List of Contents for Dr. M. Sahinoglu's Curriculum Vitae

1) Contact Information (Title Page) **and Research Interests:** ***p. 2***

2) Educational History: p. 3

3) Professional History: pp. 3-4

4) Scholarships, Awards and Honors, and Professional Memberships: pp. 4-6

5) Refereed Journal Publications, Books and Book Chapters: pp. 6-10

6) Conferences and Colloquia Organized: pp. 11-12

7) IT Colloquium and WSorld Conference Honorary Speakers Invited (2000-2009): p. 13-28

8) Invited Academic Meetings and NPR Radio Interviews: pp. 29-32

9) Refereed and Presented Conference Proceedings: pp. 32-45

10) Technical Reports and Dissertations: pp. 46-48

11) Industrial Projects and Grants: pp. 49-52

12) List of Courses Instructed (1976-2013): pp. 53-58

13) Candidate's Activities for the Advancement of Engineering, Science and Technology et al.: pp. 59-69

14) Compact Resume and A Sample of Academic Activities during 2012-2013: pp. 70-72

15) Website cited for CLOUD COMPUTING publication as No. 1 most accessed and NETWORK RELIABILITY EVALUATION publication, as No. 2 most accessed respectively nationwide: p. 73-74

16) CSIS Program Poster Flyers and Cybersecurity Test Lab: pp. 75-76

17) Award Letter and Certification of the AUM/Cybersystems and Information Security program by the Committee on National Security Systems and The National Security Agency for "Information Systems Security Professionals, NSTISSI No: 4011 for June 2013 – 2018" or www.aum.edu/csis: pp. 77-78

18) Text Book (2007) by the author (used as text in CSIS program) and Microsoft Grant etc. Optionals: pp. 79-82
http://www.amazon.com/dp/0470085126 ***(original at Amazon website)***
http://www.emka.si/avtorji/mehmet-sahinoglu/485956) ***(in a Slovenian book website)***

19) Thirty Five Selected Publications' Title+ Pages: **(Sahinoglu-Libby pdf in context on p. 83)** ***pp. 83-124***

20) **www.aum.edu/csis** ***Informatics Institute website screenshots: pp. 125-128***

21) CD ROM TWC Trustworthy Computing/ p. 14, #22; Screenshots for Author's own JAVA Apps: pp. 129-147

22) Documents from U.S. High School Diploma to Doctorate (PhD) at Texas A&M University: pp 148-153

CURRICULUM VITAE – 2013

Mehmet Sahinoglu, BS, P.E. (1973), MS (1975), PhD (1981)

SDPS Fellow ('02) www.sdpsnet.org, IEEE Senior Member ('93) www.ieee.org, ISI Elected Member ('95) www.isi-web.org

Founding Director, Informatics Institute
Founder Head of Cybersystems and Information Security
M.S. Graduate Degree Program
www.aum.edu/csis
Auburn University, Montgomery, AL 36124-4023, USA

Contact Information:

Auburn University Montgomery, Mail: P.O. Box 244023Montgomery, AL 36124-4023, USA (Office: 601-603 Library)

Home Address: 7542 Mossy Oak Dr. Montgomery AL 36117-5606

E-Mail: msahinog@aum.edu (**university**); **msahinog@bellsouth.net** (**private**)

Phone:	(334) 244-3769
Fax:	(334) 244-3127
Cell:	(334) 538-5445

RESEARCH AND TEACHING INTERESTS

Research Interests: Cybersystems and Information Security/Privacy Risk Assessment & Management, Trustworthy Computing, Software Reliability Modeling and Network Metrics, Cost-Effective Testing (Stopping Rule Algorithms), Electric Power Systems Reliability Estimation, Applied (Engineering) and Mathematical Statistics, Built-in-Self-Testing (BIST), Computational Statistics,Computational Simulation (Monte Carlo and Discrete Event), Cloud Computing, Information Assurance. Please see peer-reviewed publications and proceedings.
Teaching Interests: Please see the instructed courses listed.

Author of Textbook titled: "Trustworthy Computing: Analytical and Quantitative Engineering Evaluation", CD ROM included, John Wiley (2007)

New Text Book Proposal by NovaPublishers (2013); Cyber-Risk Informatics (publication due Oct. 14)

Associate Editor with the International Journal of Computers, Information Technology and Engineering (IJCITAE) since 2007

Reviewer with IEEE Trans. Software Engineering, CAD, IEEE Reliability, IEEE Computer

EDUCATIONAL HISTORY

Diploma (High School), Orchard Park Central High School, N.Y, USA, 1969
B.S. (ECE: Electrical & Computer Engineering) Middle East Technical University (METU) Ankara, Turkey, 1973
M.S. (Electrical Engineering) Institute of Science and Technology University of Manchester (UMIST) Manchester, England, 1975
Ph.D. (Statistics and ECE: Electrical & Computer Engineering jointly) Texas A&M University, College Station, Texas, USA, 1981

PROFESSIONAL HISTORY

Certified Electrical Engineer (P.E.)	*Turkish Electricity Authority, Ankara- Turkey*	*1973-76*
Teaching Assistant	*Dept. of Applied Statistics, M.E.T.U, Ankara*	*1976-77*
Graduate Research and Teaching Assistant	*Dept. of Electr.& Computer Eng. (GRA) and Institute of Statistics (GTA) at Texas A&M University, College Station, Texas*	*1978-81*
Instructor	*Dept. of Applied Statistics, M.E.T.U., Ankara*	*1981-82*
Assistant Professor	*Dept. of Applied Statistics, M.E.T.U., Ankara*	*1982-84*
Associate Professor	*Dept. of Applied Statistics, M.E.T.U., Ankara*	*1984-89*
Visiting Associate Professor (CIS Fulbright Scholar)	*Depts. of Statistics and Computer Science, Purdue University*	*1989-90*
Software-Reliability Consultant	*Ministry of Defense, TAFICS Project*	*1990-92*
Professor	*Dept. of Applied Statistics, M.E.T.U., Ankara*	*1990-92*
Electric Power Reliability Chief-Analyst and Consultant Engineer	*Turkish Electricity Authority (TEK), Ankara*	*1982-97*

Founder and Dean	*College of Science & Arts, Dokuz Eylul University, Izmir, Turkey*	*1992-95*
Founder and Head	*Dept. of Statistics and Quantitative Sciences, Dokuz Eylul University, Izmir, Turkey*	*1992-97*
Visiting Professor (NATO-TUBITAK Fellow)	*Purdue University, jointly with Dept. of Statistics/Computer Science*	*1997-98*
Visiting Professor	*Case Western Reserve University, jointly with Dept. of Statistics/EECS (Electr. Eng. and Computer Science)*	*1998-99*
Professor (tenured), ACHE Eminent Scholar- Endowed Chair, Department Chair, Member of Deans' Council	*Troy State University Montgomery Department of Computer & Information Science (as of 2005, Computer Science)*	*1999 - 2008* *Resigned as Dept. Chair Feb. 2007*
Founder Director and Program Coordinator, Distinguished Professor	*Informatics Institute, Cyberystems and Information Security M.S. Degree Program, Auburn University at Montgomery (in the Auburn University System)*	*August 2008-*

SCHOLARSHIPS, AWARDS AND HONORS, AND PROFESSIONAL MEMBERSHIPS

1. *NATO Essay Contest National/Int'l Winner, April 1-8, 1967, Prize week to Paris by SHAPE/NATO, France.*
2. *AFS Scholarship, 1968-69, High School Senior, Orchard Park, N.Y.*
3. *Polymetron – Zellweger, 1971, Switzerland's electronics summer-internship (practicum) award, 1971.*
4. *IASTE Summer Internship Stipendium electrical and electronics engineering summer-internship (practicum), summer 1972, Siemens, Nurnberg and Erlangen, Germany.*
5. *Borsa (Fellowship) del Centro di Studi Italiani, Linguistics Award, Summer 1974, L'universita di Siena, Italy.*
6. *The British Council Scholarship, 1974-75, M.S. in Elec. Eng. at the Victoria Univ. of*

Manchester, Inst. of Science & Technology, Manchester England.
7. *Ambassade de France,1989, Summer Research and Linguistics Award, Univ. de Grenoble, France.*
8. *Fulbright Scholarship, 1989-90, Purdue University, Statistics & Computer Science.*
9. *TUBITAK (Turkish Scientific Technical Research Council) Research Scholarship Grant, 1992-94, Software Testing on MOTHRA - Automated Testing Tool in cooperation with SERC-Purdue University.*
10. *Salzburg Seminar, Austria, May 1-15, 1993, Sasakawa Young Leaders Fellowship Program Award on G3 (Europe, Japan, and North America): New World Order.*
11. *IEEE Senior Member Award, 1993. On advances in Computer Software and Hardware Reliability.*
12. *ISI (International Statistical Institute) Elected Member, 1995, for international services (organized 3. IASC: Int'l Assoc. Stat. Computing - Summer School in Izmir Turkey)*
13. *TUBITAK NATO Fellowship Award (1997-98) for research on Software Reliability at Purdue University's Computer Science and Statistics Departments.*
14. *Elected to be the first Eminent Scholar of Computer and Information Science at Troy State University Montgomery, AL, 1999.*
15. *Recipient of the Extraordinary Alien Scientist by INS, US Gov't, 2000.*
16. *Recipient of "SDPS Fellow" grade and plaque at http://www.sdpsnet.org presented in June 2002 at IDPT2002 / SDPS in Pasadena, California.*
17. *Redmond Washington Meeting April 2006. One of the 14 Winners of TCC in the World Microsoft Grant Competition among 114 contestants. http://research.microsoft.com/ur/us/fundingopps/RFPs/TWC_Curriculum_2005_RFP_Awards.aspx; also see www.areslimted.com for Trustworthy Curriculum Microsoft report.*
18. *Recipient of "Software engineering Society Excellence in Leadership" award and plaque "In Recognition of meritorious leadership and commitment to both SDPS http://www.sdpsnet.org and SES since their founding. Presented at the Twelfth Transdisciplinary Conference-Workshop on Integrated Design and Process Science: Informatics and Cyberspace." Montgomery Alabama November 2009.*
19. *First Place - Most Accessed WIREs (Wiley Interdisciplinary Review Series) article for two consecutive years 2010-12 for the article titled "CLOUD Computing", Vol. 3.1. Co-authored with Luis Cueva-Parra from AUM's Math/CS Option. See last page of this CV document on p. 54.*

20. Certification of the AUM/Cyberystems and Information Security program by the Committee on National Security Systems and The National Security Agency for "Information Systems Security Professionals, NSTISSI No: 4011 for June 2013 – June 2018" *See page 51-52 or www.aum.edu/csis.*

***Professional Memberships**: **1)** Member of ASA (Amer. Stat. Assoc.) since 1980, ASA-AL Chapter President (2002-03) **2)** Elected Fellow of ISI (International Statistical Institute) and Member of IASC (Intern. Assoc. of Stat. Computing) since 1987 **3)** Member of EMO (Professional Electrical Engineers of Ankara, Turkey) since 1973 **4)** Alumni Members of METU-Ankara since 1973, UMIST-UK (since 1975) and Texas A & M U. since 1981 **5)** Member of Education and Head of Research/Development subcommittees, MACC (Montgomery Area Chamber of Commerce) since 1999 **6)** Elected Fellow SDPS (Soc. for Design and Process Science), TX since 2000 **7)** Member of AFCEA (Armed Forces Communications and Electronics Association) since 2002 **8)** Member of the World Energy Council (WEC) since 1999 **9)** Member of ASQ (Amer. Society of Quality) since 2007 **10)** Member of AMC (2000-2007) **11**) Lifetime Member of Cambridge's Who's Who'08 **12)** Member of ISSA (Information Systems Security Association) since 2013*

REFEREED JOURNAL PUBLICATIONS, BOOKS AND BOOK CHAPTERS

1. *Patton A.D., Singh, C., Sahinoglu M., "Operating Considerations in Generation Reliability Modeling – Analytical Approach,"* IEEE Transactions on Power, Apparatus, and Systems (PAS), ***Vol. 102,*** *pp. 2656-2663, May 1981.*

2. *Sahinoglu, M., Longnecker, M.T., Ringer, L.J., Singh, C., Ayoub, A.K. (1983); "Probability Distribution Function for Generation Reliability Indices-Analytical Approach,"* IEEE Transactions on Power, Apparatus, and Systems (PAS), ***Vol. 104****, pp. 1486-1493, June 1983.*

3. *Sahinoglu M., " On central limit theory for statistically non-independent and non-identical variables", Journal for M.E.T.U. Studies in Development, Applied Statistics* ***Special Volume****, Ankara, ISSN 0907-0816, , pp. 69-88, 1982.*

4. *Sahinoglu, M., Gebizlioglu, O.L. "Exact PMF Estimation of System Indices in a Boundary -Crossing Problem,"*Commun. Fac. Sci. Univ. of Ankara, Series A_1, *ISSN 0251-087*, ***Vol. 36****, No.2, pp. 115-121, 1987.*

5. *Sahinoglu, M., "The Limit of Sum of Markov Bernoulli Variables in System Reliability Estimation," IEEE* Transactions on Reliability, ***Vol. 39,*** *pp. 46-50, April 1990.*

6. *Sahinoglu, M., "Compound-Poisson Software Reliability Model,"* IEEE Transactions on Software Engineering, ***Vol. 18,*** *pp. 624-630, July 1992.*

7. *Sahinoglu, M., Selcuk, A. S., "Application of Monte Carlo Simulation Method for the Estimation of*

Reliability Indices in Electric Power Generation Systems," TUBITAK Doga-Tr.,Turkish Journal of Engineering and Environmental Sciences*, ISSN 1010-7606,* ***Vol. 17****, pp. 157-163, 1993.*

8. *Randolph, P., Sahinoglu, M., "A Stopping Rule for a Compound Poisson Variable,*" J. Applied Stochastic Models and Data Analysis*, ISSN 8755-0024,* ***Vol. 11,*** *pp. 135-143, June 1995.*

9. Sahinoglu, M*., "Alternative Parameter Estimation Methods for the Compound Poisson Software Reliability Model with Clustered Failure Data,"* Journal of Software Testing Reliability and Verification (STVR)*, ISSN 0960-0833,* ***Vol. 17,*** *pp. 35-57, March 1997.*

10. Sahinoglu, M., *Çapar, S., Deely, J., "Stochastic Bayesian Measures to Compare Forecast Accuracy of Software Reliability Models,"* IEEE Transactions on Reliability, ***Vol. 50****, pp. 92-97, March 2001.*

11. Sahinoglu, M, *Bayrak, C., Cummings T., "A Study of High Assurance Software Testing in Business and DoD,"* Transactions of the SDPS, Journal of Integrated Design and Process Science, *ISSN: 1092-0617,* ***Vol. 6****, pp. 107-114, June 2002.*

12. Sahinoglu M.*, "An Empirical Bayesian Stopping Rule in Testing and Verification of Behavioral Models",* IEEE Transactions on Instrumentation and Measurement, ***Vol. 52****, No. 5, pp. 1428-1443, October 2003.*

13. *Das S. R., Sudarma M., Assaf M. H., Petriu E., Jone W. B. and* Sahinoglu M*., "Parity bit signature in response data compaction and built-in self-testing of VLSI circuits with nonexhaustive test sets,"* IEEE Transactions on Instrumentation and Measurement*,* ***Vol. 52****, No. 5, pp. 1363-1380, October 2003* .

14. *Das S. R., Petriu E., Assaf M. H. and* Sahinoglu M*., "Aliasing-Free Compaction in testing Cores-Based System-on –Chip (SOC), Using Compatibility of Response data Outputs,"* Transactions of the SDPS, ***Vol. 8****, No.1, pp. 1-17 March 2004.*

15. Sahinoglu M*., Libby D., Das S. R., "Measuring Availability Indices with Small Samples for Component and Network Reliability using the Sahinoglu-Libby Probability Model,"* IEEE Transactions on Instrumentation and Measurement, ***Vol. 54****, No.3, pp. 1283-1295, June 2005.*

16. Sahinoglu M., *Ramamoorthy C.V., "RBD Tools Using Compression and Hybrid Techniques to Code, Decode and Compute s-t Reliability in Simple and Complex Networks",* IEEE Transactions on Instrumentation and Measurement, Special Guest Edition on Testing*,* ***Vol. 54****, No.3, pp.1789-1799, Oct. 2005.*

17. *Das S. R., Ramamoorthy C. V., Assaf M., Petriu E., Jone W. B., and* Sahinoglu M.*, "Revisiting Response Compaction in Space for Full Scan Circuits With Non-exhaustive Test Sets Using Concept of Sequence Characterization," IEEE Transactions on Instrumentation and Measurement,* ***Vol. 54****, No. 5, pp. 1662-1677, Oct. 2005.*

18. *Das S. R., Assaf M., Petriu E., Jone W. B., and* Sahinoglu M*., "*Fault simulation and response compaction in full-scan circuits using HOPE*," IEEE Transactions on Instrumentation and Measurement,* ***Vol. 54****, No. 3, pp.2310-2328, Dec. 2005.*

19. Sahinoglu M*., "Security Meter- A Practical Decision Tree Model to Quantify Risk,"* IEEE

Security and Privacy Magazine, ***Vol. 3***, *No. 3, pp.18-24 April/May 2005.*
20. *Das S. R., Zakizadeh J., Biswas S., Assaf M. H., Nayak A. R., Petriu E. M.,Jone W–B. and Sahinoglu M., Testing analog and mixed-signal circuits with built-in hardware – new approach, IEEE Transactions on Instrumentation and Measurement,* ***Vol. 56***, *No. 3 pp. 840-855, June 2007.*
21. *Sahinoglu M., Trustworthy Computing: Analytical and Quantitative Engineering Evaluation (Book),* John Wiley & Sons, Inc., Hoboken, N. J., *CD ROM, Library of Congress: QA76.9.A25 S249 2007.*
22. *Sahinoglu M., Exercise Solutions Manual to Trustworthy Computing: Analytical and Quantitative Engineering Evaluation with CD ROM,* John Wiley& Sons, Inc., Hoboken, N. J., *pp.1-280, 2008. NOTE: This computational intensive solution manual is an integral educational supplement to the J Wiley textbook for classroom use by the instructor for in-depth applications of its contents; www.areslimited.com*
23. *Sahinoglu M., An Input-Output Measurable Design for the Security Meter Model to Quantify and Manage Software Security Risk, IEEE Transactions on Instrumentation and Measurement,* ***Vol. 57***, *No. 6, pp. 1251-1260, June 2008.*
24. *Sahinoglu M., Rice B, Tyson D, "An Analytical Exact RBD Method to Calculate s-t Reliability in Complex Networks", IJCITAE - International Journal of Computers, Information Technology and Engineering ISSN: 0973-743X,* ***Vol. 2***, *No.2, pp. 95-104, July-December 2008.*
25. *Sahinoglu M., "Can We Quantitatively Assess and Manage the Risk of Software Privacy Breaches", IJCITAE – International Journal of Computers, Information Technology and Engineering ISSN: 0973-743X,* ***Vol. 3***, *No 2, pp.189-191, July-December 2009.*
26. *Das S. R., Hossain A., Assaf M. H., Petriu E. M., Sahinoglu M. and Wen-Ben Jone.*, On a new graph theory approach to designing zero-aliasing space compressors for built-in self-testing, *IEEE Transactions on Instrumentation and Measurement, Vol.* ***57***, *No. 10, pp. 2146-2168, October 2008.*
27. *Sahinoglu M.*, Rice B., *"Network Reliability Evaluation", Invited Author Contributor for Wiley Interdisciplinary Reviews: Computational Statistics, New Jersey,* ***Vol. 2*** *Issue 2, pp. 189-211, March/April 2010.*
28. *Sahinoglu M., Cueva-Parra L., "CLOUD Computing," Invited Author (Advanced Review) for* Wiley Interdisciplinary Reviews: Computational Statistics*, New Jersey, Ed.-in-Chief: E. Wegman, Yasmin H. Said, D. W. Scott,* ***Vol. 3***, *Number 1, pp. 47-68, March 2011. http://authorservices.wiley.com/bauthor/onlineLibraryTPS.asp?DOI=10.1002/wics.139&ArticleID=771921*
29. *Sahinoglu M., Y.-L. Yuan, D. Banks, "Validation of a Security and Privacy Risk Metric Using Triple Uniform Product Rule," IJCITAE - International Journal of Computers, Information Technology and Engineering,* ***Vol. 4***, *Issue 2, pp. 125–135, December 2010.*

30. Sahinoglu M., *"Cybersystems and Information Security: Master of Science Program at Auburn University Montgomery," GSTF International Journal on Computing, pp. 71-76,* **Vol. 1**, *No.3 August 2011.*
31. Sahinoglu M., *Simmons S.J., Matis J.H, "Cost-Effective Security Testing of Cybersystems Using Combined LGCP: Logistic-Growth Compound-Poisson," IJCITAE - International Journal of Computers, Information Technology and Engineering, Vol.* **5**, *Issue 2, Dec. 2011.*
32. Sahinoglu M., *Cueva-Parra L., Ang D., "Game-theoretic computing in risk analysis", WIREs Comput. Stat 2012, doi: 10.1002/wics, 1205, 2012.* *http://authorservices.wiley.com/bauthor/onlineLibraryTPS.asp?DOI=10.1002/wics.1205&ArticleID=961931*
33. Sahinoglu M., *Simmons S. J., Cahoon L., "Ecological Risk-O-Meter:A Risk Assessor and Manager Software for Decision-Making in Ecosystems," Submitted on 4/30/2102 as an Invitational paper to a special "Environmental Risk Assessment" issue of Environmetrics and accepted on October 27, 2012.(wileyonlinelibtraray.com) DOI: 10.1002/env.2186. Environmetrics 2012: 23: 729-737.* *http://www.aum.edu/UR_Media/NandH/13nandh/130107/http___authorservices.wiley.com_bauthor_onlineLibraryTPS.asp_DOI=10.1002_env.pdf*
34. Sahinoglu M., *Akkaya A. D., Ang D., "Can We Assess and Monitor Privacy and Security Risk for Social Networks," (ELSEVIER) The 2012 International Summer Conference on Asia Pacific Business Innovation & Technology Management, at First World Hotel, Genting, Kuala Lumpur, Malaysia; Theme: "Green Business Innovation & Technology Management, Parallel Session Group M1- Technology/Human Resource Management, July 1 – 3, 2012. Full paper in Elsevier PROCEDIA indexed by Science Direct and Scopus: Procedia - Social and Behavioral Sciences 57 (2012) 163 – 169 http://www.sciencedirect.com/science/journal/18770428/57.*
35. Sahinoglu M., *CLOUD Computing Risk Assessment and Management, Book Chapter, (Risk Assessment and Management) Academy Publish, November 2012.* *http://www.academypublish.org/book/show/title/risk-assessment-and-management*
36. Sahinoglu M., *Cueva-Parra L., Simmons Susan J., "Software Assurance Testing Before Releasing Cloud for Business- A Case Study on a Supercomputing Grid (Xsede)", IJCITAE – International Journal of Computers, Information Technology and Engineering,* **Vol. 6**, *Issue 2, pp. 73-81, December 2012.*
37. Sahinoglu M., *Akkaya Aysen D., "Are Social Networks Risky? Assessing and Mitigating Risk" in* Significance, *the bimonthly magazine and website of the Royal Statistical Society and the American Statistical Association, July 2012.*
38. Sahinoglu M., *Ganguly S., Morton S., Samelo E., "A New Metric for Usability in Trustworthy Computing of Cybersystems" in* Significance, *the bimonthly magazine and website of the Royal Statistical Society and the American Statistical Association, July 2012.*
39. Sahinoglu M., *Akkaya A., Ang D., "Can We Assess and Monitor Privacy and Security Risk for*

Social Networks?", Procedia Social and Behavioral Sciences available on line at www.sciencedirect.com © 2012 Published by Elsevier Ltd.Selection and/or peer-review under responsibility of the Asia Pacific Business Innovation and Technology Management Society (APBITM).

