a formal language to describe the communication behavior of a system, which is modeled as message-passing instances. Mobius is an extensible tool that incorporates different formalisms and enables models from different formalisms to interact with each other. We will integrate MSC into Mobius framework to provide a new formalism for Mobius users. Together with other formalisms of Mobius, MSC can be used as a building block for large hybrid models. Users will have additional flexibility in choosing modeling languages. Not like other formalisms so far included in Mobius, MSC has both textual and graphical representations. Modeling with a text editor is the same as writing a traditional program while the graphical representation gives us a direct view of the system.

References

- **Sheldon, F.T.** and Zhou, Z, "Integrating the CSP formalism into Mobius Framework for Performability Analysis," Fifth Int'l Workshop on Performability Modeling of Computer and Communication Systems [PMCCS 2001], Erlangen, Sept. 2001.

Funding: School of EECS, WSU (Research Assistantship)

Collaborators: Zhihe Zhou, MS/Ph.D. Candidate and Prof. Bill Sanders (Univ. of Illinois, Urbana)

Process and Verification of Safety Properties for Embedded Software Systems. In recent years the role of computers in control applications has increased significantly. In virtually all of today's applications computers have been tightly integrated into control systems (e.g., steer-by-wire/ driver assistance). The integration of computers results in complex dynamical systems called hybrid systems that contain both discrete and continuous dynamics. Typically, the discrete dynamics corresponds to the logic implemented in the computers (e.g., Stateflow) and the continuous dynamics corresponds to the physical system being controlled by the computer (e.g., Simulink). This project concerns the problem of applying formal verification to hybrid systems. Given a desired safety property, we would like to guarantee that the hybrid system satisfies the property under all situations. This is a very important problem in the validation of the system design, especially for a safety-critical application that cannot tolerate any unexpected system behavior. The desired results provide a highly automated (but hand-guided) prototype toolset for semi-exhaustive state space exploration method based on a mechanizable abstraction method for Mathlab's Simulink/Stateflow Models that can be model checked.

Moreover, such methods need to be merged with respect to conventional state-of-the-art hardware/software co-design processes (more than FTA and FMEA) to create a comprehensive and effective SSA (System Safety Analysis) process. In this way, we ensure that *all* failure modes combined with *all* operational (e.g., driving) situations are considered in the process of risk analysis that produces a complete set of consistent safety requirements resulting in software that is fail-safe and fault-tolerant.

Funding: DaimlerChrysler

Collaborators: Stefan Greiner, Ph.D., Markus Degen and Juergen Schwarz, Ph.D.

Research Philosophy

As researchers, we must have a clear understanding of the variety of research goals, research means, and the relations between these means and ends. Among research goals, we distinguish between theoretical research, whose purpose is to enhance our understanding, and practical research, whose purpose is to use our understanding to enhance practice. Among research means, we distinguish between analytical research, which builds models to explain observed behavior, empirical research, which builds models that account for observed behavior without necessarily explaining it, and experimental research, which validates existing models against further observations.

Variety of Goals

With respect to the variety of goals, we characterize our position by means of three premises:

- i. Concern for Practice. The best theoretical research is one that maintains a focus on practice although we also recognize that, historically, the most influential ideas arose from disinterested research.*

- ii. *Concern for Soundness. The best practical research is one that is based on sound theory. We feel strongly that focus on practice is no excuse for poor theory.*
- iii. *Concern for Simplicity. The main goal of scientific research is the relentless discovery of simple explanations behind seemingly complex observations.*

These premises are most visible in our approach to the project of Software Specification/ Design Methods and Metrics: before we derive any metrics, we focused on understanding and analyzing existing metrics and the mathematical properties of our proposed metrics. Now we are analyzing their statistical/ functional relationships to the quantitative functions (Maintainability of Class Inheritance Hierarchies), and assessing to what extent and under what conditions the metrics approximate the target functions using experimental research to validate our claims.

Variety of Means

With respect to the variety of means, I feel that analytical, empirical, and experimental research all play complementary roles in a research effort and should ideally be deployed within their respective roles. In particular, doing experimental research is no excuse for dispensing with empirical/ analytical methods.

Teaching Philosophy

An education should be an opportunity to realize and reinforce your potential (talents and skills). An educator should present the problems and issues in a positive light and endeavor to draw forth the student's capabilities in addressing those issues. An education, in my view, is not a matter of pouring the facts and solutions into the student's head. Rather it should be a process of discovery and affirmation so that the results can be an honest and long-lasting resource to the student. The process should be fun, exciting, edifying, practical and productive.

It is important to establish opportunities for students to explore their creative and analytical abilities: developing guidelines for practical, challenging and innovative group projects, sending outstanding project reports to conferences, recruiting students by inviting them to weekly presentations/ discussions in our SEDS Laboratory, developing new courses related to my research, collaborating with internal/ external faculty on cross-disciplinary courses and research projects, or bringing in industry to motivate and sponsor class topics and semester projects.