40. Sahinoglu M., *"The modeling and simulation in engineering",Invitational Overview article for WIREs (Wiley Interdisciplinary Review Series), WIREs Comput. Stat 2013, p: 239-266 Doi:10.1002/wics 1254, April 2013.* http://www.aum.edu/UR_Media/NandH/13nandh/130429/Sahinoglu_WICS1254_article.pdf

41. Sahinoglu M., *Wool K., "Risk Assessment and Management to Estimate and Improve Hospital Credibility Score of a Patient Health Care Quality", Book Chapter (Society of Design and Process Science - In Development (Sept/Oct 2012): Cyber physical Systems of the Future: Transdisciplinary Convergence in the 21st Century, Editors: Sang Suh et al., to be published in August 2013 by Springer publishing, contracted 'Applied Cyber Physical Systems'.* http://www.springer.com/computer/information+systems+and+applications/book/978-1-4614-7335-0

42. *Sahinoglu M., Marghitu D., Cueva-Parra L.,Phoha V, Morton S., Stockton S., "*Analytical and Simulation Study of Operational Variations in Onshore Land Oil-Drilling Rigs for Risk Assessment and Mitigation *Advances in Security Information Management: Perceptions and Outcomes, Nova Science Publishers Book Chapter at* www.novapublishers.com *and pending for publication in Nov. 2014.*

43. *Sahinoglu M., Samelo Erman, Morton S., "Hospital Healthcare Satisfaction Risk Assessment and Management using an Automated Risk-O-Meter Software with a Game Theoretic Algorithm –, Quantitative Case Study (2013) in Alabama USA", Accepted for Publication* at Transactions of the SDPS, Journal of Integrated Design and Process Science, *ISSN: 1092-0617,* ***Vol.18,*** *Issue: 2 , pp. 1-32, DOI 10.3233/jid-2014-0001,* April 2014. http://jidps.rndsphere.com

44. *Sahinoglu M., Kramer W., "How to Increase the ROI of a Software Development Lifecycle by Managing the Risk using Monte Carlo and Discrete Event Simulation,"* Transactions of the SDPS, Journal of Integrated Design and Process Science, *ISSN: 1092-0617,* http://jidps.rndsphere.com

45. *Sahinoglu M., Stockton S., Morton S., "A Case Study on Digital Forensic Crime Risk using an Automated Software", submitted in January 2013 to* http://jidps.rndsphere.com Transactions of the SDPS, Journal of Integrated Design and Process Science, *ISSN: 1092-0617 and accepted as a book chapter*

46. *Sahinoglu .M, Morton S., Vasudev P." Airport Security and Satisfaction Risk Assessment - Management using Cost Factors,", submitted to* Submitted to JAIRM (Omniascience): *Journal of Airline and Airport Management* http://www.jairm.org; January 2013.

47. *Sahinoglu, M.; Samelo, E.; Morton, S., Hospital Healthcare Satisfaction Risk Assessment and Management using an Automated Risk-O-Meter Software with a Game Theoretic Algorithm –, Quantitative Case Study (2013) in Alabama USA, Transactions of the SDPS, Journal of Integrated Design and Process Science, ISSN: 1092-0617,* Vol.18, Issue: 2, *pp. 1-32, DOI 10.3233/jid-2014-0001, April 2014. http://jidps.rndsphere.com*

48. *Sahinoglu M., Cyber-Risk Informatics: Metrics-Based Engineering Evaluation and Statistical Analysis of Cybersystems Information Security, Textbook pp.1-450 , NOVA Science Publishers'*

Contract signed Dec. 4, 2013, submitted July 2014 and to be published in Oct. 2014.

49. *Sahinoglu M., Morton S.,Vasudev P., Eryilmaz M,* **"**Bank Customer Satisfaction: Quantitative Risk Assessment and Management", *IJCITAE – International Journal of Computers, Information Technology and Engineering*, Vol. 8, Issue 2, June-July 2014.
50. *Sahinoglu M., Morton S.,Kelsoe C., Eryilmaz M.,"Quantitiatve Metrics to Assess and Manage National Cyber Security Risk Using Risk Meter Software", IJCITAE – International Journal of Computers, Information Technology and Engineering, Vol. 8, Issue 2, June-July 2014.*

CONFERENCES and COLLOQUIA ORGANIZED

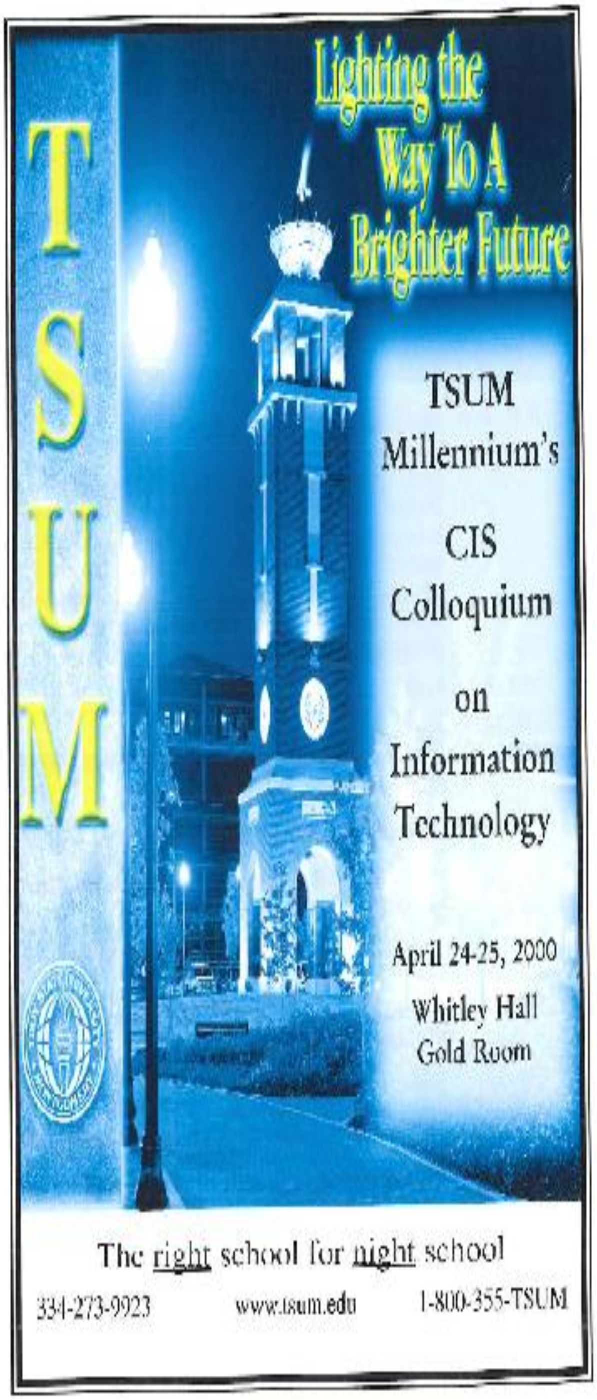
1. *Organizing Committee Chair and Academic Comm. Co-Chair, ISI/IASC/ERS; International Summer School on Model Choice and Design of Experiments- Computational Software Aspects and Practical Applications, 10-23 September, 1995, Izmir-Turkey.*
2. *Organizing Committee Chair and Academic Comm. Chair, TSUM Millennium's First CIS Symposium (3 days-20 speakers) and Colloquium on Information technology ; Keynote Speakers: Prof. C. V. Ramamoorthy, U Cal-Berkeley, Prof. C. Syzgenda, UAB-Birmingham, Prof. M. Tanik, UAB-Birmingham), April 24-25-26, 2000, Montgomery AL.*
3. *Organizing Committee Chair and Academic Comm. Chair, TSUM Millennium's Second CIS Colloquium on Information technology ; Keynote Speaker: Prof. E. P. Spafford, Purdue Univ., W. Lafayatte, IN; Feb. 27-28, 2001, Montgomery AL.*
4. *Organizing Committee Chair and Academic Comm. Chair, TSUM Millennium's Third CIS Colloquium on Information technology ; Keynote Speaker: Prof. N. Schneidewind, NPS (Naval Postgrad. School), Monterrey, Calif.; April 1-2, 2003, Montgomery AL.*
5. *Organizing Committee Chair and Academic Comm. Chair, TSUM Millennium's Fourth CIS Colloquium on Information technology ; Keynote Speaker: Dr. John Peterson, Retired NASA Software Exec. Manager, Pasadena, California; Feb. 3-4, 2003, Montgomery AL.*
6. *ASA-Alabama Chapter President's Annual Speaker Event; Speaker: Distinguished Professor Alice Smith, Head-Industrial Engineering, Auburn University, Jan. 17, 2003, TSUM, Montgomery, AL.*

7. Organizing Committee Chair and Academic Comm. Chair, TSUM Millennium's Fifth CIS Colloquium on Information technology ; Keynote Speaker: Dr. Raymond Paul, IC^{2}Technical Director, Office of the Assistant Secretary of Defense, Networks and Information and Integration, Washington D.C., Feb. 2-3 , 2004, Montgomery, AL.
8. Organizing Committee Chair and Academic Comm. Chair, TSUM Millennium's Sixth CIS Colloquium on Information technology ; Keynote Speaker: Dr. C. V. Ramamoorthy, IEEE Life Fellow, Distinguished Professor, Feb. 7-8 , 2005, Montgomery, AL.
9. Organizing Committee Chair and Academic Comm. Chair, TSUM Millennium's Seventh CIS Colloquium on Information technology ; Keynote Speaker: Dr. Alec Yasinsac, Assoc. Professor, Florida State University, Feb. 7-8, 2006, Montgomery, AL.
10. Organizing Committee Chair and Academic Comm. Chair, TSUM Millennium's Eighth CIS Colloquium on Information technology ; Keynote Speaker: Dr. Jeff Gray, Assoc. Professor, University of Alabama at Birmingham, April 3, 2007, Montgomery, AL.
11. Organizing Committee Chair and Academic Comm. Chair, TSUM Millennium's Ninth CIS Colloquium on Information technology ; Keynote Speaker: Dr. David Banks, Professor, Duke University, April 7, 2008, Montgomery, AL.
12. Organizing Committee Chair and Academic Comm. Chair, TSUM Millennium's Ninth CIS Colloquium (cont'd) on Information technology ; Keynote Speaker: Dr. James Cross, Professor, Auburn University, April 28 , 2008, Montgomery, AL.
***13.** Organizing Comm. Co-Chair of the SDPS/AUM Workshop and Conference on Informatics and Cyber-Space, Keynote Speakers: Oktay Sinanoglu (Yale), David Gibson (U of Texas), J.V. Ramamoorthy (U of Cal. Berkeley), Vir Phoha (La Tech), James Joshi (U of Pittsburgh), Stephen Goldsby (ICS Inc.), Greg Garcia (754th electronic Wing, Maxwell-Gunter AFB); Nov.1-5, 2010.* *http://www.aum.edu/uploadedFiles/Academics/Informatics_Institute/SDPSWorkshopflyer09-2.pdf*=

IT COLLOQUIUM HONORARY SPEAKERS INVITED (2000- 2009)

YEAR	*SPEAKER*	*AFFILIATION*
2000	*Prof. C.V. Ramamoorthy* *University of California, Berkeley*	*IEEE Life Fellow*
2001	*Prof. E.H. Spafford* *Purdue University, Indiana*	*IEEE &ACM Fellow* *Presidential Advisor to B.Clinton and G.W. Bush*
2002	*Prof. Norman Schneidewind* *Naval Postgraduate School, Monterrey, California*	*IEEE Fellow, IEEE Congressional Fellow*
2003	*Mr. John Peterson* *Ret. NASA / JPL / California*	*Marslander* *Project Manager*
2004	*Dr. Raymond Paul* *Pentagon / Washington, D.C.*	*IEEE Fellow, DOD Deputy under Secretary*
2005	*Prof. C.V. Ramamoorthy* *University of California, Berkeley*	*IEEE Life Fellow, Founder of IEEE Trans. SWE*
2006	*Ass. Prof. Alec Yasinsac* *Florida State University Tallahassee*	*FSU – SAIT LAB* *Founder & Director*
2007	*Assoc. Prof. Jeff Gray* *University of Alabama at Birmingham*	*IEEE Comp. Society Pres. of State of Alabama*
2008	*Prof. David Banks* *Duke University*	*ASA Journal Coordinating Editor and Member of Board of Directors, ASA Chair of the Defense and National Security*
2008	*Prof. James Cross* *Auburn University*	*Professor Chair, Co-inventor of jGRASP programming language*
2009	*http://sciences.aum.edu/departments/informatics-institute/sdps-transdisciplinary-conference*	*SDPS International Conference on Cyberspace and Cybersecurity (www.sdpsnet.org)*

Troy State University Montgomery
P.O. Drawer 4419
Montgomery, Al 36103-4419



Program

Monday, April 24:

8:30 - 9:00 Welcome Remarks by Dr. J. Sutton, Interim Vice President, Academic Affairs, TSUM; Opening Remarks by Dr. C. Martindale, Interim President, TSUM; Colloquium Highlights and Introduction of the Keynote Speaker, Prof. M. Sahinoglu, Eminent Scholar, Colloquium Chair, TSUM

9:00 - 10:00 *Main Keynote Speech*:
A Study of the Service Industry - Functions, Features and Control, by Distinguished Prof. Emeritus C. V. Ramamoorthy, UC Berkeley

10:00 - 10:15 *Break*

10:15 - 12:15 *Panel Discussion on Information Technology*:
IT Education - Challenges and Solutions for 21st Century
Panel Organizer: C. Bayrak, Colloquium Co-Chair, CIS, TSUM;
Panelists: J. Sutton, VPAA, TSUM; C.V. Ramamoorthy, UC Berkeley; S. Szygenda, Dean, UAB; M. Tanik, ECE, UAB; H. Kirkici, NASA, Huntsville; Daniella Marghitu, CS, AU; D. Watkins, Chairman, MACC, Info. Tech. Comm., S. Gramling, Appointed Director, MACC, Board of Directors; M. Sahinoglu, CIS, TSUM; J. Ala, IT Lead Teacher, Brewbaker Magnet; N. Hetzel, Major, SSG

12:15 - 1:15 Lunch

1:30 - 2:00 *Keynote Speech* (Gold Room, Whitley Hall):
Information Engineering in 21st Century: Prof. S. Szygenda, Dean of Engineering, UAB

IT Presentations/Session 1: (Session Chair: M. Mariano, Ph.D., CIS, TSUM)

2:05 - 2:20 How Can We Save More While Testing Software for Better Products? M. Sahinoglu, Ph.D., CIS, TSUM

2:20 - 2:35 Supporting Education with Adaptive Hypermedia: R. Hubscher, Ph.D., CS, AU

2:35 - 2:50 Dynamics and Control of a Flexible Link with Impact: Dan Marghitu, Ph.D., Mech. Eng., AU

2:50 - 3:05 *Break*

IT Presentations/Session 2: (Session Chair: C Bayrak, Ph.D., CIS, TSUM)

3:05 - 3:20 Unified Architectural Framework for more Complete Projects: C. Bayrak, Ph.D., CIS, TSUM

3:20 - 3:35 TABU Search and its Applications: E. Perry, Ph.D., CIS, TSUM

3:35 - 3:50 The Embedded Systems and Applications: A. Yildirim, Ph.D. Candidate, Adjunct CIS, UAB

3:50 - 4:00 Validity of some Nonlinear Measures for Varying Data Length: R. Seker, Ph.D. Candidate, UAB

4:00 - 4:10 Knowledge Discovery in Databases: S. Carmony, M.S. Candidate, CIS, TSUM

4:10 - 4:20 Past, Present Future of Encryption: R. Meyers, M.S. Candidate, CIS, TSUM

4:20 - 4:30 Implementations of a Barcode Reader Data Acquisition Interface with PIC16F84 Microprocessor: T. Mansfield, M.S. Candidate, CIS, TSUM

4:30 - 4:40 Data Link Communication: A Similation Project: M. McAndrew, M.S. Candidate, CIS, TSUM

4:40 - 4:50 A Microcontroller Aided Data Logging System: E. Udoh, S. Smith, M.S. Candidates, CIS, TSUM

4:50 - 5:00 Should Places of Online Education Use Java in Support Areas in the Classroom? F. Strickland, M.S. Candidate, CIS, TSUM

Tuesday, April 25:

9:00 - 9:30 *Keynote Speech*:
Electronic Enterprise Engineering: Prof. M. Tanik, ECE, UAB

IT Presentations/Session 3: (Session Chair: M Sahinoglu, CIS, TSUM)

9:30 - 9:45 Information Security - Past, Present and Future: S. Goldsby, CEO, INTEGRATED COMPUTER SOLUTIONS

9:45 - 10:00 ASP Intregration for Enterprise Solutions: P. Patterson, CEO, INTRANOLOGY

10:00 - 10:15 Convergence of Voice, Data and Video (AVVID): G Miles, Account Manager, CISCO

10:15 - 10:30 Electronic Commerce and Internet Security: R. Traphan, Montgomery City Director, INLINE

10:30 - 10:45 *Break*

IT Presentations/Session 4: (Session Chair: M. Sutton, CIS, TSUM)

10:45 - 11:00 Changing Directions - Moving from Client/Serve to Web-Based IT: J. Junker, Major, Software Eng. Div. Chief - SSG & Adjunct, CIS, TSUM

11:15 - 11:30 Design Pattern in Object Oriented Programming: J. Bush, Captain USAF, Air-Force Wargaming Institute

11:30 - 11:45 Computer Science Tutorials in Java: M. Mariano, Ph.D., CIS, TSUM

11:45 - 12:00 TSUM Instructional Technology Enhancement Center - An Overview: M. Stewart, Tech. Enhancement Coordinator, Adjunct, CIS, TSUM

12:00 noon Closing Remarks

Mehmet Sahinoglu, PHD

Eminent Scholar/Chair

Division of Computer & Information Science

TSUM-Montogmery AL

Will Present a Lecture On

Achieving the Quality of Verification for Behavioral Models with Minimum Effort

Where: Bldg 892 Auditorium

When: 7 April 00 1000-1100

Who: Anyone interested in Software Testing

Need more info? Check out the following slides!

POC: Debbie Mikolajczyk 416-3217 SSG/MST

Former Presidential Advisor Captures Audience at The Rosa Parks Library and Museum on Internet Security

Professor Eugene Spafford, IEEE Fellow, recipient of National Computer Systems Award 2000, and an internet security advisor to former President Clinton, captivated a full auditorium at Rosa Parks Library and Museum on February 27, 2001 with his stunning yet highly informative remarks on "The Challenge of Secure Software." His morning lecture to the Chamber of Commerce audience of 200, including attendees from Maxwell and Gunter AFB and software engineering related companies with interest on software security, was also successful. Dr. Terry Dixon, vice president for academic affairs, introduced Dr. Spafford's and praised him for his contributions to the field.

Dr. Spafford first cited a brief history of where the secure software 12 years ago, with only 75,000 machines connected, has developed into a non-secure one today, with an excess of 250 million users over 150 countries with a volume of traffic doubling every 90 days. In 1989, there were a handful of security breaches. In 2001, this figure is estimated to reach 65,000. The state of security is poor. DOD reported 22,000 attacks on Pentagon Systems in 2000. Real losses exceed billions of dollars. In March 1999, "Melissa," caused $300 million in approximately four days affecting 150,000 systems, and in May 2000, "ILOVEYOU," in one day affecting more than 500,000 systems, caused a shocking $10 billion in damages. Average losses for the Internet connected companies are $1 million per year. Moreover, 50-60 incidents per day on the Internet, 10-12 incidents per day on DSL and 5-6 incidents per day on dial-up still prevail. For defenses the following are needed: (a) virus prevention on largely pattern based methods need updates, (b) firewalls largely pattern based as well need updates as we can't control users, and (c) security scanners should look for known flaws and misconfiguration. At this rate, the world in 2004 will face 100,000 computer viruses causing an estimated loss of $100 billion per year. Dr. Spafford added that a typical user is an open target since he has less than one year on line with no background in computer science, has a major OS with 1 Ghz machine but uses only 3 applications, does not take back ups and he is on-line constantly surfing the net. He said COTS (Commercial Products over the Shelf) have poor quality and consumers should push for quality and assurance not for extra features they do not ever use. Wireless technology even enhances eaves dropping and unsafe environments. New technology is needed where stronger encryption is required and automated self-defenses are required with a greater reach from far away. How about the law? He said, a new law UCITA (http://www.4cite.org/; http://www.acm.org/usacm/IP/) is pro-commercial-companies, not protecting the poor defenseless end-user. Law enforcement on software assurance and security is handicapped. National and international laws have to be unanimously passed and enforced. Dr. Spafford focused on the importance of the university education to help resolve the big picture. He said he was happy to see that software quality based engineering courses were offered at TSUM/CIS. He concluded that better security is certainly possible if the users demand for it. Dr. Spafford also responded to questions from the audience ranging from Linux Security to security education at colleges. His closing thought was: "There is more to life than increasing its speed" by Mahatma Gandhi. Dr Spafford's journey to Montgomery was co-sponsored by TSUM/CIS and ICS, a local software security company.

TSUM/CIS is grateful to Professor Spafford, TSUM administration, Montgomery Chamber of Commerce's business, military, and civil audience for making this event a memorable and unforgettable learning experience for all involved.

Dr. M. Sahinoglu, Eminent Scholar, CIS

Troy State University Montgomery Presents The Third Annual

Colloquium on Information Technoloc

Dr. Norman Schneidewind

Director of the Software Metrics Research Center, Division of Computer and Information Sciences, and Operations at the Naval Post Graduate School in Monterey, CA

Distance

Software Reliability

Modeling

Software Quantity

Computer *Metrics*

Performance

Analysis

Monday, April 1, 2002

5:30 – 6:30 p.m.
r. Schneidewind will address TSUM Students on the topic of oftware Engineering – Risk & Reliability.

COST: $No charge to TSUM students

LOCATION:
The Rosa Parks Library & Museum Auditorium

In January 2002, Dr. Schneidewind was awarded the **"IEEE Reliability Engineer of The Year (2001)" by the IEEE Reliability Society.** Dr. Schneidewind is developer of the Schneidewind software reliability model that is used by NASA to assist in the prediction of software reliability of the Space Shuttle, by the Naval Surface Warfare Center for Trident and Tomahawk software reliability prediction, and by the Marine Corps Tactical Systems Support Activity for software reliability assessment. Other projects have included:

- Studies on information systems for the Library of Congress
- National Traffic Data Center, U.S. Department of Transportation
- Bay Area Rapid Transit System computer control system
- Navy Submarine Logistics project, and the Marin County data processing study

SPONSORED BY

Bb Blackboard www.blackboard.com

Cisco Systems Empowering the Internet Generation

Blackboard | **I Tech** | **Cisco**

FOR TICKETS contact Angela Barrow at (334) 241-9764, abarrow@tsum.edu or Contact Loretta Kirk at (334) 273-9923 or lkirk@tsum.edu at the Gunter Annex

The Colloquium is supported by the Department of Computer and Information Science and the Distance Learning Center of Troy State University Montgomery.

Troy State University Montgomery (TSUM) Presents The Fourth Annual

Colloquium on Information Technology

John C. Peterson

Vice President of Sales and Marketing for TLC - Watch, Inc.

Monday, February 3, 2003

"Shall We Dance"
5:30 - 6:30 p.m.
(Student Audience - Reception to follow)

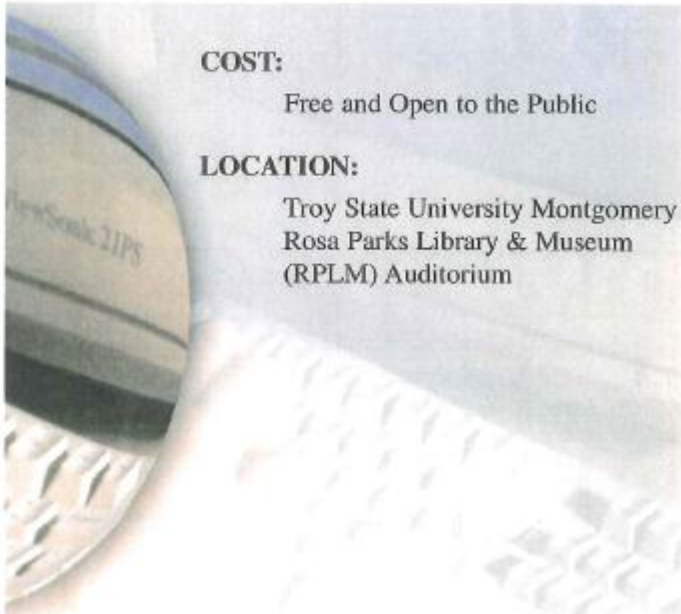
Our ability to build software–intensive systems in order of magnitude is greater today than it was just five decades ago. Yet, our appetite for software has grown even faster and the software industry is still evolving from craft to an engineering discipline.

John C. Peterson will demonstrate and simulate complex software systems for product development. Mr. Peterson draws upon his own personal experiences, but also upon a range of companies as diverse as Boeing, Sony, Daimler Chrysler, Starbucks etc...

Tuesday, February 4, 2003

"Let's Be Realistic About the Future of Our Companies"
11:30 a.m. - 12:15 p.m.
(Local IT Industry and Community Audience/ Montgomery Area Chamber of Commerce)

Mr. Peterson will explain a time-tested approach to implement an adaptive organization based on the hybrid method. This approach defines ten essential elements of adaptive organizations and presents models that illustrate how each element fits into the overall enterprise picture. Speed-to-market, customer intimacy, operational excellence, and organizational agility (however important) are not adequate strategic objectives in and of themselves. They are attributes of the real objective—systematic adaptation. Adaptation implies more than agility. It requires appropriate and quick organizational response to change.



COST:

Free and Open to the Public

LOCATION:

Troy State University Montgomery
Rosa Parks Library & Museum
(RPLM) Auditorium

John C. Peterson has 25 years of experience in R&D management at the Jet Propulsion Laboratory in distributed high performance computing, networking, and complex system simulations.

Mr. Peterson is now working as a VP of Sales and Marketing for TLC-Watch, Inc., a startup company manufacturing digital video surveillance systems for traffic transportation and building security.

He was a key contributor to the NASA pathfinder mission to Mars in 1996. During this period, Mr. Peterson:

* granted seven patents
* published over thirty articles
* gave numerous keynote speeches
* earned two NASA service medals for his contribution to complex system simulations and high performance computing
* received three additional NASA service awards for product innovation and technology transfers

For additional information, please contact Dr. Mehmet Sahinoglu, Professor and Chairman, Department of CIS, Troy State University Montgomery (TSUM), at (334) 273-9923 or E-mail (mesa@tsum.edu).

The Colloquium is supported by the TSUM Department of Computer and Information Science, College of Business, and The Graduate School.

Troy State University
Montgomery

Presents The Fifth Annual
Colloquium on Information Technology

Dr. Raymond Paul
Office of the Assistant Secretary of Defense
Networks and Information and Integration, Technical Director

Monday, February 2, 2004

"The Future of Computer Software Systems: Educational Outlook"
5:30 - 6:30 p.m.
(Student Audience)

Web Services (WS) received significant attention recently by government agencies and computer industries. WS provides a new architecture/paradigm for building distributed computing applications based on XML. It provides a uniform and widely accessible interface to glue the services implemented by the other middleware platform over the Internet by utilizing standard Internet protocols such as WSDL, SOAP, and UDDL.

While WS is still early in its maturing processes, many issues still need to be addressed, e.g., finalizing draft specifications, runtime verification and validation, and quality assurance by the UDDI servers. Many keen observers agree that WS represents a new significant trend for software systems integration that will be developed, structured, acquired, and maintained. For example, instead of buying and maintaining software, software can be leased and downloaded when needed. In this way, software upgrades will be automated because the latest version will be used when the service is called at runtime.

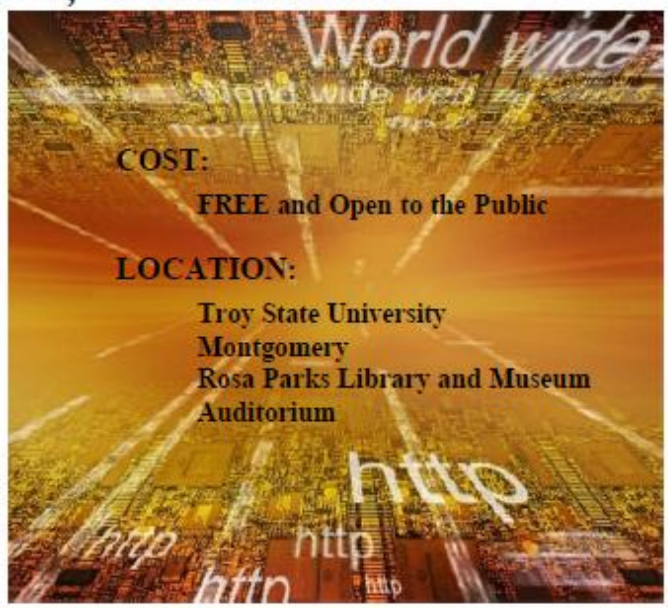
WS implementation also requires a loosely coupled architecture where new services can be added at runtime and old services can be replaced. Furthermore, vendors will compete to supply most dependable and/or marketable services on the web, and this will also change the way software industries earn their revenue.

Tuesday, February 3, 2004
11:00 - 11:40 a.m.

"The Future of Computer Software Systems: Commodity or Service?"
(Local IT Industry, Community Audience and Montgomery Area Chamber of Commerce)

The concepts of Web Services (WS) is far beyond software. In the future, hardware will also have a corresponding service where hardware vendors will supply new components to fit into existing well-published architecture for specific applications. Quality assurance, as well as security and privacy, will be important for both service clients and providers, including those serving as intermediate agents such as UDDI servers.

WS provides a new way for globalization where companies, regardless of their background, such as nationalities, languages and culture, must now compete in a global market, where the only rule is interoperability via architecture and interfaces. It is no longer possible to have local or national markets where local companies can do well, due to market segmentation. If a company does not compete in the service market globally, it will wither as soon as new replacement services are published on the web. This will increase the pace of global competition and the companies that have the great software technology will win, instead of the one that has the great financial resources only.



COST:

FREE and Open to the Public

LOCATION:

Troy State University
Montgomery
Rosa Parks Library and Museum
Auditorium

As a professional electronics engineer, software architect, developer, tester and evaluator for the past 24 years, **Dr. Raymond Paul**, has held many positions in the field of software engineering. Currently, Dr. Paul serves as the technical director for command and control (C2) policy in the Office of the Assistant Secretary of Defense Networks and Information and Integration. In this position, Dr. Paul supervises command and control systems engineering development and capabilities for objective, quantitative and qualitative measurements concerning the status of software/systems engineering resources and evaluates project outcomes to support major investment decisions. This measurement data is required to meet various Congressional mandates, most notably the Clinger-Cohen Act.

Dr. Paul holds a doctorate in software engineering and is an active member of the IEEE Computer Society. He has published more than 59 articles on software engineering in various technical journals and symposia proceedings, primarily under DoD and IEEE sponsorship. IEEE awarded Dr. Paul with the Fellow grade in December 2003 for his contributions to metric-guided testing and evaluation of software systems.

For additional information, please contact Dr. Mehmet Sahinoglu, Professor and Chairman, Department of CIS, Troy State University Montgomery at (334) 273-9923 or E-mail (mesa@troyst.edu).

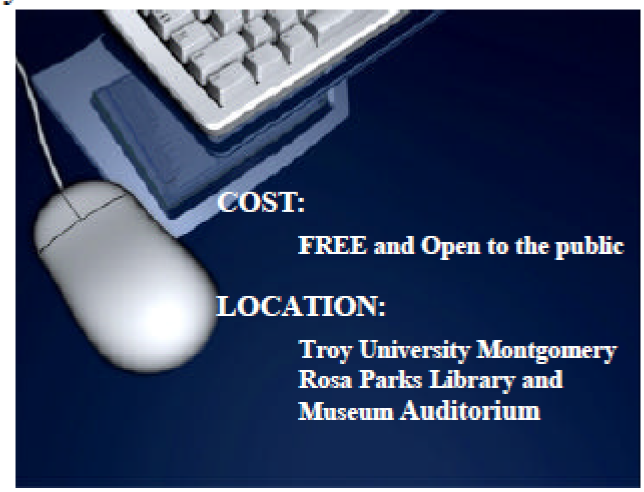
The Colloquium is supported by the TSUM Department of Computer and Information Science College of Business and The Graduate School.

www.tsum.edu

Troy University, Montgomery Campus

Presents The Sixth Annual
CIS Colloquium on Information Technology

Professor Emeritus C.V. Ramamoorthy
Computer Science Division
University of California, Berkeley



Monday, February 7, 2005
5:30 - 6:30 p.m.

"Quality Concerns in Software Supported Systems - Modeling Approach"
(Student Audience)

We introduce three new models. The first is the Dynamic Life Cycle Product Model. This model considers the life cycle quality considerations of the product, the product line and the product family. The second is the Endo-Exo Model, which is based on analogous notions of the Heisenberg Uncertainty Principle. These models explore the multiple views of quality as seen by different stakeholders. In simpler terms, they are the models of 'inside-out' views as seen by the designers and the 'outside-in' views as seen by the users and others. The third model is the Delta model, which helps designers and modifiers (maintainers) to make fast but effective trade-off decisions while performing major design tasks. These models are simple geometric models, and many of them use triangles as the primary tool. We provide examples for these models and show how that they give valuable insights.

Tuesday, February 8, 2005
11:30 - 12:15 p.m.

"Quality Concerns in Software Supported Systems - Business Approach"
(Local IT Industry, Community Audience and Montgomery Area Chamber of Commerce)

Complex systems, services and enterprises are very dependent on computer-communication technology and in particular on their supporting and controlling software. The system quality or the degree of its user satisfaction, also called its utility, often is based on the effectiveness of its software component. The quality of the system is felt only after the system or the product is introduced and used. Designers attempt to introduce quality-creating attributes during every phase of development and implementation. Quality models should anticipate quality concerns ahead of the product introduction and its use. They also should help in instrumenting and monitoring the effectiveness of quality measures during the lifetime of the products, product lines and product families. In this presentation, we shall provide a historical overview of the evolution of software quality and its essential quality attributes to improve customer satisfaction.

C. V. Ramamoorthy, Professor Emeritus, received two M.S. degrees, one in Mechanical Engineering from the University of California, Berkeley, CA, and another M.S. and a Ph.D. degree in applied mathematics and computer science from Harvard University, Cambridge, MA. He is the author of more than 200 journal papers, co-editor of three books, as well as a supervisor to 79 doctoral students. He is the recipient of many awards and honors: IEEE Centennial and Millennium, 2000; IEEE Computer Society's Group and Taylor-Booth and Kanai-Hitachi, 2000; Golden Core Recognition, 1999; T. T. Yeh Distinguished Achievement; Distinguished Scholar, SDPS, 1995; IEEE Fellow for Life 1993; IEEE Richard E. Merwin, 1993; IEEE Computer Society Meritorious Service, 1991; Keynote Speaker, IEEE International Conference on Distributed Computing Systems, 1991; IEEE Computer Society Taylor Booth, 1990; IEEE Computer Society, Outstanding and Best Paper, 1987, 2003; IEEE Centennial Medal, 1984; Fellow, IEEE, 1978; IEEE Computer Society, Special Education, 1978; and IEEE Computer Society, Honor Roll, 1974. Professor Ramamoorthy conducts research on the evolution of computer hardware & software systems.

For additional information, please contact Dr. Mehmet Sahinoglu, Professor and Chair, Department of CIS, Troy University, Montgomery Campus at (334) 273-9923 or E-mail (mesa@troyst.edu).

The Colloquium is supported by the Troy University, Montgomery Campus' Department of Computer and Information Science, College of Arts and Sciences and The Graduate School.

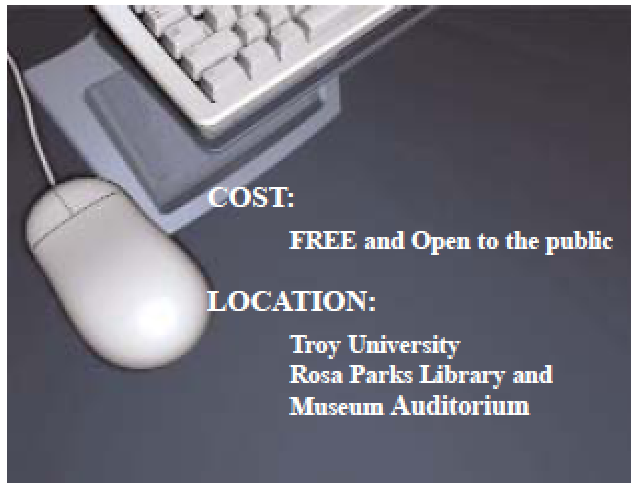
www.tsum.edu

Troy University

Presents the Seventh Annual

Computer Science Colloquium on Information Technology

Associate Professor Alec Yasinsac
Computer Science Department
Florida State University (FSU)



Tuesday, February 7, 2006
5:30 - 6:30 p.m.

"SAIT Laboratory: Synthesizing Research, Outreach and Education"
(Student Audience - Reception to follow)

Basic research is primarily conducted in three venues: Government, industry and academia; each with its distinct strengths and weaknesses. Carnegie I universities, such as FSU, demand top quality research, validated through peer reviewed publication and federal funding. At SAIT Laboratory, our charter is to integrate our research and teaching to improve the quality and impact of each. Faculty-student partnerships facilitate mentor relationships that continue the researcher pipeline and ensure topical and approach freshness in the research process. In this talk, we present the SAIT Laboratory academic research approach, including detailing past successes and highlighting existing and upcoming opportunities.

Wednesday, February 8, 2006
11:00 a.m. - 12:15 p.m.

"Security Aware Software"
(Local IT Industry, Community Audience and Montgomery Area Chamber of Commerce)

Most instances of software exploitation are really software failure. Even though we cannot eliminate vulnerability from modern information systems, we can reduce exploitable code long term with sound robust development practices. We argue that the current hot topic of so-called "secure coding" represents commonly taught coding techniques that ensure robustness, rather than ensuring any commonly understood concept of security. Weaving the practice of rigorous coding techniques into curriculum is essential-coding for security is useless apart from fault-tolerant foundations. However, security-specific coding techniques should be integrated pedagogically alongside robustness so that students can distinguish the two. We propose a shift in instructional methods based on this distinction to help future programmers, developers and software engineers produce "security-aware" software.

Dr. Alec Yasinsac is an associate professor at Florida State University. He joined the FSU Computer Science Department in August 1999 after a twenty year career in the United States Marines as a Data Systems and Communications Officer. He has operational experience in software development, information systems management, network engineering and information security, having spent active duty tours in Japan, Korea, North Carolina, California and Virginia.

Dr. Yasinsac received his doctoral degree in computer science from the University of Virginia, where his thesis advisor and mentor was Bill Wulf. His major research interests are network and wireless security, cryptography, intrusion detection and security protocols. He has published over forty refereed conference, symposium and journal papers in the past five years on formal methods, cryptographic authentication, group encryption, secure routing protocols, wireless security, intrusion detection, digital forensics and on a variety of computing education topics.

He is presently funded by the National Science Foundation, Department of Defense, the Army Research Office and several industrial partners. His professional activities include membership in several program committees including the European Symposium on Research in Computer Security, International Symposium on Recent Advances in Intrusion Detection, IEEE Information Assurance Workshop, the IRMA International Conferences, the International Conference on Information Systems Security and the International Performance Computing and Communications Conference.

For additional information, please contact Dr. Mehmet Sahinoglu, Eminent Scholar, Professor and Chair, Department of Computer Science, Troy University at (334) 832-7289 or E-mail (mesa@troy.edu) or Angela Crooks, department secretary at (334) 832-7282 or E-mail (acrooks@troy.edu).

The Colloquium is supported by the Troy University Department of Computer Science, College of Arts and Sciences, The Graduate School and Co-sponsored by Integrated Computer Solutions Inc.

www.troy.edu

TROY UNIVERSITY

Presents the Eighth Annual
Computer Science Colloquium on Information Technology

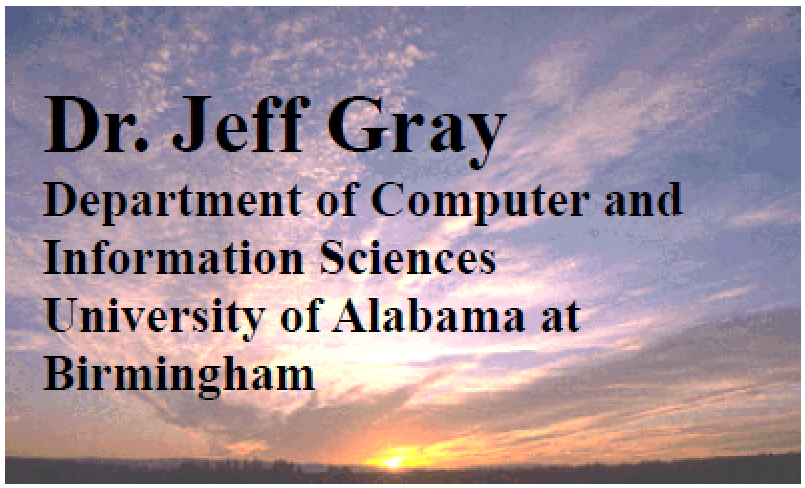
Automating Software Evolution through Model-Driven Engineering

Tuesday, April 3, 2007
5:30 - 6:30 p.m.
Troy University
Rosa Parks Library and Museum Auditorium
Montgomery Campus
(Reception to follow)

Model-Driven Engineering (MDE) represents a design approach that enables description of the essential characteristics of a problem in a manner that is decoupled from the details of a specific solution space (e.g., dependence on specific middleware or programming language). Domain-Specific Modeling (DSM) is an MDE methodology that generates customized modeling languages and environments from metamodels that define a narrow domain of interest. From these models, other artifacts of software development (e.g., source code or configuration files) can be generated by model translators.

The interest and adoption of DSM over the past decade has surged. Strong support for basic research has been committed by the large European Union ModelWare project ($30M Euros). Metamodeling tools that support DSM continue to emerge from both commercial and open source projects (e.g., Microsoft's DSL Toolkit and the Eclipse Modeling Project), as well as numerous academic research projects (e.g., Vanderbilt's Generic Modeling Environment). Initial success stories from industry adoption of DSM have been reported, with perhaps the most noted being Saturn's multi-million dollar cost savings associated with timelier reconfiguration of an automotive assembly line driven by domain-specific models.

This presentation will provide a general introduction to MDE with a specific focus on the capability to evolve software artifacts through model transformation and program transformation. The benefits of MDE will be showcased through case studies taken from models supporting different domains (e.g., avionics mission computing).



Dr. Jeff Gray is an assistant professor in the Department of Computer and Information Sciences at the University of Alabama at Birmingham (UAB) where he directs research in the Software Composition and Modeling (SoftCom) laboratory. He received his Ph.D. in May 2002 from the Electrical Engineering and Computer Science department at Vanderbilt University, where he also served as a research assistant from 1999-2002 at the Institute for Software Integrated Systems (ISIS).

Dr. Gray's research interests include model-driven engineering, aspect-oriented software development and generative programming. He has recently published on these topics in *Communications of the ACM* and *IEEE Computer*. In the past, his research was supported by DARPA and an IBM Eclipse Innovation grant. He currently is supported by two NSF grants, including a 2006 NSF CAREER award.

Dr. Gray is currently the chair of the Alabama IEEE Computer Society. He has served on over 90 organizing and programming committees and was a recent guest editor for three different journal special issues. He is a cofounder of the Domain-Specific Modeling series of workshops at OOPSLA and serves on the organizing committees of the upcoming MODELS and GPCE conferences.

More information about his research and publications can be found at (http://www.cis.uab.edu/gray).

For additional information, please contact Dr. Mehmet Sahinoglu, Eminent Scholar and Professor, Department of Computer Science, Troy University at (334) 832-7289 or E-mail (mesa@troy.edu).

The Colloquium is supported by the Troy University Department of Computer Science, College of Arts and Sciences and The Graduate School.
www.troy.edu

TROY UNIVERSITY

Presents the Ninth Annual Computer Science Colloquium on Information Technology

Applications in Adversarial Risk Analysis

Monday, April 7, 2008
5:30 p.m. - 6:30 p.m.
Troy University
Rosa Parks Library and Museum Auditorium

Adversarial risk analysis is a new research area that combines elements of statistical risk analysis, mathematical game theory and economic portfolio analysis. This talk describes applications in counterterrorism, computer security, corporate competition and regulatory policy. A key ingredient is the Kadane-Larkey formulation of game theory, which is a Bayesian alternative to the less flexible, and less realistic, minimax criterion.

Dr. David Banks
Duke University

Dr. David Banks is a Professor of Practice of Statistics at Duke University. He is currently the coordinating editor of the Journal of the American Statistical Association, Chair of the ASA Section on Defense and National Security, and a member of the ASA Board of Directors. Previously, he held three positions in the federal government (the FDA, the DOT, and the National Institute of Standards and Technology) and academic positions at Carnegie Mellon and the University of Cambridge. His research involves Risk Analysis, metabolomics, network models, and data mining.

For additional information, please contact Dr. Mehmet Sahinoglu, Eminent Scholar and Professor, Department of Computer Science, Troy University at (334) 832-7289 or E-mail (mesa@troy.edu).

The Colloquium is supported by the Troy University Department of Computer Science, College of Arts and Sciences and The Graduate School.

TROY UNIVERSITY
A future of opportunities.
www.troy.edu

Troy University Computer Science Dept.'s Information Technology Seminar - 2008

jGrasp: Intuitive Visualizations for Understanding Software

Presented by:
Dr. James H. Cross II
Dept. of Computer Science and Software Engineering
Auburn University

Tuesday April 29, 2008
5:30 pm - 6:30 pm
Troy University Rosa Parks Library and Museum Auditorium

For additional information, please contact Dr. Mehmet Sahinoglu, Eminent Scholar and Professor, Dept. of Computer Science, Troy University—Montgomery at:

Phone: 334-832-7289 or 334-832-7282
Fax: 334-241-9589
E-mail: mesa@troy.edu

ABSTRACT: jGrasp is an IDE that provides automatic generation of visualizations for the major object-oriented concepts in Java: control structures, classes, interfaces, objects, inheritance, polymorphism, composition, and data structures. jGrasp produces Control Structure Diagrams (CSDs), UML class diagrams and most recently, dynamic object views that work in conjunction with the visual debugger and workbench. A data structure identifier mechanism attempts to identify and render traditional abstract visualizations for common data structures such as stacks, queues, linked lists, binary trees, heaps, and hash tables. These are dynamic visualizations in that they are generated while running the user's program in debug mode. Hence, they can help bridge the gap between implementation and the conceptual view of data structures.

BIO: Dr. Cross is a Professor of Computer Science and Software Engineering at Auburn University where he served two terms as department chair (1996-2006). Dr. Cross teaches and directs research in the areas of object-oriented design and programming, visualization, and environments. His recent efforts include the jGrasp research project which is focused on the automatic generation of Graphical Representations of Algorithms, Structures and Processes for software (http://www.jgrasp.org).

SOCIETY FOR DESIGN AND PROCESS SCIENCE

SOFTWARE ENGINEERING SOCIETY

Final Program 2009

Montgomery, Alabama

The Informatics Institute
Auburn University at Montgomery
November 1-5, 2009

Dedicated to the memory of Dr. Percy Julian

Theme

Informatics & Cyberspace: Transdisciplinary Research and Education

Sponsored by

Society for Design & Process Science (SDPS)
Software Engineering Society (SES)
Auburn University at Montgomery
GEMSAN-Istanbul-Turkey

Co-sponsored by

IC² Institute, University of Texas
Intelligent Systems Technology Inc.
University of Alabama at Birmingham

Invitation from Auburn Montgomery

It is my great pleasure to welcome you to "Informatics & Cyberspace: Transdisciplinary Research and Education" on the campus of Auburn University at Montgomery. We are honored to host SDPS, its members and guests and to give you a taste of the hospitality for which the South is known.

As part of the conference, you will have the opportunity to learn about our new Informatics Institute. We are excited about the opportunities the institute will provide our students as well as its potential for fruitful research in the field of data and information security. We are deeply committed to the creation of programs addressing transdisciplinary issues and the potential they have for expanding knowledge and learning.