Teaching Approaches and Goals

My approach to teaching is influenced by my educational background, and my teaching experience. As far as my educational background is concerned, I have studied at Saint Johns University, The University of Minnesota (both the College of Biological Sciences and the Institute of Technology in Minneapolis) and The University of Texas at Dallas and at Arlington and a various scholarly research visits at Duke University. I have a unique perspective from both the classroom and as a distance learning student (my MS course work was entirely at a distance). My teaching experience spans the period from 1993 until 2001 and began as a graduate student at UT Arlington where I also taught for three years, then at the University of Colorado (Colorado Springs) for three years and finally at Washington State University.

I have been major advisor to 15 graduate students and taught eleven different courses over five years in tenure track. My teaching evaluations while at WSU have been outstanding. Due to the distributed nature of the School of EECS (four plus campuses), I had the unique opportunity to utilize progressive methods and the latest teaching/Internet technologies in demonstrating how distance learning can be successfully employed. My senior level Software Engineering Class has been televised in Washington State and video streamed to various high tech companies. I have received various commendations because the course has a very high correlation with needed industrial strength applications, practice and experience. Refer to my CV for a list of the courses I have taught including such details as when, how often and coverage.

My teaching is based on the following principles that are somewhat interrelated and/or redundant.

Focus on Fundamentals. In a field such as ours, which evolves at such a high speed, it would be foolish to evolve our educational programs at the pace of our subject matter. Rather it is much more practical, more judicious, and, in the long run, more useful to focus on principles, which are less prone to chaotic evolution, and which will better serve the student irrespective of the future of our field.

Concern for Practice. The requirement above must be carefully balanced against the requirement that students be able to serve their employers on short order. Hence while the bulk of the course should be on fundamentals, the course should also be oriented towards today's needs.

Teaching the students how to learn. Because we cannot possibly predict all the challenges that students will encounter in their professional careers, it is best to teach them how to learn, by developing their analytical/ critical skills.

Challenging/ stimulating the students. My lectures involve a great deal of interaction with the students. I usually distribute lecture notes and handouts to the students, which represent a skeleton of the material that I intend to cover. Students can fill the blanks into their notes following question/answer sessions. I also give them pop quizzes that I ask them to self-grade. This allows me to keep students interested, and encourages them to think about the questions and the answers before they write them down.

Kindle students enthusiasm. I am mindful of the student's desire to learn and of my responsibility to kindle their intrinsic enthusiasm.

Showing a keen interest in the student. I feel that it is very important to show interest in the students; students have to feel that the instructor has a stake in their success. I make a conscious effort to learn their names, and am genuinely interested in making sure that they learn in my class, and that they enjoy their learning experience.

Emphasis on homework. It has been my experience, as a student, that homeworks are a very important part of the learning experience. As a teacher, I keep students busy all semester long with successive homeworks. Grading their homeworks gives me feedback on their individual progress and collective progress. In my graduate formal methods course, to start everyone at the same level I have developed an online tutorial they must review within the first two-three weeks (see <http://www.eecs.wsu.edu/seds/ds/index.html>).

Emphasis on learning. The important question to ask is whether and/or how much the student has learned in my course. This is, in my opinion, the primary enduring legacy of taking a class. For example, my software engineering (SE) course combines the theoretical and philosophical issues in SE from lectures with experiential learning using a project oriented approach. The project gives first hand knowledge about how those theories can be put into practice. I try to ensure that students understand, participate, practice and experience current SE processes, techniques and tools including the development of foundational skills necessary to successfully:

- Apply their knowledge of mathematics, science and engineering in solving a real-world SE problem,
- Develop a clear statement of requirements and utilize abilities inherently acquired within the SE curriculum so as to demonstrate their ability to analyze (including interpret data), design, implement and/or integrate and test (with limited experimentation) a software system developed within a project group context,
- Apply and participate within an assigned multidisciplinary team context (i.e., group leader, designers, programmers, testers, and documentation writers) based on their acquired skills within the SE curriculum,
- Demonstrate their ability to solve problems from within the SE problem domain context (i.e., identify specific requirements, design, implement, and test [through inspection, analysis, or analogy] to determine that such requirements have been satisfied),
- To summarize, this course provides an introduction to software systems development with emphasis on requirements analysis, specification, design, implementation and testing (unit and integration), and finally demonstration. Students participate in a course project to give them hands-on experience with SE principles. There is documentation (including the appropriate artifacts) required as exit and entrance criteria to each phase of the process. All course material is available on the instructor's home page.

Ethics

Ethics, especially as it is taught and experienced in school is important because today's students will be tomorrow's leaders. One should not only teach the technology, making a complicated subject simple, but also instill a sense of responsibility and good character in using and applying such technology. In order to be effective in such an ideal, the teacher should strive in setting well meaning standards. Honesty in the classroom should be emphasized by rewarding independent work and conversely, by rewarding the fruits of team projects in an appropriate manner. It's extremely important to be fair, approachable and encouraging in a practical and sensible light. Sometimes it's not a matter of answering or solving the problem as much as its asking the right questions. For example, my software engineering (SE) course makes it possible for students to experience and understand, within the SE problem context, the issues of professional and ethical responsibility based on limited and shared resources (e.g., common lab and common examples of artifacts) and also based on lectures that cover the more philosophical and theoretical issues on the impact of engineering solutions in a societal context.