In addition to the learning opportunities at the SDPS conference, we have planned a variety of activities to "show off" Montgomery. The city is the birthplace of both the Civil War and the Civil Rights Movement and offers much to see and do. Specifically, we have planned an evening at the renowned Alabama Shakespeare Festival, an evening in historic downtown Montgomery and a relaxing dinner cruise on a 19th century riverboat.

John G. Veres III
Chancellor
Auburn University at Montgomery

From the President

Dear Fellow Transdisciplinarians:
It is a special honor and privilege to invite all of you to the SDPS 2009 conference-workshop, which is being organized at the Auburn University at Montgomery campus on 1-5 November 2009. This significant event is the result of a collaboration between the Informatics Institute at Auburn University at Montgomery, SDPS, and SES.

Our special gratitude goes to Professor Murat M. Tanik, Professor Mehmet Sahinoglu, various SDPS committees, and the local organizing committee for planning its fruition. The significant commitment of resources for this event by Dr. John Veres III, chancellor of AUM, is greatly appreciated.

It is our hope and expectation that various conference activities and the informal atmosphere of the workshops will attract a wide spectrum of participation as well as members of the transdisciplinary community to explore new and original themes under the broad umbrella of cross-disciplinary research and education, which we will then expand and develop into full tracks at the SDPS 2010 conference in Dallas.

As usual, this SDPS-AUM conference-workshop will represent an experiment in challenging the research and education community to push into new frontiers in complementary forms to disciplinary thinking. Please consider joining us to make this experiment a grand success with your contributions and presence.

Sincerely,
Sumit Ghosh, President, SDPS

Founding Fathers of Software Engineering

C. V. Ramamoorthy and R. T. Yeh, while they were establishing the discipline during late 1960s and early 1970s, probably never envisioned the discipline they were developing would one day be intimately tied to all other disciplines. With their seminal role in the establishment of SDPS during the mid-1990s they showed us the ubiquitous nature of software. Nobel Laureate Herb Simon's seminal talk at SDPS 2000, on the role of software in the society, paved the way for the establishment of the Software Engineering Society (SES) as a transdisciplinary function of SDPS in 2000.

Since then SES is in the process of development towards becoming the society of the future. Software engineering, being inherently transdisciplinary, certainly owns the future. I invite all software practitioners and engineers to join me in the expansion of SES. See you at beautiful Montgomery on November 1-5, 2009, to get engaged and prepare a grand SES event for the next SDPS conference.

Hiroshi Yamaguchi,
SES President,
Japan

Transdisciplinarity: The George Kozmetsky Way

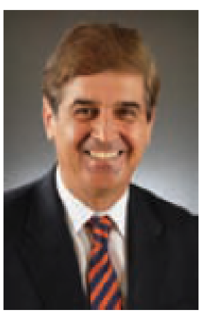
As the prefix "trans" indicates, transdisciplinarity (a term introduced in 1970 by Jean Piaget) concerns that which is at once between the disciplines, across the different disciplines, and beyond each individual discipline. Its goal is the understanding of the present world, of which one of the imperatives is the overarching unity of knowledge.

During the 1994 Systems Integration Conference in Brazil, fate brought together David Gibson and Murat M. Tanik. Murat explained the plans for establishing a new society in the flavor of transdisciplinarity without being familiar with the term at the time. David told Murat that he should visit with George Kozmetsky and explain these ideas to him. Eventually, David, George, and Murat met at IC² institute. The beginnings of SDPS were already taking shape, including the name, star-shaped logo, bylaws and basic concepts. The logo represents information integration through communication. After some discussions, George said, "Tell Ram to call me," meaning Prof. C.V. Ramamoorthy. The rest is history for the establishment of the Society for Design and Process Science. Eventually, SDPS is established by the founding board, which was composed of late Dr. G. Kozmetsky (chairman), Dr. C. V. Ramamoorthy, Dr. R. T. Yeh, Dr. A. Ertas, and Dr. M. M. Tanik. SDPS was incorporated in the State of Texas on September 6, 1995 and Dr. R. T. Yeh was elected as the first president of SDPS.

This year, at the newly minted Informatics Institute of AUM, located in the historical heart of the beautiful state of Alabama, we will again discuss the transdisciplinary solutions for the issues and problems concerning our immediate surrounding and the society-at-large.

David Gibson, Stan Gatchel, and Murat M. Tanik

The Informatics Institute



Informatics studies the application of information technology to practically any field while also considering its impact on individuals, organizations, and society. In practice, it uses computation as a universal tool to solve problems to communicate, generate, process, store, and express ideas.

Montgomery and the surrounding River Region are home to many businesses and military functions that greatly need degree programs in Information Assurance. The Informatics Institute at AUM will initiate a new graduate program in cyber systems and information security to help meet current and future workforce needs in south central Alabama. The Informatics Institute and AUM proudly invite the participants from all corners of the globe to dicuss these current educational and research trends. I only hope that you will carry back unforgettable memories from our beautiful capital city and dynamic, scenic campus as a result of this enviable collaboration between AUM and SDPS.

Mehmet Sahinoglu
Director
AUM Informatics Institute

Scheduled Speakers

Professor Oktay Sinanoglu
Keynote Speaker
Endowed Chair,
Molecular Biology

Professor Oktay Sinanoglu has been nominated twice for Nobel Prize. He is a Turkish scientist of theoretical chemistry and molecular biology. At age 28, he became the youngest person in 20th century at Yale University to attain status as a full professor. He earned a degree in chemical engineering from the University of California, Berkeley with the highest rank. In only eight months, he graduated from MIT in 1957 with the highest degree. In two years, he finished his doctorate at UC Berkeley.

He theorized the "Many-Electron Theory of Atoms and Molecules" in 1962 by solving a mathematical theorem that had been unsolved for 50 years. The same year, he earned the Alfred P. Sloan prize. He has two lifelong chairs at Yale in Molecular Biology and was the first to earn the Alexander von Humboldt Science Prize in 1973. In 1975, he won the award of Japan's International Outstanding Scientist. In the 1980s, he theorized a new method from 180 theories concerning mathematics and physics, considered revolutionary, which enables chemists to predict the ways in which chemicals combine in the laboratory and to solve other complex problems in chemistry using simple pictures and periodic tables.

David V. Gibson

David Gibson is associate director of IC² Institute. His Ph.D. is from Stanford University with an emphasis in organizations, communication theory, and innovation. During 2000-2001, he was a Fulbright Scholar at Insituto Superior Tecnico, Lisbon, Portugal. He teaches Knowledge/ Technology Transfer and Adoption in IC²'s MSSTC degree

INVITED ACADEMIC MEETINGS and NPR RADIO INTERVIEWS

1. *Compound Poisson density estimation of the number of software failures. First Kickoff Workshop Conference on Software Reliability Engineering, Washington DC, 1990.*
2. *Academic-professional training of statisticians and industry-university relations. III Harma Meeting of Design of Experiments and Statistical Education; Proceeding of Design of Exp. and Stat. Education pp. 216-228, Cordoba, Spain, 1994.*
3. *Statistical measures to evaluate and compare predictive quality of software reliability estimation methods. IP-46, 51st Session of the ISI, Istanbul, Turkey, 1997.*
4. *Bayesian measures to compare predictive quality of software reliability estimation methods (1998), invited session on software reliability, International Conference on Reliability and Survival Analysis, NIU, DeKalb, IL, May 21-24, 1998.*
5. *Is your Computer Working? Radio Interview on National Public Radio (NPR), Montgomery, AL, Oct 14, 2000.*
6. *Empirical Bayesian Availability Index of Safety and Time Critical Software Systems with Corrective Maintenance., The University of Alabama, Electrical and Computer Engineering Department, International Seminar Series, Birmingham, Alabama, October 27, 1999.*
7. *A Software Stopping Rule Algorithm for Industry to Save Time and Effort? RST (Reliable Software Technologies), Washington D.C., Nov 19, 2000.*
8. *Testing International Waters? Radio Interview on National Public Radio (NPR), Montgomery, AL, Dec. 31, 2000.*
9. *Rapid Response Research and Development Pool (R3DP), Montgomery Area Chamber of Commerce (MACC), April 4, 2000.*
10. *Impacts of AOL and Time -Warner Merger on Cyber-World? Radio Interview on National Public Radio (NPR), Montgomery, AL, April 4, 2000.*
11. *Panel Organizer: IT Education: Challenges and Solutions for 21st Century, CIS Colloquium on IT, April 24, 2000.*
12. *The New Trends in Information technology, jointly with Prof. C.V. Ramamoorthy; Radio Interview on National Public Radio (NPR), Montgomery, AL, April 25, 2000.*
13. *Panel Organizer and Chair, Panel Topic: The Impact of Software Quality and Reliability in 21st Century, IDPT2000, Dallas, June 4-8, 2000.*
14. *Achieving the Quality of Verification for Behavioral Models with Minimum Effort, Bldg. 892,*

Auditorium, SSG/MST Gunter AFB, Montgomery AL, and April 7, 2000.
15. *Reliability Index Calculations of Integrated Software Systems (Internet) for Insufficient Failure and Recovery Data using Sahinoglu-Libby PDF, The First Biennial International Conference on Advances in Information Systems, ADVIS'2000, Dokuz Eylul University, Dept. of Computer Engineering, Izmir-Turkey, Oct. 25-31, 2000.*
16. *Invited Panelist in the panel:" Testing in High Assurance Systems Engineering" and Session Chair, HASE'00, Albuquerque, NM, Nov. 2000.*
17. *Has Internet been on your mind? NPR (National Public Radio) Interview with Carolyn Hutcheson January, 2001.*
18. *On Internet Security Seminar by Former Pres. Advisor, Prof. E. Spafford, Purdue U. with S. Goldsby, CEO, ICS, NPR (National Public Radio)Interview with Carolyn Hutcheson Feb. 2001.*
19. *Honorarium Speaker at SDPS IDPT Conference in Pasadena, Cal., June 2001.*
20. *On Software Reliability with Prof. N. Schneidewind, NPS (Naval Postgraduate School), IEEE Reliability Engineer Year 2001, NPR (National Public Radio) Interview with Carolyn Hutcheson Apr. 2, 2002.*
21. *On "Power Generation Reliability Estimation and Planning- A Case Study in Turkish Interconnected System", a slide presentation invited by Tom Newdome, Scott Thurman et. al. of Alabama Power Company in Montgomery, April 2002*
22. *On Software Testing, a series of invited presentations at Ankara University, Ankara and DEU, Izmir, July 2002.*
23. *On Algorithms, invited to be the Session Chair at MSE2002, Multimedia System Engineering, Newport Beach, Ca., December 2002.*
24. *On Software Management and NASA Statistics with John Peterson, NPR (National Public Radio) Interview with Carolyn Hutcheson, Feb.3, 2003.*
25. *On "An Exact Reliability Block Diagram Calculation Tool to design Very Complex Systems", Invited Honorary Speaker, 1stACIS International Conference on Software Engineering, Research and Applications (SERA'03), San Francisco, June 25-27, 2003.*
26. *On "The Future of Computer Software Systems" with Dr. Raymond Paul, DoD , NPR (National Public Radio) Interview with Carolyn Hutcheson, Feb. 2, 2004.* 27. *Keynote, IGS2004, International Statistics Days; Izmir-Turkey (May 2004)*
28. *On "The Evolution of the Reliability of Cyber-Systems" with Dr. C. V. Ramamoorthy, NPR*

(National Public Radio) Interview with Carolyn Hutcheson, Feb. 3, 2005.
29. *On "Security Aware Software", with Dr. A. Yasinsac, NPR (National Public Radio) Interview with Carolyn Hutcheson, Feb. 7, 2006.*
30. *On "Automating Software Evolution through Model-Driven Engineering", with Dr. J. Gray, NPR (National Public Radio) Interview with Carolyn Hutcheson, April 3, 2007.*
31. *On "Applications in Adversarial Risk Analysis", with Dr. D. Banks, NPR (National Public Radio) Interview with Carolyn Hutcheson, March 28, 2008.*
32. *Invited Keynote Speaker on"Availability Analysis in Components and Networks" during IGS04 held in Pine Bay resort in Kusadasi /Izmir/ Turkey, May 20-27, 2004.*
33. *Invited to Microsoft's HQ in Redmond Washington to attend "Trustworthy Computing Days" as one if its 14 global scholars, April 7-8, 2006.*
34. *Invited to present a Book-Tutorial on the J. Wiley "Trustworthy Computing" at IDPT-2006, San Diego, California, and June 23-29, 2006.*
35. *Invited keynote speaker by Yonsei University at the Korean Digital Society's Seminar (DII-06) on Security and Privacy, Seoul, S. Korea, Nov. 15, 2006.*
36. *Invited speaker at U-Mass in Amherst, MA on Security and Privacy, Dec. 8, 2006.*
37. *Invited speaker at UAB's CIS Dept. in Birmingham, AL on Security and Privacy, Dec. 1, 2006.*
38. *Invited distinguished speaker at IV International Conference on Systems Integration (ICSI'07) held in Brasilia, Brazil, 2-5 December 2007.*
39. *Invited Speaker to INTERFACE/SAMSI by Duke University, May 22-24, 2008.*
40. *Invited distinguished speaker at IV International Conference on Systems Integration (ICSI'08) held in Brasilia, Brazil, 9-11 November 2008.*
41. *Invited Discussant Speaker, Risk Section of the JSM (Joint Stat Meetings), Denver, CO; Aug. 3-8, 2008.*
42. *Invited Speaker, "Quantitative Risk Assessment of Software Security and Privacy, and Risk Management with Game Theory", CERIAS/Purdue University Annual Symposium Seminars, Feb 11, 2009.*
43. *Invited Discussion Paper Presenter on "Adversarial Risk Analysis, Influence Diagram, and Auctions" by Jesus Rios, David Rios and David Banks; "Adversarial Risk Analysis Counterterrorism" by David Banks and Bernard Harris; and "A Framework for Adversarial Risk Analysis" by Nozer D. Singpurwalla and Anna Gordon,* The 57th Session of the International *Statistical* Institute (ISI09): Adversarial Risk Analysis – IPM 95, Aug 20, 2009.

44. *Invited Speaker and Invited Session Organizer, Session Title: Statistical Risk Assessment of Trustworthy Computing, ISI Risk Meetings, Dublin-Ireland, August 2011.*

45. *M. Sahinoglu, "Cloud Meter, A Risk Assessment and Mitigation Tool," Cyber Security Training Conference (CSCT), Colorado Springs, August 1-2, 2012.*

46. *M. Sahinoglu, Kenneth Wool, "RISK ASSESSMENT AND MANAGEMENT TO ESTIMATE HOSPITAL CREDIBILITY SCORE OF PATIENT HEALTH CARE QUALITY," ISSA (Information Systems Security Association) Montgomery Chapter Monthly Meeting, Baptist Medical Center East, Monday, August 20, 2012 11:00 AM-11:30PM .*

47. *M. Sahinoglu, "QUANTITATIVE CYBER-SECURITY AND PRIVACY RISK ASSESSMENT FOR QUALITY IMPROVEMENT OF HEALTH CARE IT IN THE ALABAMA DEPARTMENT OF PUBLIC HEALTH JURISDICTION AREA," ISSA (Information Systems Security Association) Montgomery Chapter Monthly Meeting, Baptist Medical Center East, Monday, August 20, 2012 11:30 AM-12:00PM, Montgomery, AL.*

48. *M. Sahinoglu, "Cybersecurity Risk Preventions and Metrics- A Case Study for the Implementation of the Quantitative Security Risk Meter to Personal Computers", S. James High School, Montgomery Alabama, March 2013.*

49. *M. Sahinoglu, A seminar on the prospects of "Cyber-Risk Informatics: Metric-Based Evaluation in Cybersystems and Information Security, and Reliability Modeling, Textbook with NOVA Science Publishers' Contract signed Dec. 4, 2013, due March 2014 to be published in July 2014", UAB (University of Alabama at Birmingham), Electrical and Computer Engineering), January 22, 2013*

50. *M. Sahinoglu, Cyber-Risk Informatics, Summer School, Informatics Institute METU-Ankara-Turkey, Aug. 11-15, 2014*

REFEREED and PRESENTED CONFERENCE PROCEEDINGS

1. *M. Sahinoglu, Use of Markov Modeling and Statistical Data Analysis in Spare Plant Assessment-Its Economic Evaluation, Proceedings for the 7th Annual Reliability Conference on Reliability for Electric Power Industry, Madison, Wisconsin, USA, pp. 269-278, April 1980.*

2. *A. K Ayoub, M. Sahinoglu, A More Realistic Reliability Index for Generating Systems, Proceedings of Eleventh Annual Pittsburgh Conference on Modeling*

and Simulation, Pittsburgh, Pennsylvania, USA, Vol.11, Part 3, pp. 851-56, May 1-2, 1980.

3. *C.Singh, M. Sahinoglu, On Network Methods in Transmission and Distribution Networks, Proceedings of 8th Annual Reliability Conference on Reliability for Electric Power Industry, Portland, Oregon, USA, pp. 183-189, April 21-23, 1981.*

4. *M. Sahinoglu, Implementing the Triple Product Rule in the Numerical Integration of the Joint p.d.f. of three Random Variables in Computational Statistics, Proceedings of Numerical Analysis Symposium, pp. 226-239, METU, Ankara, December 23-25, 1983.*

5. *M. Sahinoglu, Analytical Reliability Evaluation Scheme in Large Power Systems - An Application to Turkish Interconnected System (1992), EP/SEM.12/R.12, Proceedings for the Seminar on Comparison of Models of Planning and Operating Electric Power Systems, Moscow, USSR, June 1987.*

6. *Engin Sungur, M. Sahinoglu, Handan Dingiloglu, Stochastic Modeling for Outage Processes, The First International Conference on Statistical Computing, p.594, ICOSCO-1 Proceedings Volume 1: Statistical Computation, Simulation and Modeling (Edited by E.J. Dudewicz), Cesme, Izmir, 30 March-2 April 1987.*

7. *M. Sahinoglu, D.Guven, E.Sungur, Comparison of Multivariate Exponential and Normal Distributions to Estimate the Reliability of Network, Proceedings Intern. AMSE Confer. Modeling & Simulation, Istanbul, AMSE Press, Vol.1C, pp. 211-224, June 29-July 1, 1988.*

8. *M. Sahinoglu, Setup Selcuk, Estimation of Power System Reliability Indices by Monte Carlo Simulation, Proceedings Intern. AMSE Confer. Modeling & Simulation, Istanbul, AMSE Press, Vol.1C, pp. 225-237, June 29-July 1, 1988.*

9. *M. Sahinoglu, Derya Guven, The Estimation of Operating Life of a Parallel-Dependent Computer Network, Proceedings of the Third International Symposium on Computer and Information Sciences, NOVA Press , pp. 527- 537, Cesme, Izmir - Turkey, Oct. 29-Nov.2, 1988.*

10. *M. Sahinoglu, Derya Guven, Reliability Estimation in K-out-of-N:G Network with Dependent Failures, Proceedings of the International Statistical Institute, 47th Session, Book 2, pp. 291-92, Paris-France, Aug 29- Sept 6, 1989.*

11. *M. Sahinoglu, Said Ebu Shaar, Ferda N. Civelek, A Statistical Expert System for Network Reliability Estimation, Proceedings of the International Statistical Institute, 47th Session, Book 2, pp. 293-94, Paris-France, Aug 29- Sept 6, 1989.*

12. *M. Sahinoglu, Geometric Poisson Density Estimation of the Number of Software Failures, IEEE Proceedings of the 28th Annual Reliability Spring Seminar of the Central New England Council (Reliability Trends: Calculation versus*

Application-Today and Tomorrow), The Boston Chapter Reliability Soc., pp. 149-174, April 1990.
13. *M. Sahinoglu, A Sequential Statistical Mutation- Based Testing Strategy, IEEE Proceedings of the 28th Annual Spring Reliability Seminar of the Central New England Council (Reliability Trends: Calculation versus Application-Today and Tomorrow), The Boston Chapter Reliability Soc., pp. 127-149, April 1990.*
14. *M. Sahinoglu, Derya Guven, Estimation of Total Operating Life in Shock Dependent Networks, Session 72, Joint Statistical Meetings of the American Statistical Association, Anaheim, California, USA, Aug. 6-9, 1990.*
15. *M. Sahinoglu, E. H. Spafford; A Bayes Sequential Statistical Procedure for Approving Software Products, Proceedings for the IFIP Conference on Approving Software Products (ASP-90), Garmisch-Partenkirchen, Germany, Sept.17-19, 1990.*
16. *M. Sahinoglu, Negative Binomial (Poisson Logarithmic) Density of the Software Failure Count, Proceedings of the Fifth International Symposium on Computer and Information Sciences (ISCIS V), pp. 231-39, Nevsehir-Cappadocia, Turkey, Oct 30 - Nov. 1, 1990.*
17. *P. Randolph, M. Sahinoglu, A Compound Poisson Bayesian Stopping Rule for Software Reliability, ASA Joint Stat Meetings, Atlanta, GA, USA, Session 183: Computer Packages, Aug. 21, 1991.*
18. *M. Sahinoglu, Sequential Statistical Procedures for Test-Case Adequacy in Software Testing, 1. State Institute of Statistics (DIE) Symposium, Ankara, Nov. 1991.*
19. *M. Sahinoglu, The Role of Statistics in Modern Positive Sciences and Development, MPM (National Productivity Center) Stat - OR and CS Applications, Ankara, pp. 1.1-1.9, 12-14 May, 1992.*
20. *M. Sahinoglu, The Analysis of Survival Data, MPM (National Productivity Center), Ankara; pp. 6.1-6.20, 12-14 May, 1992.*
21. *M. Sahinoglu, P. Randolph, An Optimal Stopping Rule for Software Reliability Testing, Proceedings of the Engineering Systems and Design Analysis (ESDA '92), Istanbul-Turkey, PD-Vol. 47-1, pp. 429-434, June 29-July 3 1992.*
22. *M. Sahinoglu, Derya Guven, Estimation of Total Good-Operating Life in k-out-of-N Parameter Dependent Networks, Proceedings of the Engineering Systems and Design Analysis (ESDA '92), PD-Vol.47-1, pp. 441-445, Istanbul, Turkey, June 29-July 3 1992.*
23. *M. Sahinoglu, Ibrahim Baltaci, E.H.Spafford, Monte Carlo Simulation on*

Software Mutation Test Case Adequacy, Proceedings of the 10th Symposium on Computational Statistics, COMPSTAT 1992, Neuchatel, Switzerland, Vol. 1, Physica-Verlag, pp. 47-52, Aug. 24-28, 1992.

24. *M. Sahinoglu, Unal Can, An Efficient Productive NLR Method for Reliability Modeling in Software Testing, Proceeding of the Second Bellcore/Purdue Symposium, pp. 29-38, Bellcore-Livingstone, N.J.,USA, Oct. 12-13, 1992.*

25. *M. Sahinoglu, The Energy Sector and Its Future, Turkiye Ekonomi Kurumu, pp. 89-106, 1992.*

26. *M. Sahinoglu, Neslihan Koc, Taguchi Squared-Loss Function vs. Absolute Loss Function (ALF) in Quality Control for Continuous and Discrete Variables, Proceedings of the 2nd Asian Congress on Quality and Reliability, pp. 436-439, Beijing-CHINA, May 31 - June 3, 1993.*

27. *M. Sahinoglu, Cihan Vural, Censored Data Analysis in Survival Studies for Quality Testing, 1. National Econometrics and Statistics Symposium, Izmir, 11-12 Nov. 1993.*

28. *Mehmet SAHINOGLU, Ibrahim Baltaci, Statistical Modeling and Parameter Estimation for the Reliability of Software Mutation Testing, 3. DIE Research Symp. Ankara. Nov. 22-24, 1993.*

29. *M. Sahinoglu, Cihan Vural, Censored Data Analysis for Exponentially Distributed Failure Data in Software Testing, Proc. of 7th Mediterranean Electrotechnical Conference (IEEE-MELECON '94), Session B22, Vol.1, pp. 371-74 Antalya, Turkey, April 1994.*

30. *M. Sahinoglu, Unal Can, A Software Reliability Model for Grouped Failure Data, Proc. of 7th Mediterranean Electrotechnical Conference (IEEE-MELECON '94), Session A32, Vol.1, pp. 149-152, Antalya, Turkey, April 1994.*

31. *Mehmet SAHINOGLU, CPMLE and CPNLR Models in Software Reliability Estimation, 4. DIE Research Symp. Ankara, Nov. 22-24, 1994.*

32. *M. Sahinoglu, Academic-Professional Training of Statisticians and Industry-University Relations, Invited Paper at III. Harma Meeting of Design of Experiments and Statistical Education, Proceedings of Design of Experiments and Statistical Education pp. 216-228, Cordoba-Spain, Dec. 17-18, 1994.*

33. *M. Sahinoglu, Editor, Proceedings of the 3. International Summer School on Model Choice and Design of Experiments (Lecture Notes), Izmir, Vol. I-II, Sept. 11-22, 1995.*

34. *M. Sahinoglu, S. Çapar, Statistical Performance Measures to Assess Forecast Quality of Parameter Estimation Methods for a Software Reliability Model,*

Proceedings of the 5th Annual Research Symposium, State Institute of Statistics, pp. 190-194, Ankara, Nov. 27-29, 1995.

35. *M. Sahinoglu, M. Gokmen, An Exact Compound Poisson (Poisson^LSD) Probability Distribution Function for Loss of Load in Electric Power Generation Reliability Evaluation, Proceedings of 6th Annual Research Symposium pp. 216-221, State Inst. of Stat., Ankara, Nov. 25-27, 1996.*

36. *M. Sahinoglu, S. Çapar, Stochastic Measures of Prediction Quality for Software Reliability Estimation Methods with Clustered Failure Data, Proceedings of 6th Annual Research Symposium, pp. 42-45, State Inst. of Stat., Ankara, Nov. 25-27, 1996.*

37. *M. Sahinoglu, A.Sattar Al-Khalidi, A Bayesian Stopping Rule for Negative Binomial Distribution, III. National Econometrics and Statistics Symposium, Uludag Univ., Uludag-Bursa, 29-30 May, 1997.*

38. *M. Sahinoglu, A. Sattar Al-Khalidi, A Bayesian Stochastic Stopping Rule for a Compound Poisson^LSD Distribution and Application to Software Testing, Istanbul, Turkey, ISBA Meeting - Satellite to ISI-97, Aug. 16-18, 1997.*

39. *M. Sahinoglu, Statistical Measures to Evaluate and Compare Predictive Quality of Software Reliability Estimation Methods, Invited Session No: 46, 51st Session of the International Stat. Inst., 18-26 Aug. 1997.*

40. *John Deely and M. Sahinoglu, Bayesian measures to compare predictive quality of software reliability estimation methods (1998), invited session on software reliability, International Conference on Reliability and Survival Analysis, NIU, DeKalb, IL, May 21-24, 1998.*

41. *John Deely and M. Sahinoglu, Bayesian Measures to Assess the Predictive Accuracy of Software Reliability Estimation Methods/Informative Priors (1998), Int. Symp. on Software Reliability Eng. (ISSRE'98), Paderborn, Germany, Nov. 1998.*

42. *M. Sahinoglu, A. von Mayrhauser, A. Hajjar, T. Chen, Ch. Anderson, On the Efficiency of a Compound Poisson Stopping Rule for Mixed Strategy Testing, IEEE Aerospace Conference, Colorado, March 1999.*

43. *M. Sahinoglu, Abdulsattar Al-Khalidi, A Stopping Rule for Time-Domain Software Testing, Proceedings of ISSRE99 (The 10th International Symposium on Software Reliability Engineering) pp. 11-12, Boca Raton, Florida, November 1-4, 1999.*

44. *M. Sahinoglu, A. von Mayrhauser, A. Hajjar, T. Chen, Ch. Anderson, How Much Testing is Enough? Applying Stopping Rules to Behavioral Model Testing, Proceedings of the 4th International Symposium on High-Assurance Systems*

Engineering (HASE1999) pp.249-256, Washington D.C., November 17-19, 1999.

45. *M. Sahinoglu, E. Chow, Empirical Bayesian Availability Index of Safety and Time Critical Software Systems with Corrective Maintenance, Proceedings of the 1999 Pacific Rim International Symposium on Dependable Computing (PRDC1999), Hong Kong, pp. 84-91, December 16-17, 1999.*

46. *Mehmet SAHINOGLU, A. von Mayrhauser, A. Hajjar, T. Chen, Ch. Anderson, Achieving the Quality of Verification for Behavioral Models with Minimum Effort, pp. 234-239, Proceedings of the 2000 IEEE 1st International Symposium on Quality Electronic Design (ISQED2000), San Jose, pp. 234-39, March 20-22, 2000.*

47. *M. Sahinoglu, 'How Can We Save More Time While testing Software for Better Products', TSUM Millennium's CIS Colloquium on Information Technology, Montgomery AL, April 24-25, 2000.*

48. *M. Sahinoglu, E. Chow, A New Availability Index of Safety and Time Critical Integrated Software Systems, Proceedings of the 2000 Integrated Design and Process Technology (IDPT2000), Dallas June 4-8, 2000.*

49. *M. Sahinoglu, Reliability Index Calculations of Integrated Software Systems (Internet) for Insufficient Failure and Recovery Data, The First Biennial International Conference on Advances in Information Systems, ADVIS'2000, Dokuz Eylul University, Dept. of Computer Engineering, Izmir-Turkey, Oct. 25-27, 2000.*

50. *C. Bayrak, M. Sahinoglu, Timothy Cummings; High Assurance Software testing in Business and DoD, Proceedings of the High Assurance Systems Engineering'2000 (HASE2000), Albuquerque, NM, pp. 207-211, Nov.15-17, 2000.*

51. *M. Sahinoglu, W.P. Munns, Availability Index Calculations in Integrated Software System with Emphasis on a Star Network Using Sahinoglu-Libby p.d.f., Proceedings of the 9th SCTF Meeting of IFIP, pp. 123-135, Florianopolis, Brazil, March 2001.*

52. *M. Sahinoglu, C. Bayrak, E. Orhun, D. Tyson, S. Westbrook; Some Quality Metrics in Internet-Based Distance Education, SDPS (Society of Design & Process Sciences)Workshop, Pasadena, CA, June 2003.*

53. *C. Bayrak, M. Sahinoglu, E. Orhun; "Global Learning Network: The Structure for Online Learning", Proceedings of the Integrated Design and Process Technology IDPT-**Vol** 1, pp. 35 – 43, 2002.*

54. *M. Sahinoglu, S. Glover, "A Cost-Benefit Analysis for Implementing and Efficient Stopping-Rule Algorithm in Software Coverage Testing". Proceedings*

ISQED 2002; San Jose, California; March 18 - 20, 2002.

55. *Jeffrey Bush, Bruce Jenkins, Steve Michaud, and M. Sahinoglu; "Applied Selective Quality for Increased Software Development Productivity", The Sixth World Conference on Integrated Design and Process Technology, Doubletree Hotel, Pasadena, California; June 23-28, 2002.*

56. *M. Sahinoglu, "Sahinoglu Reliability Model", The Sixth World Conference on Integrated Design and Process Technology, June 23-28, 2002, Doubletree Hotel, Pasadena, California.*

57. *Mehmet Sahinoglu, S. Glover, "A Cost Effective Testing Algorithm", The Sixth World Conference on Integrated Design and Process Technology Doubletree Hotel, Pasadena, California, June 23-28, 2002.*

58. *Mehmet Sahinoglu, " An Algorithmic JAVA Applet to Demonstrate the Merits of Stopping-Rule Algorithms in Software Testing", 2002 International MSE (Multimedia Software Engineering) Symposium, New Port Beach, California, Dec. 10-12, 2002.*

59. *M. Sahinoglu, "Security-Meter Design to Evaluate Computer Security", Proceedings of the Troy Business Symposium, Destin, FL, January 2003.*

60. *M. Sahinoglu, D. Libby, "Sahinoglu-Libby (SL) Probability Density Function – Component Reliability Applications in Integrated Networks," Proc. Ann. Reliability and Maintainability Symp., (RAMS03), Tampa, FL, pp.280-287, January 27-30, 2003.*

61. *M. Sahinoglu, J. Larson, B. Rice, "An Exact Reliability Calculation Tool to Improve Large Safety-Critical Computer Networks",* Proceedings DSN2003, IEEE Computer Society, *San Francisco, Cal.,* pp. B-38-39, *June 22-25, 2003.*

62. *M. Sahinoglu, "An Exact RBD Calculation Tool to Design Very Complex Systems", Invited Talk,* Proceedings of the 1st ACIS International Conference on Software Engineering Research and Applications, *San Francisco, Cal., June 25-27, 2003.*

63. *M. Sahinoglu, A. Smith, B. Dengiz; "Improved Network Design Method When Considering Reliability and Cost using an Exact Reliability Block Diagram Calculation (ERBDC) Tool in Complex Systems", ANNIE- Smart Engineering Systems,* Proceedings of the Intelligent Engineering Systems Through Artificial Neural Networks, *Vol. 13, pp. 849-855, St. Louis, Mo., Nov. 1-4, 2003.*

64. *S. R. Das, M. H. Assaf, E. M. Petriu, and M. Sahinoglu, "Aliasing Free Compaction in Testing Core-Based Systems-on-a-Chip Using Compatibility of Response Data Outputs"*, Proceedings of the 7th World Conference on Integrated Design and Process Technology, *Austin, TX, , Conference*

Proceedings, pp. 772-778, December 3-6, 2003.
65. *S. R. Das, M. H. Assaf, E. M. Petriu, D. Biswas, and M. Sahinoglu, "Systems on-Chip Test – Using Modified Cut-Sets of Response Data Outputs to Achieve Aliasing Free Compaction",* Proc. 6th Int. Conf. Information Technology, *Bhubaneswar, India, HWE005, Conf. Proc. pp.1-6, December 22-25, 2003.*
66. *M. Sahinoglu, C. V. Ramamoorthy, A.E. Smith, and B. Dengiz, "A Reliability Block Diagramming Tool to describe Networks," Proc. Ann. Reliability and Maintainability Symp., RAMS04, Los Angeles, CA, pp. 141-145, Jan. 26-29, 2004.*
67. *S. R. Das, M. H. Assaf, E. M. Petriu, L. Jin, C. Jin, D. Biswas, and M. Sahinoglu, "Testing Embedded Cores-Based System-on-a-Chip (SoC) – Test Architecture and Implementation"*, Proc. 23rd IASTED Int. Conf. Modeling, Identification, and Control, *Grunewald, Switzerland, 412- 807, pp.300-306, Feb. 23-25, 2004.*
68. *M. H. Assaf, S. R. Das, E. M. Petriu, and M. Sahinoglu, "Enhancing Testability in Architectural Design for the New Generation of Core-Based Embedded Systems"*, Proceedings of the 8th IEEE International Symposium on High Assurance Systems Engineering (HASE *), Tampa, FL, , pp.312-314, March 25-26, 2004.*
69. *S. R. Das, M. H. Assaf, E. M. Petriu, L. Jin, C. Jin, and M. Sahinoglu, "Implementation of an IP Core-Based Testing Environment", Proceedings of the IEEE Instrumentation and Measurement Technology Conference, Como, Italy, , Conf. Proc.* ***Vol*** *2, pp. 1503-1508, May 18-20, 2004.*
70. *M. H. Assaf, S. R. Das, E. M. Petriu, L. Jin, C. Jin, W. B. Jone, and M. Sahinoglu, "Hardware and Software Co-Design Verification in Space Compaction of Digital Circuits", Proceedings of the IEEE Instrumentation and Measurement Technology Conference, Como, Italy, , Conf. Proc.* ***Vol*** *3, pp. 2027-2030, May 18-20, 2004.*
71. *M. Sahinoglu, Keynote Speaker, "Notes on the Application of the SL: Sahinoglu-Libby Probability Distribution Function to Availability Analysis in Computer Components and Networks", Proceedings of STAT'04 (Stat-Days), Pine-Bay, Kusadasi, Izmir, May 20-24, 2004*
72. *S. R. Das, M. H. Assaf, E. M. Petriu, L. Jin, C. Jin, and M. Sahinoglu, "Test Implementation of Embedded Cores-Based Sequential Circuits Based on Verilog HDL Under Altera Max Plus II Development Environment," Proceedings of the 8th World Conference on Integrated Design and Process Technology, , Izmir-Turkey, pp.84-91, June 28- July 2, 2004.*

73. *M. Sahinoglu, " Security-Meter Model – A Simple Probabilistic Model to Quantify Risk," 55th Session of the International Statistical Institute (ISI), Sydney, Australia, Conference Proceedings, p. 163-168, April 2005.*
74. *S.R. Das, M. Sahinoglu, "Implementation of Embedded Cores-based Digital Devices in Jbits Java Simulation Environment", Proceedings for CIT 2004, LNCS 3356, pp. 315-325, Springer-Verlag, Berlin Heidelberg, Hyderabad, India, pp. 315-325, Eds: G. Das and V. P. Gulati, Dec 20-23, 2004.*
75. *Mansour H. Assaf, Rami S. Abielmona, Payam Abolghasem, Sunil R. Das, Emil M. Petriu, Voicu Groza, M. Sahinoglu, "Altera Max Plus II Development Environment in Fault Simulation and Test Implementation of Embedded Cores-Based Sequential Circuits", Proc. of CIT 2004, , Calcutta, India, pp. 352-359, Eds: A. Sen* et al., *Dec. 27-30, 2004.*
76. *J. Zakizadeh, S. R. Das, M. H. Assaf, E. M. Petriu, and M. Sahinoglu, "*Built-in self-test techniques for analog and mixed-signal circuits", *Presented at the IASTED International Conference on Modeling, Identification and Control, Innsbruck, Austria, Conference Proceedings, pp. 494-499, Feb. 16-18, 2005.*
77. *S. R. Das, J. Zakizadeh, M. H. Assaf, E. M. Petriu, and M. Sahinoglu, "* Testing analog and mixed-signal circuits with built-in hardware – new approach", *22nd IEEE Instrumentation and Measurement Technology Conference, Ottawa, Ontario, Canada, Conference Proceedings, Vol. I, pp. 166-171, May 16-19, 2005.*
78. *S. R. Das, D. Biswas, M. H. Assaf, E. M. Petriu, and M. Sahinoglu, "*Developing test environment for embedded cores-based system-on-a-chip (SOC)", *22nd IEEE Instrumentation and Measurement Technology Conference, Ottawa, Ontario, Canada, , Conference Proceedings,* ***Vol****. I, pp. 172-177, May 16-19, 2005.*
79. *S. R. Das, J. Zakizadeh, M. H. Assaf, E. M. Petriu, and* M. Sahinoglu*, "*Test Methodology for embedded system-on-chip (SOC) with mixed-signal and analog cores", *International Symposium on Integrated Design and Process Technology, Beijing, China, Conference Proceedings, Vol. I, pp. 245-251, June 13-17, 2005.*
80. *M. Sahinoglu, "Quantitative Risk Assessment for Software Maintenance with Bayesian Principles", ICSM 2005 (International Conference on Software Maintenance), Budapest, Hungary, ICSM Proceedings, pp. 67-70, 26-29 September, 2005*
81. *S. R. Das, J. Zakizadeh, M. H. Assaf, E. M. Petriu, and M. Sahinoglu,"* System-on-chip (SOC) test with mixed-signal and analog cores", *Presented at the 8th International Conference on Information Technology, Bhubaneswar, India, Conference Proceedings, pp.283-288, December 20-23, 2005.*

82. *M. Sahinoglu, "Quantitative Risk Assessment for Dependent Vulnerabilities", The International Symposium on Product Quality and Reliability (52^{nd} Year), pp. 345-350, New Port Beach, CA, Jan. 23-26, 2006.*
83. *S. R. Das, D. Biswas, E. M. Petriu, M. H. Assaf, and M. Sahinoglu:* Test environment for embedded cores-based system-on-chip (SOC) – development and methodologies*, Presented at the IASTED International Conference on Modeling, Identification and Control, Lanzarote, Canary Islands, Spain, Conference Proc., pp.343-348, February 6-8, 2006.*
84. *S. R. Das, A. Hossain, M. H. Assaf, E. M. Petriu, M. Sahinoglu, and W. – B. Jone, "* On a new graph theory approach to designing zero-aliasing space compressors for built-in self-testing", *Presented at the 23^{rd} IEEE Instrumentation and Measurement Technology Conference, Sorrento, Italy, Conference Proceedings, pp. 1890-1895, April 24-27, 2006.* 85. S. R. Das, S. Mukherjee, E. M. Petriu, M. H. Assaf, M. Sahinoglu, and W.– B. Jone, "An Improved Fault Simulation Approach Based on Verilog with Application to ISCAS Benchmark Circuits", *Presented at the 23^{rd} IEEE Instrumentation and Measurement Technology Conference, Sorrento, Italy, Conference Proceedings, pp. 1902-1907, April 24-27, 2006.*
86. *S. R. Das, A. Hossain, E. M. Petriu, M. H. Assaf, M. Sahinoglu, W. –B. Jone, and S. Biswas, "*A new graph theory technique to design zero-aliasing space compressors", *Presented at the 9^{th} World Conference on Integrated Design and Process Technology, San Diego, CA, Conference Proceedings, pp. 331-338. June 25-30, 2006.*
87. *M. Sahinoglu, "A Universal Quantitative Risk Assessment Design to Manage and Mitigate", Proceedings (in Power Point) of International Conference on the Digital Information Industry, pp. 333-405, Seoul, Korea, November 14-15, 2006.*
88. *S. R. Das, A. Hossain, A. R. Nayak, E. M. Petriu, S. Biswas, and M.Sahinoglu, "*Designing zero-aliasing space compressors – graph theory approach", *Presented at the 26^{th} IASTED International Conference on Modeling, Identification and Control, Innsbruck, Austria, Conference Proceedings, pp. 326-331, February 12-14, 2007.*
89. *A. Hossain, S. R. Das, A. R. Nayak, E. M. Petriu, S. Biswas, and M. Sahinoglu, "*Further studies on zero-aliasing space compression based on graph theory", *Presented at the 24th IEEE Instrumentation and Measurement Technology Conference, Warsaw, Poland, Conference Proceedings, pp.1-6, May 1-3, 2007.*
90. *M. H. Assaf, S. R. Das, W. Hermas, S. Biswas, E. M. Petriu, W–B. Jone, and M. Sahinoglu:* Complex ASIC core design using coverage-driven functional verification and reuse methodology*, Presented at the 10^{th} World Conference on Integrated Design and Process Technology, Antalya, Turkey, Conference*

Proceedings, pp. 294-301, June 3-8, 2007.
91. *M. Sahinoglu, B. Rice, D. Tyson, "Comparison of Simulation and Analytical Methods to Compute Source-Target Reliability in Very Large Complex Networks", Proceedings of the YA/EM (Operations Research / Industrial Engineering Conference, Izmir, Turkey, pp. 1096-1102 (D:\kitap.pdf) July 2007.*
92. *M. Sahinoglu, "Statistical Inference to Quantify and Manage Risk of Privacy," Proceedings of the 56th Session of the International Statistical Institute (ISI), Session 22 (S80: Risk), Lisbon, Portugal; ISI Book of Abstracts, p. 506. August 2007.*
93. *M. Sahinoglu, "A Measurable Design for the Security Model to Quantify and Manage Software Security and Privacy Risk", Distinguished Speaker, Proceedings of the IV. International Conference on Systems Integration (ICSI07), Brasilia, Brazil, 2-5 December, 2007.*
94. *M. Sahinoglu, "A Measurable Design for the Security Model to Quantify and Manage Software Security and Privacy Risk", Invited Speaker, Universiadade de Brasilia, Instituto de Ciencias Exatas, Departmento de Ciencia da Computacao, Brasila, Brasil- Brazil, 7 December, 2007.*
95. *M. Sahinoglu, "Generalized Game Theory Applications to Computer Security Risk", Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May 18-21, 2008.*
96. *M. Sahinoglu, "Game Theory Applications to Security-Meter Design to Quantify/Manage Security Risk," (Invited Speaker) Proceedings of Interface/SAMSI Risk Conference, May 22-24, 2008 Duke University, Durham, N. Carolina.*
97. *S. R. Das, Jun-Geng Li, A. Hossain, A. R. Nayak, E. M. Petriu, S. N. Biswas, M. A. Assaf, W-B Jone, and M. Sahinoglu,"Testing Cores-Based System-on-Chips Using ModelSim Verification Tool, Integrated Design and Process Technology", IDPT Conference Proceedings pp.111-118, Taiwan, June 2008.*
98. *M. Sahinoglu, "Discussion Topics on Environmental Risk: Risk Assessment and Dose-Response Models", Discussant, Session 180, JSM (Joint Statistical Meetings), Denver, CO, August 2008.*
99. *M. Sahinoglu, D. Banks, Yanling Yuan, " Statistical Inference on the Residual Risk Metric of the Quantitative Security-Meter Model", Accepted for presentation on 8/5/2009 at the Invited Session #204120: Quantitative Security and Cybersytems, JSM, Washington DC, August 2009.*
100. *M. Sahinoglu, Luis Cueva-Parra, D. Tyson, S. Das, "Statistical Inference and Simulation on Security Metrics in Cloud Computing for Large Cybersystems", Accepted for presentation on 8/5/2009 at the Invited Session #204120:*

Quantitative Security and Cybersytems, JSM, DC, August 2009.
101. *M. Sahinoglu, S. Simmons, J. Matis, "Determining an Efficient Stopping Rule for the Security testing of Cyber Attacks in Computer and Communication Networks" Accepted for presentation on 8/5/2009 at the Invited Session #204120: Quantitative Security and Cybersytems, JSM, Washington, DC, August 2009.*
102. *M. Sahinoglu, Invited Discussion Paper on "Adversarial Risk Analysis, Influence Diagram, and Auctions" by Jesus Rios, David Rios and David Banks; "Adversarial Risk Analysis Counterterrorism" by David Banks and Bernard Harris; and "A Framework for Adversarial Risk Analysis" by Nozer D. Singpurwalla and Anna Gordon,* The 57th Session of the International *Statistical* Institute (ISI09): Adversarial Risk Analysis – IPM 95 Thurs. Aug 20, 2009.
103. *M. Sahinoglu, Lynn Dennard, S. Morton, "Quantitative Ecological Risk Assessment and Risk Management", SEC-19, Air Force Information Technology Conference (AFITC'09), Abstract Book p.56, August 24, 2009.*
104. *M. Sahinoglu, S. Ganguly, S. Morton, "A Quantitative Index for Software Usability in Trustworthy Computing", Proc. Integrated Systems, Design and Process Science, 12th SDPS Transdisciplinary Workshop-Conference, Montgomery, AL, November 1-5, 2009.*
105. *M. H. Assaf, L.A. Moore, S. Das, S.N. Biswas and M. Sahinoglu, "Low-Level Fault Testing ASIC Simulation Environment", Proc. Integrated Systems, Design and Process Science, 12th SDPS Transdisciplinary Workshop-Conference, Montgomery, AL, November 1-5, 2009.*
106. *R. M. Barclay and M. Sahinoglu, " The Computer User-The IT Security's Weakest Link", Proc. Integrated Systems, Design and Process Science, 12th SDPS Transdisciplinary Workshop-Conference, Montgomery, AL, November 1-5, 2009.*
107. *Luis A. Cueva-Parra and M. Sahinoglu. "Security Metrics on Cloud Computing using Statistical Simulation and Markov Process," Proc. Integrated Systems, Design and Process Science, 12th SDPS Transdisciplinary Workshop-Conference, Montgomery, AL, November 1-5, 2009.*
108. *M. Sahinoglu, "Five Themes of the Quantitative Security-Meter Software", Tutorial-Demo, SDPS/AUM Workshop Conference, 1:30-2:15 pm, Montgomery, AL, Wednesday Nov. 4, 2009.*
109. *M. Sahinoglu, David Ang, Luis Cueva-Parra, Serajul Bhuiyan, Tom Lucy-Bouler, Judy Kamnikar, Robert Underwood, Bob Gehling, " Workshop IV: Transdiscipline: Integrating Arts and Sciences, Engineering, and Business Principles", SDPS/AUM Workshop Conference, Montgomery, AL, Nov. 4, 2009.*

110. *M. Sahinoglu, "Multivariate Statistical Modeling on the 3-State (Up, Derated, Down) Availability of a Repairable Component with the Sahinoglu- Libby (SL) Probability Distribution using Monte Carlo Simulation," AU-AUM Mathematics and Statistics Colloquia, Faculty Host: Nedret Billor; Monthly Seminar, Auburn University, http://www.amth.auburn.edu/colloquia/index.htm; April 2, 2010.*
111. *M. Sahinoglu, Yan Ling Yuan, "Multivariate Statistical Modeling on the 3-State (up, Derated, Down) Availability of a Repairable Component with the Sahinoglu-Libby Probability Distribution using Monte Carlo Simulation", Grand Challenges Multiconference Simulation (GCMS'10) and SummerSim, Ottawa, Canada, July 11-14, 2010.*
112. *M. Sahinoglu, "The Applications of the Quantitative Security-Meter Algorithm to Health-Care Cyber Security and Others", Tutorial-Demo, SDPS 2010, June 6-11, 2010, Dallas, TX.*
113. *M. Sahinoglu, "New Method for Cyber-Security Risk Assessment and Cost-Efficient Management in Wireless Sensor Networks", Proceedings of Cyberspace Research Workshop, http://csc.latech.edu/crw10/proceedings.pdf, pp. 8-12, Shreveport, LA; Nov. 15-17, 2010.Nov. 15-17, 2010.*
114. *M. Sahinoglu, " How to Apply Game Theory to Computer Security Risk Assessment", Invited Speaker, SAMSI Symposium, Proceedings of Interface /SAMSI Risk Conference, SAS Institute, Cary , N. Carolina, June 1-3, 2011.*
115. *Aysen Dener Akkaya, Mehmet Sahinoglu, Scott Morton, Vir Phoha, "A Quantitative Security and Privacy Risk Assessment and Management Method for Social Networks," IPS018 (Invited Session on Trustworthy Computing), ISI 2011, Dublin, Ireland, August 22-26, 2011.*
116. *Mehmet Sahinoglu, Sedat Capar, YanLing Yuan, "Statistical Inference on the Two- and Three-State Availability of Repairable Units with the Sahinoglu-Libby Model," IPS018 (Invited Session on Trustworthy Computing), ISI 2011, Dublin, Ireland, August 22-26, 2011.*
117. *Susan J. Simmons, Mehmet Sahinoglu, James H. Matis, "Efficient Stopping Rules for Quantitative Security Testing of Cyber-Attacks," IPS018 (Invited Session on Trustworthy Computing), ISI 2011, Dublin, Ireland, August 22-26, 2011.*
118. *M. Sahinoglu, "National Cyber-Security Risk Assessment and Management," AFITC (Air Force Information Technology Conference), Montgomery, AL, August 2010; Eisenhower Series Invited Speaker, Air War College, Maxwell AFB, Montgomery AL, April 2011.*
119. *D. Ang, M. Sahinoglu," Achieving Educational Learning Objectives through Innovative Production Management System", International Conference on Business and Information (BAI2012), Sapporo-Japan, , Proceedings of Business and Information, http://bai-conference.org, Volume 9, Issue 1, 2012, ISSN 1729-*

9322, July 3-5, 2012.
120. *S.Das, M. Assaf, D, Shaw, S. Biswas, S. Morton, M. Sahinoglu,"Atalanta and FSIM Simulation in Response Data Compaction of Multi-Output Digital Circuits with Array of Two-Input" , Conference of Society of Design and Process Science(SDPS), Session X1 Cloud Computing: Security and Reliability, Berlin, Germany, 1:30-3:15pm, 13 June 2012.*
121. *M. Sahinoglu, Scott Morton, "Cloud Risk-O-Meter: An Algorithm for Cloud Risk Assessment and Management," Conference of Society of Design and Process Science (SDPS), Session X1 Cloud Computing: Security and Reliability, 1:30-3:15pm, Berlin, Germany, 13 June 2012.*
122. *Dan Marghitu, M. Sahinoglu, "Computing Reliability in a Complex Electric Power Generation Grid using the Analytical Overlap and CLOUD Simulation Techniques for Directional and Non-directional System Topologies," Conference of Society of Design and Process Science (SDPS), Session X1 Cloud Computing: Security and Reliability, Berlin, Germany, 1:30-3:15pm,13 June 2012.*
123. *Luis Cueva-Parra, M. Sahinoglu, Susan Simmons, "Reliability Testing before Releasing CLOUD using a sequential Stopping Rule with Logistic-Growth Compound Poisson Modeling", Conference of Society of Design and Process Science(SDPS), Session X1 Cloud Computing: Security and Reliability, Berlin, Germany, 1:30-3:15pm,13 June 2012*
124. *S. Das, M. Assaf, S. Biswas, M. Sahinoglu, "Session Initiation Protocol in Multimedia Communications- Server Performance by Software Profiling" , Conference of Society of Design and Process Science(SDPS), Session XV1 Innovative Approaches in Radio Frequency Engineering Applications, Berlin, Germany 3:45-5:30pm,13 June 2012.*
125. *M. Sahinoglu, "Cloud Meter, A Risk Assessment and Mitigation Tool", Cyber Security Training Conference (CSCT), Colorado Springs, August 1-2, 2012.*
126. *David Ang, Dave Jahadanga, M. Sahinoglu, "Organizational Competitive Principles in Cellular Manufacturing",* Proc. of International Conf. on Business and Information, **Vol** 10, Issue 1, 2013, ISSN: 1729-9322, http:/ibac-conference.org, *(pp. F235-F239). Bali, Indonesia: Academy of Taiwan Information Systems Research,* July 07-09. *2013.*
127. *M. Sahinoglu, S. Morton, "An Automated Algorithm to Assess and Manage Ecological Risk", http://www.aum.edu/docs/default-source/news-and-headlines/sahinogluicoest2013fullpaper.pdf?sfvrsn=2. Presented at ICOEST'2013, Urgup-Turkey, June 18-21, 2013. http://icoest.org/arsiv/files/Conference-Programme.pdf*   128. *Sahinoglu, M.; Stockton, S.; Morton, S.; Eryilmaz, M., Metrics to Assess and Manage Software Application Security Risk, Conference Proceedings, SAM'14, Las Vegas July 20.*

129. *Sahinoglu, M.; Stockton, S.; Morton, S.; Barclay, R.; Eryilmaz, M., ASSESSING DIGITAL FORENSICS RISK: A METRIC SURVEY APPROACH, SDPS Conference Proc. (Theme: Smart Innovative Societies), Sarawak, Malaysia , 15-19 June 2014, http://www.swinburne.edu.my/sdps2014/*

TECHNICAL REPORTS and DISSERTATIONS

NOTE: All technical reports if so after 1990 have been listed under the Grants & Projects thereafter.

1. *Mehmet SAHINOGLU*, Use of Markov Modeling in Power System Reliability Studies, *Master of Science Dissertation, University of Manchester Institute of Science and Technology, Manchester, England, October 1975.*
2. *Mehmet SAHINOGLU*, Statistical Inference on Reliability Performance Index for Electric Power Generation Systems, *Ph.D. Dissertation (Doctor of Philosophy), The Institute of Statistics, College of Science, Texas A&M University, College Station, 77843, Texas, USA, December 11, 1981.*
3. *Mehmet SAHINOGLU, Reliability Study-Spare Plant Assessment, TEK Planlama ve Koordinasyon Dairesi, Pub. No:22, May 1976.*
4. *Mehmet SAHINOGLU, Basic Reliability Study in Electric Power Systems, TEK Planlama ve Koordinasyon Dairesi, Pub. No:23, June 1976.*
5. *Mehmet SAHINOGLU, Reliability Evaluation Studies in 380 kv. Transmission System, TEK Planlama ve Koordinasyon Dairesi, Pub.No:24, July 1976.*
6. *Mehmet SAHINOGLU, Application of Markov Modeling in Electric Power System Reliability Evaluation and Statistical Data Analysis, Applied Statistics Dept., M.E.T.U. Working Paper No:2, Third National Operations Research Conference, Izmir, Turkey, May 1977.*
7. *A.D.Patton, A.K.Ayoub, Associated Power Analysts Inc.; C. Singh, G. L. Hogg (main authors), M. Sahinoglu, P .Resto, S. Asgarpoor (programmers), Texas A&M University; J.H. Blackstone, Auburn University; Modeling of Unit Operating Considerations in Generating Capacity Reliability Evaluation, Vol.1 : Mathematical Models, Computing Methods and Results, Vol.2 : Computer Program Documentation, EPRI EL.2519 Project 1534-1 Final Report, July 1982.*
8. *Mehmet SAHINOGLU, On the Power System Reliability Evaluation and*

Reliability Statistics), TMMOB Elektrik Muh. Dergisi, Ankara, April 1983.

9. *Mehmet SAHINOGLU, Balkan Interconnected Power System Reliability and Statistical Data Analysis, Ad-Hoc Meeting of Experts on Power System Planning Strategy, Istanbul-Turkey, May 1983.*

10. *Mehmet SAHINOGLU, Balkan Interconnected Power System Reliability and Statistical Data Analysis, Ad-Hoc Meeting of Experts on Power System Planning Strategy, Athens-Greece, October 10-11, 1983.*

11. *Mehmet SAHINOGLU, Omer Gebizlioglu, Balkan Interconnected Power System Reliability Evaluation and Statistical Data Analysis, Department of Statistics-M.E.T.U. & Planning Coordination Dept - Turkish Electricity Authority (TEK), Ankara, June 1984; Selected ECE Document Published in the Field of Energy in 1985/86 EP/GE/2/R.70/Add.1; E.C.E., Comm. on Electric Power, Group of Experts on Problems of Planning, 16th Session, Geneva, Switzerland, 4-6 June 1984.*

12. *Mehmet SAHINOGLU, Balkan Interconnected Power System Reliability and Statistical Data Analysis, Ad-Hoc Meeting of Experts on Power System Planning Strategy, Poiana Brasov-Romania, November 12-14, 1984.*

13. *Mehmet SAHINOGLU, Problems of Planning and Operating Large Power Systems, Economic Commission of Europe, Committee on Electric Power, 43rd Session, Geneva, Switzerland, 14-18 Jan. 1985.*

14. *Mehmet SAHINOGLU, Balkan Interconnected Power System Reliability Evaluation (1990), Project 06.3.1.3. - EP/GE.2/ R.70/Addenda 1., Economic Commission of Europe, Group of Experts Meeting, Committee on Electric Power, 17th Session Geneva, Switzerland, 1-3 April 1985.*

15. *Mehmet SAHINOGLU, Balkan Interconnected Power System Reliability Evaluation for the Planning Year 1990 and Statistical Analysis-Final Report, Dept of Statistics M.E.T.U. & Planning Coordination Department - T.E.K., Ankara, July 1985 presented at the Ad-Hoc Meeting of Experts on Power System Planning Strategy, XIVth Session of the Coordinating Committee of the Interconnection of the Electric Power Transmission Systems of the Balkan Countries in Istanbul; Nov.26-29, 1985.*

16. *Mehmet SAHINOGLU, Balkan Interconnected Power System Reliability Evaluation (1990), Project 06.3.1.3. - EP/GE.2 /R.70/Addenda 2., Economic Commission of Europe, Comm. on Electric Power, 18th Session, Geneva, Switzerland, May 28-30, 1986.*

17. *Mehmet SAHINOGLU, The Evaluation of Reliability Indices for the Off-Site Electric Power System at the Akkuyu Nuclear Power Plant for the*

Assessment and Planning of On-Site Plant Reliability, Progress Report, July 1986.
18. Mehmet SAHINOGLU, Global Benefits of Interconnection Among Balkan Power Systems (1990) - Economic Operation of International Interconnections, Coordinating Committee for the Development of Interconnection of the Electric Power Systems of the Balkan countries, Novisad-Yugoslavia April 7-10, 1987.
19. Mehmet SAHINOGLU, Report of the Seminar on Comparison of Models of Planning and Operating Electric Power Systems, Moscow-Rapporteurship Duty by the Government of Turkey, Presented to ECE (Economic Commission of Europe), Committee on Electric Power-Secr., Geneva, Switzerland, Dec 1986.
20. Mehmet SAHINOGLU, Statistical Chaos and Remedies, Gunes Gazetesi (Daily Newspaper SUN), 15 Sept. 1987.
21. Mehmet SAHINOGLU, The Evaluation of Reliability Indices for the Off-Site Electric Power System at the Akkuyu Nuclear Power Plant for the Assessment and Planning of On-Site Plant Reliability Ankara, Final Report, Oct.1987.
22. Mehmet SAHINOGLU, Global Benefits of Interconnection among Balkan Power Systems (1990), Final Report, Coor. Co. for the Interconnection of the Electric Power Systems of the Balkan countries ,Geneva-Switzerland, Jan. 1988, U.N. Economic and Social Council, Econ. Comm. for Europe, Comm. on Electric Power, Meeting of Experts on Problems of Planning and Operating Large Power Systems, Proj. No. EP/GE.2/R.70 /Add.3 /Rev.1 by Govt of Turkey, March 1988.
23. Mehmet SAHINOGLU, Avrupa Enerji Konferansi ve Enerji Planlamasinda Istatistik Disiplini, (Moscow/USSR- European Conference on Energy and Statistics Discipline in Energy Planning), E.M.O Monthly (Chamber of Electrical Engineers), Ankara, Turkey, April1988.
24. W.Hsu, Mehmet SAHINOGLU, E.H. Spafford, An Experimental Approach to Statistical Mutation-Based Testing, Technical Report, SERC-TR 63, SERC, Dept. of Comp. Sciences, Purdue Univ., Feb. 1990.
25. Mehmet SAHINOGLU, Compound Poisson Density Estimation of the Number of Software Failures, Proceedings of the Software Reliability Symposium-Proc. of Kick Off Meeting, Tech. Comm. on Software Rel. Eng. & Subcomm. on Software Rel. Eng., Washington D.C., April 1990.
26. Mehmet SAHINOGLU, E.H. Spafford, Sequential Statistical Procedures for Approving Test Sets Using Mutation-Based Software Testing, SERC-

TR 79-P, SERC, Dept. of Computer Sciences, Purdue Univ., Feb 1990.

INDUSTRIAL PROJECTS & GRANTS

1) Project Code	82-06-04-01
Project Name	*Akkuyu Nuclear Power Plant Off-Site Reliability & Evaluation for the Security of the On-Site System Operation*
Supported By	*Turkish Electricity Authorities (TEK) Nuclear Management*
Project Grant	*36.000.000 TL (US$60000) (US$=600 TL in 1986 Sept.)*
University Allotment	*14.500.000 TL*
Project Duration	*Jan.1, 1986-Dec.31, 1986*

2) Project Code	84-01-06-01
Project Name	*Balkan Power Systems Interconnection Reliability & Evaluation with Respect to Optimization of Short-Long Term Planning-Alternatives and Statistical Data Analysis*
Supported By	*Turkish Electricity Authorities (TEK)- Planning and Research*
Project Grant	*45.454.545 TL (US$65000) (US$=700 TL in 1986 Sept.)*
University Allotment	*18.181.818 TL*
Project Duration	*Sept.30, 1986-Dec.1, 1987*

3) Project Code	82-06-04-01
Project Name	*Balkan Power Systems Interconnection & Reliability Evaluation and Statistical Data Analysis*
Supported By	*Turkish Electricity Authorities (TEK) Planning and Research*
Project Grant	*4.950.000 TL (US$16500) (US$ = 300 Turkish Lira TL in 1982 Dec.)*
Project Duration	*Jan.1, 1983-June 30, 1984*

4) Project Code	84-01-06-01
Project Name	*Balkan Power Systems Interconnection Reliability & Evaluation with Respect to Optimization of Short-Long Term Planning-Alternatives and Statistical Data Analysis*
Supported By	*Turkish Electricity Authorities (TEK)- Planning and Research*
Project Grant	*6.000.000 TL (US$17000) (US$=350 TL in 1984 June)*
University Allotment	*2.004.00 TL*
Project Duration	*June 30, 1984-Sept. 30, 1985*

5)Project Code	85-01-09-01

Project Name	*Balkan Power Systems Interconnection Reliability & Evaluation*
Supported By	*Turkish Electricity Authorities (TEK) Planning and Research*
Project Grant	*8.500.000 TL (US$17000) (US$=500 TL in 1985 June)*
University Allotment	*4.224.000 TL*
Project Duration	*Sept.30, 1985-May 30, 1986*

6)Project Code	*87-01-09-01*
Project Name	*The Refereeing and Rapporteurship Service for the European Economic Commission-Committee on Electric Power Conference on The Planning and Modeling of Large Systems held in Moscow, USSR, June 1987 and Balkan Global Interconnected System Reliability Evaluation*
Supported By	*Turkish Electricity Authorities (TEK) Planning and Research*
Project Grant	*50.000.000 TL (US$65000) (US$=770 TL in 1987 June)*
University Allotment	*20.000.000 TL*
Project Duration	*June 1, 1987-May 31, 1988*
Research Donor	*Fulbright Research Scholarship, USA*
Project Grant	*$18700 during August 1989-1990*
Research Topic	*Software Reliability Evaluation and Automated Mutation Testing*

7)Project Code	*90-01-09-03; 91-01-09-01; 91-01-09-02 (Three projects)*
Project Name	*TAFICS (Turkish Armed Forces Integrated Communication Network) To Write Software Reliability and Security Specs*
Supported By	*Undersecretary for National Defense (Savunma Sanayii)*
Project Grant	*120.000.000 TL (US$20000) (U$=6000 TL average)*
University Allotment	*60.000.000 TL*
Project Duration	*Sept. 1990-March 1992*

8)Project Code	*92-01-09-01*
Project Name	*Statistical Re-organization and Reliability Studies in TEK*
Supported By	*Turkish Electricity Authorities (under General Director)*
Project Grant	*134.000.000TL (US$20000) (US$=7000 TL average)*
University Allotment	*60.000.000 TL*
Project Duration	*May 1, 1992-1993*

9)Project Code	*TUBITAK (NSF/Turkey)*
Project Name	*Automated Software Testing & Implementation to Turkish Industry*
Supported By	*TUBITAK (Ankara Blv. No:224; Kavaklidere)*
Project Grant	*180.000.000TL (US$18000) (US$=10000TL average)*

Equipment	*Capital Costs:100.000.000 TL*
Project Duration	*Aug. 1992- November 1994*

10)Project Code	DEVAK-93-01
Project Name	*Statistical Re-organization and Reliability Studies in TEK*
Supported By	*Turkish Electricity Authorities (under General Director)*
Project Grant	*199.000.000TL (US$22110) (US$=9000TL)*
University Allotment	*40.000.000 TL*
Project Duration	*May 1, 1993-94*

11)Project Code	DEVAK-94-01
Project Name	*Statistical Re-organization and Reliability Studies in TEK*
Supported By	*Turkish Electricity Authorities (under General Director)*
Project Grant	*500.000.000TL (US$16660) (US$=30000TL)*
University Allotment	*100.000.000 TL*
Project Duration	*May 1, 1994-95*

12)Project Code	DEVAK-95-01
Project Name	*Evaluation of Reliability Indices in Turkish Interconnected Power Generation System for Capacity Planning (1995-2000)*
Supported By	*Turkish Electricity Authorities Generation & Transmission (TEAS)*
Project Grant	*1.700.000.000. TL (US$34000) (US$=50000TL)*
University Allotment	*340.000.000 TL*
Project Duration	*Dec. 1, 1995- May 1, 1997*

13)Project Donor	TUBITAK NATO B2
Project Name	*New Statistical Measures for Assessing and Comparing the Predictive Accuracy of Software Reliability Estimation Methods*
Supported By	*Turkish Scientific Technical and Research Council*
Project Grant	*2.200.000.000 TL (US$11000) (US$=200.000TL)*
Project Duration	*Aug.'97 - June'99 (Executed at Purdue and Case Western Reserve Universities)*

14)Project Donor	Software and System Reliability Measurement in Integrated Networks
Supported By	*Troy State University Montgomery Eminent Scholar Research Funds (ACHE: Alabama Commission on Higher Education)*
Project Grant	*Annually: $20,000 (Prog. Personnel), $10,000 (Equipment-Software), $7,000 (Travel)*
Project Duration	*Sept. 1999 - Aug. 2008*

15)Project Donor	Microsoft TWC Curriculum (See the hyperlink www.areslimited.com for Final Report)

Project Name	*Trustworthy Computing Curriculum*
Supported By	*Microsoft Academic Alliance on TWC*
Project Grant	*Annually: $50,000*
Project Duration	*Jan 2006 - Jan 2007*
16)Project Donor	*ICS (Integrated Computer Solutions)*
Project Name	*Cybersecurity Lab*
Supported By	*ICS, Montgomery AL*
Project Grant	*One time equipment donation $85,000 upon request*
Project Duration	*2010-*

17)Project Donor	*National Science Foundation pending 08/15/13 proposal*
Project Name	Expanding Alabama's Research Capacity in Cyber Security and Cyber Response (AUM under Informatics Institute will be responsible for participating on the following tasks: Industrial Control Cyber Physical Systems Security, Trustworthy Infrastructure in Cloud Environments, Modeling and Simulation)
Supported By	*EPSCOR Research Infrastructure Improvement Program Track-1; (RII Track-1); Program Solicitation NSF 13-549 (pending)*
Project Grant	*Total Consortium for all participating Universities (Auburn, Tuskegee, UAB, UAH, USA, A A&M, UA and other AL Col/Univ) in AL : $4,000,000 with Auburn & AUM: $627,000*
Project Duration	*2013-2018*

18)Project Donor	*Office of Naval Research (ONR) (pending –to be soon submitted)*
Project Name	*"Information Assurance of Cyber-Physical Systems with Internal Self-Manageable Security Risk Assessment Clock - An Automated Software for Cybersystems Ubiquitous Third Wave-Computing"*
Supported By	*Long Range Broad Agency Announcement (BAA) for Navy and Marine Corps Science and Technology 13-001 (pending)*
Project Grant	*http://www.onr.navy.mil/Science-Technology/Departments/Code-31/All-Programs/311-Mathematics-Computers-Research/Software-Computing-Systems.aspx*
Project Duration	*2013-2016*

19)Project Donor	*Gulf of Mexico Research Initiative (GoMRI) (pending 12/15/13 preproposal)*
Project Name	*GoMRI Research Themes.(Theme IV)* Title Pending: Preventing Oil Spills: Risk Assessment, Detection and Mitigation with Sensor Networks (pending with Profs Iyengar/FIU School of Computing and Marghitu/Auburn U. Mechanical Engineering and Vir Phoha/Computer Science at LaTech)
Supported By	*2015-2017 GoMRI Research Consortia*
Project Grant	*GOMRI2012-II_262 Project Description.pdf available from applicant*
Project Duration	*1 January 2015–31 December 2017*

19)Project Donor	***S&T LONG RANGE LRBAA HOMELAND SECURITY** (proposal pending)*
Project Name	*Quantitative Risk Assessment and Cost-Optimal Risk Mitigation to Enhance Quality for*

	National/State Cybersystems and Information Security Assurance
Supported By	*DHS S&T : Science and Technology Directorate, Security and Trust Division*
Project Grant	*CYBER SECURITY: CSD.07 – Information system insider threat detection models and mitigation technologies. CSD.10 – Software Assurance: Including tools and techniques for analyzing software*
Project Duration	*1 June 2013 – 31 May 2016*

LIST OF COURSES INSTRUCTED (1976-2013)

1976-77	*1 Semester*	*Linear Algebra* *Introduction to Statistics*
1977-81	*PhD Studies*	*Applied courses on Statistics and Power Reliability Engineering at Texas A&M University, Institute of Statistics and Electric Power Institute respectively (Total: 8)*
1981-82	*2 Semester*	*Nonparametric Statistics*
1982-83	*1 Semester*	*Fundamentals of Probability and Statistics I* *Sampling and Survey Design*
1982-83	*2 Semester*	*Fundamentals of Probability and Statistics II* *Introduction to Reliability Theory and Application*
1983-84	*1 Semester*	*Sampling Theory (Graduate)* *Theory of Statistical Inference I*
1983-84	*1 Semester*	*Reliability Theory (Graduate)* *Theory of Stochastic Processes* *Theory of Statistical Inference II*
1984-85	*1 Semester*	*Theory of Linear Models (Graduate)* *Introduction to Reliability Theory and Application*
1984-85	*2 Semester*	*Computational Statistics & Data Analysis (Grad.)* *Bio-Assay and Bio-Statistics (Grad.)* *Regression Analysis*
1985-86	*1 Semester*	*Introduction to Mathematical Statistics I* *Operations Research*
1985-86	*2 Semester*	*Introduction to Mathematical Statistics II* *Theory of Linear Models (Graduate)*
1986-87	*1 Semester*	*Computational Statistics I* *Introduction to Multivariate Statistics*
1986-87	*2 Semester*	*Computational Statistics II* *Reliability Theory & System Applications (Grad.)*

1987-88	*1 Semester*	*Decision Theory* *Computational Statistics I*
1987-88	*2 Semester*	*Computational Statistics II* *Statistical Analysis of Designed Experiments (Grad.)*
1988-89	*1 Semester*	*Fundamentals of Probability & Statistics I* *Reliability Theory & System Applications (Grad.)*
1988-89	*2 Semester*	*Fundamentals of Probability & Statistics II* *Applied Stochastic Processes (Grad.)*
1989-90	*1 Semester*	*Stat 511-Stat Methods (Grad./Purdue University)*
	2 Semester	*Stat 301-Quality Control (Undergrad. / Purdue U.)*
1990-91	*1 Semester*	*Stat 473-Statistical Computing I (M.C. Simulation)*
		Stat 355-(Nonlinear) Optimization in Statistics
1990-91	*2 Semester*	*Stat 474-Statistical Computing II(C-Programming)*
		Stat 356-Optimization II (Stat Qual. Control)
1991-92	*1 Semester*	*Stat 443- Statistical Data Analysis*
		Stat 514- Reliability Theory & Applications
	2 Semester	*Stat 456-Stochastic Processes*
1992-93	*1 Semester*	*General Statistics (Dokuz Eylul Univ.)*
	2 Semester	*Comp. Progr., Biostatistics, Seminar in Med. Stats*
1993-94	*1 Semester*	*Introd. to Stat. and Probability I (undergrad)* *Stat Inference I (grad.), Sampling (grad.)*
	2 Semester	*Introd. to Stat. and Probability II (undergrad.)* *Stat. Inference II (grad.), Design of Exp. (grad.)*
1994-95	*1 Semester*	*Introd. to Stat. and Probability I (undergrad.)* *Stat Inference I (grad.), Nonparametric Stat. (grad.)*
	2 Semester	*Introd. to Stat. and Probability II (undergrad.)* *Stat. Inference II (grad.), Comp. Stat. & Simulation (grad.)*
1995-96	*1 Semester*	*Introd. to Stat. and Probability I (ugrad.)* *Math. Stat. I (ugrad.), Prob. Theory (ugrad.),* *Stat. Inference I (grad.), Actuarial & Risk Analy. (grad.)*
	2 Semester	*Introd. to Stat. and Probability II (ugrad.)* *Math Stat II (ugrad.), Probability Theory (ugrad.)* *Comp. Stat. & Simulation (grad.)*

1996-97	*1 Semester*	*Introd. to Stat. and Probability I (ugrad.)* *Math. Stat I (ugrad.)*
	2 Semester	*Introd. to Stat. and Probability II (ugrad.)* *Math . Stat II (ugrad.)*
	1 Semester	*Introd. to Prob.&Statistics / 2 sections (Stat 301t) ugrad. Purdue University*
1997-98		
	2 Semester	*Introd. to Prob. & Statistics/ 2 sections (Stat 301t) ugrad. Purdue University*
	Sum.Semester	*Basic Statistics for Social & Life Sciences (Stat 201) ugrad. Case Western Reserve U.*
	Sum.Semester	*Statistics for Engineering & Science (Stat 312) ugrad. Case Western Reserve U.*
1998-99	*1 Semester*	*Statistics for Engineering & Science (Stat 312) ugrad. Case Western Reserve U.*
	1 Semester	*Digital Signal Processing (Stat 332) ugrad. Case Western Reserve U.*
	2 Semester	*Statistics for Engineering & Science (Stat 312) ugrad. Case Western Reserve U.*
	2 Semester	*Reliability and Calibration (Stat 413) ugrad. / grad. Case Western Reserve U.*
	2 Semester	*Basic Statistics for Social & Life Sciences(Stat 201) ugrad. Case Western Reserve U.*
	Sum Semester	*Basic Statistics for Social & Life Sciences(Stat 201) ugrad. Case Western Reserve U.*
	Sum Semester	*Statistics for Engineering & Science (Stat 312) ugrad. Case Western Reserve U.*

Troy State University Montgomery – Troy University Montgomery Campus

1999-00	*Fall Quarter*	*Probability and Statistics (CIS 313) ugrad.*
	Spring Quarter	*Probability and Statistics (CIS313) ugrad.*
	Summer Quarter	*Operations Research (CIS 355) ugrad.*
2000-01	*Fall Semester*	*Probability and Statistics (CIS 3313) ugrad.*

	Spring Semester	*Software Quality Engineering and Metrics(CIS6649) grad.*
	Spring Semester	*Probability and Statistics (CIS313) ugrad.*
	Spring Semester	*Operations Research (CIS 3325) ugrad.*
	Summer Semester	*Thesis and Research (CIS 6699)*
2001-02	*Fall Semester*	*Probability and Statistics (CIS 3313) ugrad.*
	Fall Semester	*Operations Research (CIS 3325) ugrad.*
	Spring Semester	*Probability and Statistics (CIS 3313) ugrad.*
	Spring Semester	*Operations Research (CIS 3325) ugrad.*
	Spring Semester	*Seminar on Software Quality and Security Engineering (CISS 4449) ugrad*
	Spring Semester	*Software Quality Engineering and Metrics (CIS6649) grad.*
	Fall/Spring Semester	*Thesis and Research (CIS 6699)*
2002-03	*Fall Semester*	*Probability and Statistics (CIS 3313) ugrad.*
	Fall Semester	*Modeling and Simulation (CIS 6647) grad.*
	Fall Semester	*Data Communications and Network Eng. (CIS 4445) ugrad.*
	Fall Semester	*Thesis and Research (CIS 6699) grad.*
	Spring Semester	*Probability and Statistics (CIS 3313) ugrad.*

	Spring Semester	*Data Communications and Network Eng. (CIS 4445) ugrad.*
	Summer Semester	*Software Quality Engineering and Metrics (CIS6649) grad.*
2003-04	*Fall Semester*	*Probability and Statistics (CIS 3313) ugrad.*
	Fall Semester	*Data Communications and Network Eng (CIS 4445) ugrad.*
	Spring Semester	*Probability and Statistics (CIS 3313) ugrad.*
2004-05	*Fall Semester*	*Probability and Statistics (CIS 3313) ugrad.*
	Fall Semester	*Seminar on Software Quality & Security Engineering (CIS 4449) ugrad.*
	Spring Semester	*Probability and Statistics (CIS 3313) ugrad.*
2005-06	*Fall Semester*	*Computer Concepts & Applications (IS 2241) ugrad*
	Fall Semester	*Applied Statistics (MTH 2210) ugrad.*
	Fall Semester	*Operations Analysis and Modeling (CS 6647) grad.*
	Spring Semester	*Computer Concepts & Applications (IS 2241) ugrad. on-line blackboard*
	Spring Semester	*Computer Security & Reliability (CS 4451) ugrad.*
	Spring Semester	*Computer Concepts & Applications (IS 2241) ugrad. on-line blackboard*
	Summer Semester	*Computer Concepts & Applications (IS 2241) ugrad. on-line blackboard*

2006-07	*Fall Semester*	*Applied Statistics (MTH 2210) ugrad.*
	Fall Semester	*Computer Security & Reliability (CS 4451) ugrad.*
	Spring Semester	*Operations Analysis and Modeling (CS 6647) grad.*
	Spring Semester	*Computer Security & Reliability (CS 6653) grad.*
2007-08	*Fall Semester*	*Operations Analysis and Modeling (CS 6647) grad.*
	Fall Semester	*Computer Security & Reliability (CS 6653) grad.*
	Spring Semester	*Computer Security & Reliability (CS 6653) grad.*

AUM Courses (2011-): See CSIS Flyer

2012 Spring Sem. CSIS 6013 –Network Reliability and Security Metrics

2012 Fall Sem. CSIS 6043 –Computer Systems Modeling and Simulation

2013 Spring Sem. CSIS 6013 Network Security and Reliability Metrics, CSIS 6952 Internship

2013 Fall Sem. CSIS 6043 –Computer Modeling Simulation, CSIS 6952 Cybersecurity Seminar Internship

2014 Spring Sem. CSIS 6013 Network Security and Reliability Metrics, CSIS 6952 Internship

Candidate's Activities for the Advancement of Engineering, Science and Technology

***A. Contributions**: 1) Dr. Sahinoglu has pioneered a failure-count prediction technique in hardware (embedded) or software testing process known as Compound Poisson Software Reliability Model (CPSRM) for estimating the residual number of software or failures in testing. He also developed a Stopping-Rule Algorithm in testing large pieces of software extending his reliability-growth model to optimize resource utilization, as contrasted to conventional techniques that require billions of test vectors. His joint research in earlier years with Professor G. Spafford from Purdue University and SERC to conduct mutation testing in 1990s on Testing and Reliability, and in later years with Professor Das in 2000s on Built-in-Self Testing (BIST) and System-on Chip (SOC) regarding the general topic of Non-Exhaustive Testing complement his research findings on his Stopping-Rule algorithm. One such publication in October 2005 by IEEE Trans. in M & I augments earlier works by the joint authors, Das et al., on space compression considering specifically full scan sequential benchmark circuits for digital testing in non-exhaustive test sets. 2) He has further developed (1981) jointly but independently with Dr. Libby, the Sahinoglu-Libby probability model of component unavailability, that is an improved finding in contrary to classical modeling of availability where small sample results replace erroneously - assumed large sample approximations of unavailability. 3) Most recently, Dr. Sahinoglu's probabilistic and game-theoretic security-meter algorithm to assess and manage risk quantitatively, has found more favor than qualitative techniques because it converts to monetary tangible assets. This novel approach can be useful to Homeland Security, or banks or companies to quantify security levels at critical locations, also useful to home PCs for ubiquitous use. Dr. Sahinoglu's contributions in assurance sciences and in particular, reliability and security research are progressing with major industrial implications. His research derives from focusing on these subjects for an extended time, which goes back to while he was finalizing his MS and PhD dissertations at the University of Manchester and Texas A & M University respectively both on reliability, which later led to his involvement with Hardware & Software Security Risk Engineering domain at large.*

***B. Details and specifics:** Dr. Sahinoglu's contributions in the field of software/hardware reliability and security science and engineering are regarded more innovative than routine. His originality in deriving a new failure-count prediction model, viz. CPSRM (Compound Poisson Software Reliability Model) in Software Reliability is an authoritative work, and has been cited by peers in various publications, and in renowned textbooks. Dr. Sahinoglu applied his accumulation of knowledge and expertise in creating a cost-efficient stopping-rule algorithm, MESAT, to save substantial amounts of test vectors in achieving a desirable degree of coverage reliability or security. Through cost-benefit analysis, he has shown how cost-efficient his proposed stopping-rule algorithm is, as compared to those employing conventionally exhaustive "shot-gun" or "testing-to-death" approaches. This novel and cost-effective technique is valued for its industrial potentials as well. Dr. Sahinoglu has subsequently proposed a practical method to compare the forecast accuracy of software reliability prediction models.those used The method assesses the superiority of one failure-count software reliability model over the other by measuring its probability of how much better. The technique calculates the Bayes probability of how much better the prediction accuracy is for one* *software reliability estimation method relative to a competitor. This is more informative than only qualifying that one is superior to the other in terms of hypothesis testing of equality of means or a mere arithmetic difference of AREs (average relative error) without incorporating the inherent variability of predicted values. The algorithm involves non-informative and informative priors that are placed on the mean of ARE of the predictions, taken this time to be a r.v., rather than a conventional deterministic quantity. This work facilitates to compare between competing software reliability models such as those used in the outer space.*

Dr Sahinoglu has demonstrated pioneering applied research in developing what is now known as Sahinoglu-Libby formula, a probability density function (pdf) of the unavailability parameter to closely characterize the probabilistic behavior associated with the error distributions in components in relation to their application in network reliability. His "security-meter" discovery of a first-time quantitative risk model, published in IEEE Security and Privacy, and later in his class-tested Wiley textbook titled "Trustworthy Computing" has been a timely achievement in the era of security malwares and notorious data breaches. Dr. Sahinoglu covered all these innovative topics in his 2007 Wiley Textbook. This class–tested book (seven years before it got published), complete with CD ROM containing cases and projects give readers a hands-on experience on, reliability, security, privacy and a combined index of trustworthiness as a reference for practicing software designers and developers, computer reliability, security-privacy risk specialists, network administrators to work with data.

***C. Other Specifics**: Dr. Sahinoglu served in 1980s as a Network Reliability analyst to TEK (Turkish-Electricity-Authority) and Defense Industry on energy projects besides representing the Turkish Energy Ministry as a principal technical reporter with Economic Commission of Europe, and UN (United Nations) in Geneva and Moscow. His co-authored paper, i.e. M. Sahinoglu, M. Longnecker, L. Ringer, C. Singh, and A. K. Ayoub, "Probability Distribution Function for Generation Reliability Indices-Analytical Approach," IEEE Trans. PAS, Vol. 102, 1486-93, (1983) introduces the main aspects of the author's Ph.D. dissertation with a system emphasis on Power Generation Reliability Indices, and also the first time introduction of the pdf of the FOR (unavailability), later named Sahinoglu-Libby probability model, under certain underlying statistical assumptions.*

He has pioneered an engineering-statistical sampling scheme, and then extensively collected data in entire Turkey and Balkan countries for electrical power generation and failure-repair activities during his consultancy work (1982-1997). He established the first automated mutation-based MOTHRA software testing laboratory in Turkey at METU- Ankara and at DEU-Izmir under a TUBITAK (Turkish NSF) grant in collaboration with Purdue University's Software Engineering Research Center (SERC). He was the founder Dean of the College of Science at DEU (1992-1997) where he developed computer reliability engineering courses. He also served as the project manager for the first-time introduction of the Internet facility to DEU and city of Izmir in 1993. He organized the first international summer school in Turkey on Computer Software-Intensive Model Selection in Quality Control under ISI-IASC (1995). He introduced the reliability courses in Turkish higher-ed schools (1982-97) until he relocated in USA. Dr. Sahinoglu recently wrote a textbook on "Trustworthy Computing" (2007) published by Wiley & Sons for graduate students while finalizing his 2006 international Microsoft Trustworthy Computing Curriculum grant. Since his Eminent Scholar assignment at Troy University, he organized the first kick-off conference on IT (2000), and nine annual and two separate symposia at TROY University by inviting the world's prominent speakers under IT Colloquium Series in cooperation with the local IEEE Chapter. He has jumpstarted the Software Quality and Security Engineering program at TROY University system globally as of 2000.

Dr. Sahinoglu subsequently founded Informatics Institute in 2008 at AUM in Montgomery AL, and later in 2009 CSIS (Cybersystems and Information Security) graduate program, the fiursdt one of its kind in the Southeast USA which later was accredited by SACS Southern Association of Colleges and Schools) in 2010 and NSA (National Security Association) accredited in 2013.

(*) The candidate has innovated a new engineering-statistical chronological sampling scheme, and collected extensively vital data in entire Turkey for electrical power generation, failure and repair activities during his consultant work (1982-1997) as a Reliability Engineer and Statistician for Turkish Electricity Authority (TEK). His sampling survey model now is in effect as adopted in all generation plants in Turkey's vast power generation arena exceeding 360 generating units (in 25 major categories) generating approximately 22000 Mega-Watts. He has published these works within 15 years during his consultant status in 8 different projects as Technical Reports under "The Computation of Reliability Indices in Turkish Electricity Supply Network-Sensitivity Analyses and Inference" (original in Turkish) as submitted to TEK's Research, Project and Coordination division. TEK has used these results for 2000-2010 Master Strategic Plan. ECE's Committee on Planning of Large Electric Power Systems in Geneva under auspices of UN also released a technical report in 1988 on "The Interconnected Reliability Indices of Balkan Power Systems" for which he was the responsible reporter and data collector, in representation of all 5 Balkan nations' (Turkey, Bulgaria, Greece, Romania and Yugoslavia) power generation networks. Dr. Sahinoglu's work was the very first Statistical Reliability Analysis that brought an exploratory statistical approach to Turkey's quantification of the service quality of its power systems, contrary to conventional ways. He presented the same work on "Turkey's Power Generation Reliability Indices" in Moscow and St. Petersburg (1987) while serving as a reporter to UN.

(**) Dr. Sahinoglu served as a Network Reliability analyst to TEK and Defense Industry on projects besides representing the Turkish Energy Ministry as a technical reporter with ECE/UN in Geneva and Moscow. He has pioneered a new software for a statistical historical-sampling scheme, and extensively collected vital data in entire Turkey for electrical power generation, failure and repair activities during his consultancy work (1982-1997) as a Reliability Engineer and Statistician for Turkish Electricity Authority (TEK). He also served as the project manager for the first-time introduction of the Internet facility to DEU and city of Izmir in 1993. He organized the first international summer school in Turkey on Computer Software-Intensive Model Selection in Quality Control under ISI-IASC (1995). He introduced the power and software reliability engineering courses in Turkish schools (1982-97) until his relocation to USA in 1997.

(***) Dr. Sahinoglu later established a Cybersecurity Testing lab at AUM's Informatics Institute in 2013 using equipment donated by ICS/Montgomery (see grant #16, p.42). The firewall(s) will be configured to allow traffic during the three years (150 weeks) for 15 selected sample nations: 1)USA, 2) Romania, 3) China, 4) Russia, 5) N. Korea, 6) Nigeria, 7) India, 8) Turkey, 9) France, 10) Brazil, 11) Sweden, 12) South Africa, 13)Bulgaria, 14)Poland, 15) United Kingdom. The Firewall(s) will change countries every other 10 weeks by sampling different ones to evenly represent the worlds geographical demography. This will provide, by using the logging server, an overall log of information on how active a particular sample country is by recording in terms of malware traffic information. In this case, the event can be considered an attack because they dont have a valid reason for being in the AUM Informatics Institute network (a disclaimer will be placed to warn that this is not an academic web site or similar; however a proxy name will be attached such as Nuclear Solutions to attract malware traffic). They will alternate every 10th week to assure 15 nations coverage for 150 weeks. This will enable the analyst to compare various countries" attack percentages overall since we also will have the entire Internet traffic figures (such as N. Korea over a week sharing 10%, Russia 5% etc. to rank the highest at risk). See p.50 for an illustration of the test lab.

THE
NEW YORK
ACADEMY OF SCIENCES

PRESENTED TO

PROF MEHMET SAHINOGLU

IN RECOGNITION AND CERTIFICATION OF BEING ELECTED

AN ACTIVE MEMBER

OF THIS ACADEMY

December 1993

PRESIDENT

TO REMAIN IN GOOD STANDING
BY FULFILLING THE RESPONSIBILITIES
OF MEMBERSHIP

SECRETARY · TREASURER

FOUNDED 1817

IEEE THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.
345 EAST 47TH STREET, NEW YORK, N.Y. 10017-2394, U.S.A. TELEX 236411

MARTHA SLOAN
1993 PRESIDENT

DIRECT NUMBER (212) 705-7869
FAX (212) 705-7182
E.MAIL: M.Sloan@ieee.org

July 15, 1993

Dr. Mehmet Sahinoglu
Fac. of Sci. & Letters
Dokuz Eylul Univ.
1420 Sok No. 79/Kahramanlar
Izmir 35230 Turkey

Dear Dr. Sahinoglu:

It is a pleasure to advise you that you have been elected to Senior Member in IEEE. Only 8% of the over 320,000 IEEE members hold this grade.

I would be delighted to write to your employer, notifying him or her of your elevation to this high grade of membership. If it is agreeable to you, please furnish the name, title, and address of your employer on the form enclosed. A return envelope is enclosed for your convenience in responding.

Please accept my sincere congratulations on your election to Senior Member.

Sincerely,

Martha Sloan
President

MS:dp

IEEE

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

In recognition of professional standing
the Officers and Board of Directors of
the Institute certify that

MEHMET SAHINOGLU

has been elected to the grade of

Senior Member

President

Secretary

July 1993

Salzburg Seminar

hereby certifies that

Mehmet Sahinoglu

was selected

to participate in Session 301

under a grant awarded by the

Ryoichi Sasakawa Young Leaders Fellowship Program

In witness whereof we have hereunto affixed our signatures and the seal of the corporation.

President

Vice President and Treasurer

Schloss Leopoldskron
Salzburg, Austria

March 17, 1994
Date

International
Statistical
Institute

CERTIFICATE

This is to certify that

Mehmet Sahinoglu

has been elected

ORDINARY MEMBER

of the

INTERNATIONAL STATISTICAL INSTITUTE

IN 1995

Date: August 25, 1995

Witnessed by:

Z. Kenessey

Director, ISI

CERTIFICATE OF REGISTRATION

OFFICIAL SEAL — UNITED STATES COPYRIGHT OFFICE — THE LIBRARY OF CONGRESS

This Certificate issued under the seal of the Copyright Office in accordance with title 17, United States Code, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

Marybeth Peters

REGISTER OF COPYRIGHTS

FORM TX

For a Nondramatic Literary Work
UNITED STATES COPYRIGHT OFFICE

REG

TXu 1-052-690

EFFECTIVE DATE OF REGISTRATION

Month	Day	Year
9	7	01

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

1

TITLE OF THIS WORK ▼ MESAT: Mehmet Sahinoglu's Cost-Effective Stopping-Rule Algorithm on Testin[g]
http://cis.tsum.edu/~mesa/mtsg3/index.html

PREVIOUS OR ALTERNATIVE TITLES ▼ Some

PUBLICATION AS A CONTRIBUTION If this work was published as a contribution to a periodical, serial, or collection, give information about the collective work in which the contribution appeared. Title of Collective Work ▼ —

If published in a periodical or serial give: Volume ▼ Number ▼ — Issue Date ▼ On Pages ▼

2

a **NAME OF AUTHOR ▼** Mehmet Sahinoglu, Prof.

DATES OF BIRTH AND DEATH Year Born ▼ 1951 Year Died ▼ —

Was this contribution to the work a "work made for hire"? ☐ Yes ☒ No

AUTHOR'S NATIONALITY OR DOMICILE Name of Country
OR Citizen of ▶ TURKEY
Domiciled in ▶ Montgomery, AL 36117

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? ☐ Yes ☒ No
Pseudonymous? ☐ Yes ☒ No
If the answer to either of these questions is "Yes," see detailed instructions.

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼ Some new text and compilation

b **NAME OF AUTHOR ▼**

DATES OF BIRTH AND DEATH Year Born ▼ Year Died ▼

Was this contribution to the work a "work made for hire"? ☐ Yes ☐ No

AUTHOR'S NATIONALITY OR DOMICILE Name of Country
OR Citizen of ▶
Domiciled in ▶

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? ☐ Yes ☐ No
Pseudonymous? ☐ Yes ☐ No
If the answer to either of these questions is "Yes," see detailed instructions.

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼

c **NAME OF AUTHOR ▼**

DATES OF BIRTH AND DEATH Year Born ▼ Year Died ▼

Was this contribution to the work a "work made for hire"? ☐ Yes ☐ No

AUTHOR'S NATIONALITY OR DOMICILE Name of Country
OR Citizen of ▶
Domiciled in ▶

WAS THIS AUTHOR'S CONTRIBUTION TO THE WORK
Anonymous? ☐ Yes ☐ No
Pseudonymous? ☐ Yes ☐ No
If the answer to either of these questions is "Yes," see detailed instructions.

NATURE OF AUTHORSHIP Briefly describe nature of material created by this author in which copyright is claimed. ▼

NOTE

Under the law, the "author" of a "work made for hire" is generally the employer, not the employee (see instructions). For any part of this work that was "made for hire" check "Yes" in the space provided, give the employer (or other person for whom the work was prepared) as "Author" of that part, and leave the space for dates of birth and death blank.

3

a **YEAR IN WHICH CREATION OF THIS WORK WAS COMPLETED** 2001 ◀ Year. This information must be given in all cases.

b **DATE AND NATION OF FIRST PUBLICATION OF THIS PARTICULAR WORK** Complete this information ONLY if this work has been published. Month ▶ Day ▶ Year ▶ ◀ Nation

4

COPYRIGHT CLAIMANT(S) Name and address must be given even if the claimant is the same as the author given in space 2. ▼

Mehmet Sahinoglu
7542 Mossy Oak Dr.
Montgomery, AL 36117-5606

TRANSFER If the claimant(s) named here in space 4 is (are) different from the author(s) named in space 2, give a brief statement of how the claimant(s) obtained ownership of the copyright. ▼

[illegible]

See instructions before completing this space.

DO NOT WRITE HERE — OFFICE USE ONLY

APPLICATION RECEIVED JUL 31, 2002 9-7-01

ONE DEPOSIT RECEIVED 9-7-01

TWO DEPOSITS RECEIVED

FUNDS RECEIVED

MORE ON BACK ▶ • Complete all applicable spaces (numbers 5-9) on the reverse side of this page. • See detailed instructions. • Sign the form at line 8.

DO NOT WRITE HERE

EXAMINED BY SB / ORM

CHECKED BY

☑ CORRESPONDENCE Yes

FORM TX

FOR COPYRIGHT OFFICE USE ONLY

DO NOT WRITE ABOVE THIS LINE. IF YOU NEED MORE SPACE, USE A SEPARATE CONTINUATION SHEET.

5

PREVIOUS REGISTRATION Has registration for this work, or for an earlier version of this work, already been made in the Copyright Office?

☐ Yes ☐ No If your answer is "Yes," why is another registration being sought? (Check appropriate box.) ▼

a. ☐ This is the first published edition of a work previously registered in unpublished form.

b. ☐ This is the first application submitted by this author as copyright claimant.

c. ☐ This is a changed version of the work, as shown by space 6 on this application.

If your answer is "Yes," give: **Previous Registration Number** ▶ **Year of Registration** ▶

6

DERIVATIVE WORK OR COMPILATION

a **Preexisting Material** Identify any preexisting work or works that this work is based on or incorporates. ▼

M.Sahinoglu, "Compound Poisson Software Reliability Model (CPSRM), IEEE Trans. Software Engineering, Vol. 18, pp 624-630, July 1992

See instructions before completing this space.

b **Material Added to This Work** Give a brief, general statement of the material that has been added to this work and in which copyright is claimed. ▼

Some new text and compilation

7

a **DEPOSIT ACCOUNT** If the registration fee is to be charged to a Deposit Account established in the Copyright Office, give name and number of Account.

Name ▼ Account Number ▼

—

b **CORRESPONDENCE** Give name and address to which correspondence about this application should be sent. Name/Address/Apt/City/State/ZIP ▼

Prof. Mehmet Sahinoglu
7542 Mossy Oak Dr.
Montgomery AL 36117

Area code and daytime telephone number ▶ (334)273-9923 Fax number ▶ (334)274-0281

Email ▶ mesa@tsum.edu

8

CERTIFICATION* I, the undersigned, hereby certify that I am the

Check only one ▶
☐ author
☐ other copyright claimant
☐ owner of exclusive right(s)
☐ authorized agent of

Name of author or other copyright claimant, or owner of exclusive right(s) ▲

of the work identified in this application and that the statements made by me in this application are correct to the best of my knowledge.

Typed or printed name and date ▼ If this application gives a date of publication in space 3, do not sign and submit it before that date.

MEHMET SAHINOGLU Date ▶ Jan 8, 2002

Handwritten signature (X) ▼

X M Sahinoglu

9

Certificate will be mailed in window envelope to this address:

Name ▼ Prof. Mehmet SAHINOGLU

Number/Street/Apt ▼ 7542 Mossy Oak Dr.

City/State/ZIP ▼ Montgomery AL 36117-5606

YOU MUST:
- Complete all necessary spaces
- Sign your application in space 8

SEND ALL 3 ELEMENTS IN THE SAME PACKAGE:
1. Application form
2. Nonrefundable filing fee in check or money order payable to *Register of Copyrights*
3. Deposit material

MAIL TO:
Library of Congress
Copyright Office
101 Independence Avenue, S.E.
Washington, D.C. 20559-6000

As of July 1, 1999, the filing fee for Form TX is $30.

Certificate of Registration

This Certificate issued under the seal of the Copyright Office in accordance with title 17, United States Code, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

Register of Copyrights, United States of America

SHORT FORM TX
For a Nondramatic Literary Work
UNITED STATES COPYRIGHT OFFICE

P

TXu 1-134-116

TXU 1134116

Effective Date of Registration
12-5-03

Application Received
DEC 05 2003

Deposit Received
One DEC 05 2003 Two

Fee Received

Examined By
MW

Correspondence ☐

TYPE OR PRINT IN BLACK INK. DO NOT WRITE ABOVE THIS LINE.

Title of This Work: Alternative title or title of larger work in which this work was published:	**1**	SECURITY METER (Sec-Meter) - A PROBABILISTIC FRAMEWORK TO QUANTIFY SECURITY RISK
Name and Address of Author and Owner of the Copyright: Nationality or domicile: Phone, fax, and email:	**2**	Mehmet Sahinoglu 7542 Mossy Oak Drive Montgomery, AL 36117-5606 Phone (334) 270-0190 Fax (334) 274-0281 Email falconson@bellsouth.net
Year of Creation:	**3**	2003
***If work has been published,* Date and Nation of Publication:**	**4**	a. Date ______ Month ______ Day ______ Year ______ *(Month, day, and year all required)* b. Nation
Type of Authorship in This Work: Check all that this author created.	**5**	☒ Text (includes fiction, nonfiction, poetry, computer programs, etc.) ☐ Illustrations ☐ Photographs ☐ Compilation of terms or data
Signature: Registration cannot be completed without a signature.	**6**	*I certify that the statements made by me in this application are correct to the best of my knowledge.** Check one: ☒ Author ☐ Authorized agent X M Sahinoglu
OPTIONAL **Name and Address of Person to Contact for Rights and Permissions:** Phone, fax, and email:	**7**	☒ Check here if same as #2 above. Phone ( ) Fax ( ) Email

8 Certificate will be mailed in window envelope to this address:

Name ▼
Mehmet Sahinoglu, Ph,D.

Number/Street/Apt ▼
7542 Mossy Oak Drive

City/State/ZIP ▼
Montgomery, AL 36117-5606

Complete this space only if you currently hold a Deposit Account in the Copyright Office.

9 Deposit Account # ______
Name ______

DO NOT WRITE HERE Page 1 of 1 pages

*17 U.S.C. § 506(e): Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 409, or in any written statement filed in connection with the application, shall be fined not more than $2,500.

Rev: June 2002—20,000 Web Rev: June 2002 Printed on recycled paper

U.S. Government Printing Office: 2000-461-113/20,021

Compact Resume(from www.aum.edu/csis)

Director, Informatics Institute, Auburn Montgomery
With a Ph.D. jointly in EE and Statistics at Texas A&M (1981), an MS in Electric Power from UMIST, England (1975) in EE, and a BS in Electrical & Computer Engineering from METU/Ankara (1969-73), Mehmet taught at TAMU (1980-81), METU (1982-92) where he served as an assistant, associate, and then full professor. Later he taught at Purdue (1989-90, 1997-98) and Case Western Reserve University (1998-99) as Fulbright and NATO fellows in the capacity of a visiting professor. He served as the College of Arts and Sciences founding dean, and Quantitative Sciences Department founder chair at DEU in Izmir (1992-97). He served as the Eminent Scholar and Chair Professor of the CS Department at Troy University Montgomery Campus before being assigned at AUM in 2008 as a Distinguished Professor and Director of Informatics Institute.

A Fellow of Society of Design and Process Science (SDPS), and Senior Member of IEEE and ISI Elected Member, he co-created the "Sahinoglu & Libby Probability Distribution (1981)", and derived "Compound Poisson Software Reliability Model & Stopping Rule in Software Testing" and "Security Meter Quantitative Risk Assessment" algorithms. Dr. Sahinoglu published "Trustworthy Computing" textbook by Wiley & Sons (2007). He was one of the 14 global Microsoft Trustworthy Computing awardees (2006). Dr. Sahinoglu won best paper awards with Wiley Interdisciplinary Reviews (WIREs) in 2010 and 2011 on Network Reliability and Cloud Computing, and was invited to publish an advanced review on Game-theoretic Computing in Risk Analysis for 2012 and Modeling and Simulation in Engineering in 2013, both of which have been published. He has recently received funding on cyber assurance projects including Microsoft's. Dr. Sahinoglu has a total of more than 170 peer reviewed journal and proceedings research papers and book chapters combined during 30+ years of his academic career (1981-2013). He founded the Informatics Institute at AUM in 2008 and established the CSIS (Cybersystems and Information Security) Master's program approved by ACHE in 2009 and accredited by SACS in 2010. He co-organized, as expected from an SDPS Fellow, the SDPS/Auburn U world conference on Cybersystems and Informatics at AUM in 2009 (www.aum.edu/csis).

Additional Patent Information: Patent Application Serial No. 12/407,892 Filing Date 3/20/2009
Title of Invention: Method of Automating Security Risk Assessment and Management with a Cost-Optimized Allocation Plan (also known as Security Meter or Risk-O-Meter).

Mehmet Sahinoglu, Ph.D.
Director, Informatics Institute, Cyberystems and Information Security ,
P.O.Box 244023, Auburn University Montgomery, Montgomery AL 36124-4023
334 244 3769 (tel.), 334 244 3127 (fax); E-mail: msahinog@aum.edu URL: www.aum.edu/csis

(a) Professional Preparation:

Middle East Technical University (METU)	*Electrical and Control Engineering*	*B.S., 1973*
University of Manchester (UMIST)	*Electrical Engineering*	*M.S., 1975*
Texas A&M University (TAMU)	*Electrical Engineering & Statistics*	*Ph.D, 1981*

(b) Appointments:

Aug 2008 – Present	*Director, Informatics Institute, Auburn University at Montgomery*
Aug 1999 – Aug 2008	*Troy Univ., ACHE (Alabama Commission on Higher Education)- Eminent Scholar - Endowed Chair; Professor and Head, Computer Science Department*
June 1998 – Aug 2009	*Visiting NATO Professor, Case Western Reserve University, Cleveland, OH.*
July 1997 – June 1998	*Visiting NATO Professor, Purdue Univ., West Lafayette, IN.*
July 1992 – July 1997	*Founding Dean, School of Arts and Sciences, and Founding Department Chair at Dokuz Eylul University (DEU), Izmir, Turkey.*
July 1990 - July 1992	*Professor, Middle East Technical Univ., Ankara,Turkey.*
July 1989 – July 1990	*Visiting Fulbright Professor, Purdue Univ., West Lafayette, IN.*
Jan 1982 – July 1989	*Asst., Assoc., Full Professor at Middle East Technical Univ., Ankara, Turkey.*
Aug 1978 – Dec 1981	*Graduate Research/Teaching Resident Assistant at Texas A&M Univ. Texas*

FIVE SELECTED PRODUCTS

1. *Sahinoglu M., 2005, "Security Meter - A practical decision meter model to quantify risk. IEEE Security and Privacy. **3**(3), 18-24.*
2. *Sahinoglu M., 2008, "An input-output measurable design for the Security Meter model to quantify and manage software security risk. IEEE Trans on Instrumentation and Measurement, **57**(6), 1251-1260.*
3. *Sahinoglu M., 2012, CLOUD Computing Risk Assessment and Management, Book (Risk Assessment and Management) Chapter, Academy Publish.* http://www.academypublish.org/book/show/title/risk-assessment-and-management
4. *Sahinoglu M., 2013, "The modeling and simulation in engineering," Invitational Overview: WIREs (Wiley Interdisciplinary Reviews), WIREs Comput Stat 2013, 239-266. Doi:10.1002/wics 1254.* http://www.aum.edu/UR_Media/NandH/13nandh/130429/Sahinoglu_WICS1254_article.pdf
5. *Sahinoglu M, 2007, Trustworthy Computing - Analytical and Quantitative Engineering Evaluation. Wiley Inc., Hoboken, New Jersey*

FIVE RELATED PRODUCTS

1. *Sahinoglu, M, Rice B., 2010, "Network Reliability Evaluation," Invited Advanced Review for* Wiley Interdisciplinary Reviews: Computational Statistics, *New Jersey, **Vol. 2**, No. 2, 189-211*
2. *Sahinoglu, M, Libby, D., Das, S. R., 2005, "Measuring Availability Indices with Small Samples for Component and Network Reliability using the Sahinoglu-Libby Probability Model," IEEE Transactions on Instrumentation Measurement, **Vol. 54**, No.3, 1283-1295.*
3. *Sahinoglu, M., 2003, "An Empirical Bayesian Stopping Rule in Testing and Verification of Behavioral Models," IEEE Transactions on Instrumentation and Measurement, **52**(5), 1428-1443.*
4. *Sahinoglu, M., Cueva-Parra L., Ang D., 2012, "Game-theoretic computing in risk analysis", WIREs Comput Stat 2012, doi: 10.1002/wics, 1205 (d)*
5. *Sahinoglu, M., 1992, "Compound-Poisson Software Reliability Model," IEEE Transactions on Software, Engineering, **Vol. 18**, 624-630.*

Five others related but not Listed above:

Sahinoglu M, Cueva-Parra L., "CLOUD Computing," Invited Authors (Advanced Review)for Wiley Interdisciplinary Reviews: Computational Statistics, *New Jersey, Ed.-in-Chief: E. Wegman, Yasmin H. Said, D. W. Scott, **Vol. 3**, Number 1, March 2011, pp. 47-68.*

Sahinoglu, M., "The Limit of Sum of Markov Bernoulli Variables in System Reliability Estimation," on IEEE Transactions Reliability, ***Vol. 39**, pp. 46-50, April 1990.*

*Sahinoglu M., Y.-L. Yuan, D. Banks, "Validation of a Security and Privacy Risk Metric Using Triple Uniform Product Rule," IJCITAE - International Journal of Computers, Information Technology and Engineering, Vol. **4**, Issue 2, pp. 125–135, December 2010.*

*Sahinoglu M., Cueva-Parra L., Simmons Susan J., "Software Assurance Testing Before Releasing Cloud for Business- A Case Study on a Supercomputing Grid (Xsede)", IJCITAEInternational Journal of Computers, Information Technology and Engineering, Vol. **6**, Issue 2, 73-81, December 2012.*

*Sahinoglu M., Ramamoorthy C.V., "RBD Tools Using Compression and Hybrid Techniques to Code, Decode and Compute s-t Reliability in Simple and Complex Networks",*IEEE Transactions on Instrumentation and Measurement, Special Guest Edition on Testing, *Vol. **54**, No.3, Oct. 2005, pp.1789-1799*

AUM News and Headlines:

August meeting of local ISSA chapter to feature Dr. Mehmet Sahinoglu. *This month's meeting of the Central Alabama Chapter of the Information Systems Security Association will be held on Monday, Aug. 20, from 11 a.m. to 12:30 p.m. at Baptist East in the administration boardroom. The featured speaker will be AUM's own* ***Dr. Mehmet Sahinoglu****, Director of the Informatics Institute. Sahinoglu will talk about "Risk Assessment and Management to Estimate Hospital Credibility Score of Patient Health Care Quality."*


Dr. Mehmet Sahinoglu

Dr. Mehmet Sahinoglu*, Director of the Informatics Institute, has published a couple of works recently as well as spread a little knowledge of cybersecurity to a local high school class. Sahinoglu jointly published "Software Assurance Testing before releasing Cloud for Business- A Case Study on a Supercomputing Grid (XSEDE)" in the* International Journal of Computers, Information Technology and Engineering *with Dr. Luis Cueva-Parra (AUM), Dr. Susan J. Simmons (University of North Carolina Wilmington), and Dr. Sunil R. Das (University of Ottawa and Troy University). Sahinoglu's seminal invitational advanced overview paper, "Modeling and simulation in engineering," covering an extended 30-plus years of research since earning his Ph.d., has been published by Wiley's WIREs (Wiley Interdisciplinary Review Series) in the May/June edition.*

During spring break, Sahinoglu conducted a classroom talk on Cybersecurity Risk Preventions and Metrics to a senior robotics class at St. James High School in Montgomery. The students worked on the Security Metric software developed by Sahinoglu. Later, the class learned how to manage risk using game-theoretic methodology by using the second phase of the software. The results of this work indicated that, for these high school users, there is close to a 50-50 chance of running into a threat not counter-measured properly.

Dr. Mehmet Sahinoglu*, Director of the Informatics Institute, co-wrote with Dr. Kenneth Wool, a cardiologist with Central Alabama Veterans Health Care System in Montgomery, the chapter "Risk Assessment and Management to Estimate and Improve Hospital Credibility Score of a Patient Health Care Quality" for the book* Applied Cyber-Physical Systems*. In June, Sahinoglu and Scott Morton, Program Assistant in the Informatics Institute, presented the paper "An Automated Algorithm to Assess and Manage Ecological Risk" at the International Conference on Environmental Science and Technology, Cappadocia Region, Urgup, Turkey.*

Dr. Mehmet Sahinoglu*, Director of the Informatics Institute, has had several articles published in 2012, including: "A New Metric for Usability in Trustworthy Computing of Cybersystems" in* Significance*, the bimonthly magazine and website of the Royal Statistical Society and the American Statistical Association, with Scott Morton, Erman Samelo and Sukanta Ganguly "Are Social Networks Risky? Assessing and Mitigating Risk" in* Significance*, with Aysen Dener Akkaya.*
The chapter "CLOUD Computing Risk Assessment and Management," pages 412-445 of Risk Assessment and Management*, published by Academy Publish. "Cost-Effective Security Testing of Cybersystems Using Combined LGCP: Logistic-Growth and Compound-Poisson Probability Modeling" in the International Journal of Computers, Information Technology and Engineering with Susan J. Simmons and James H. Matis.*

Dr. Mehmet Sahinoglu*, Director of the Informatics Institute, has published the article "Ecological Risk-O-Meter: A Risk Assessor and Manager Software Tool for Better Decision Making in Ecosystems" in the journal* Environmetrics*. Co-authored with Susan J. Simmons and Lawrence B. Cahoon, University of North Carolina Wilmington, and Scott Morton, AUM, the article discusses a software tool that not only assesses environmental and ecological risks, but also takes into account potential solutions and provides guidance as to how spending can be optimized to reducing overall environmental risk. Also published jointly by* ***Dr. Mehmet Sahinoglu*** *was "Game-theoretic computing in risk analysis" by WIREs Comput. Stat*
http://authorservices.wiley.com/bauthor/onlineLibraryTPS.asp?DOI=10.1002/wics.1205&ArticleID=961931

Sahinoglu M., Cueva-Parra L., "CLOUD Computing" Wiley Interdisciplinary Series, 2012
http://authorservices.wiley.com/bauthor/onlineLibraryTPS.asp?DOI=10.1002/wics.139&ArticleID=771921

From:	Edward Wegman <ewegman@gmail.com>
Sent:	Friday, August 20, 2010 9:46 AM
To:	Mehmet Sahinoglu
Cc:	Yasmin Said; David Scott
Subject:	Fwd: Top papers from Wiley Interdisciplinary Reviews Computational Statistics

You are one of the top viewed papers. Congratulations. Ed

---------- Forwarded message ----------
From: **Wiley-Blackwell** <wiley-blackwell@sci.scientific-direct.net>
Date: Fri, Aug 20, 2010 at 9:51 AM
Subject: Top papers from Wiley Interdisciplinary Reviews Computational Statistics
To: E J Wegman <ewegman@gmail.com>

We are pleased to provide you with information on products and services that might be of interest to you. Want to keep receiving these valuable messages in your inbox? Click here to find out how.

Now is your chance to see **Wiley Interdisciplinary Reviews Computational Statistics** – the important new forum that promotes cross-disciplinary discussion on a broad array of computational and statistical techniques.

This authoritative and encyclopedic resource addresses key topics from the diverse perspective of traditional statistics and modern computation. The content is fully citable, qualifying for abstracting, indexing, and ISI ranking.

Recommend to Library

Your institution can get complimentary online access - recommend to your librarian today

Sign Up for E-alerts

Keep up-to-date and view the latest articles from *WIREs Computational Statistics* by signing up for the table of contents alerts today - click here

Below are the top accessed papers from the second volume— read them for **FREE** now:

Overviews

Averaged shifted histogram
David W. Scott

Censored data
Irène Gijbels

Information visualization
Chaomei Chen

Statistical data mining
David L. Banks

Information measures
Ehsan S. Soofi, Huimin Zhao, Derek L. Nazareth

Computational social science
Claudio Cioffi-Revilla

Principal component analysis
Hervé Abdi, Lynne J. Williams

Advanced Review

Response surface methodology
André I. Khuri, Siuli Mukhopadhyay

Network reliability evaluation
Mehmet Sahinoglu, Benjamin Rice

Total least squares methods
Ivan Markovsky, Diana M. Sima, Sabine Van Huffel

Fuzzy set theory
H.-J. Zimmermann

Minimum covariance determinant

School of Sciences

Master of Science in Cybersystems and Information Security

Description:

The Master of Science degree program in Cybersystems and Information Security (CSIS) prepares students to become leaders in the field of information and network security, offering instruction and research opportunities that provide graduates with the necessary knowledge and skills to effectively assess, develop, and manage secure information networks and to respond to newly developed threats. This program offers a unique opportunity for students to learn to:

- Identify and respond to information security challenges in distributed and embedded systems.
- Evaluate and recommend technological tools and protocols to protect against risks.
- Integrate the use of encryption technology in non-secure and non-private computers and systems.
- Design and conduct research in the area of cybersystems and information security.
- Critically evaluate and apply research to computer and cybersystems threats.

Why a master's degree in CSIS is important:

There is an ever-increasing need in society for greater cybersystems and information security. This calls for the development of leaders who can implement, monitor, and respond to security issues, as well as researchers who can develop original and innovative technologies to improve cybersystems security. The Cybersystems and Information Security master's program will provide specialized training in computer network and information security, secure software engineering, operating system security, secure network engineering, and applied cryptology.

Preparation for program admission:

- Undergraduate degree in Computer Science or a related field. Other majors may require prerequisite coursework.

Students in this program will develop skills to:

- Demonstrate an understanding of the technical, management, and policy aspects of cybersystems and information security.
- Recognize the impact of security issues related to software engineering on distributed information systems.
- Assess information risks faced by an organization and develop a response plan.
- Demonstrate an understanding of technological and human engineering problems linked to security risks.
- Access the impact of information security policies, and market developments on complex systems and organizational objectives.
- Mitigate system vulnerabilities and restore compromised services.
- Manage the development, acquisition, and evolution of a secure information network.
- Construct secure networked and distributed computer systems.
- Troubleshoot large–scale information networks and distributed systems.
- Develop a strategy for lifelong learning and professional development in information security disciplines.

Students in this program can find jobs in:

- Information Technology
- Homeland Security
- Government and State Agencies
- Private Business
- Armed Forces

Students in this program will be instructed by:

Qualified faculty from Auburn University at Montgomery, Auburn University, and also experienced instructors and practitioners from the IT industry professionally affiliated with Cybersystems and Information Security issues.

Location:

Auburn Montgomery campus and online at www.aum.edu./csis

Starting Semester:

Fall (August) 2011

CSIS Courses:

The curriculum consists of 36 semester hours with thesis or nonthesis options. Courses are taught by faculty from the Schools of Sciences and Business at AUM, and in partial collaboration with the Auburn University Department of Computer Science and Software Engineering.

CSIS 6003:	Introduction to Computer Security, 3hrs.
CSIS 6010:	Data Communications & Computer Networks, 3 hrs.
CSIS 6013:	Network Security & Reliability-Quantitative Metrics, 3 hrs.
CSIS 6020:	Distributed Systems, 3 hrs.
CSIS 6033:	Secure Software Systems, 3 hrs.
CSIS 6040:	Applied Cryptology, 3 hrs.
CSIS 6053:	Information Security Management, 3 hrs.
CSIS 6403:	Computer Systems Modeling & Simulation, 3 hrs.
ACCT 6180:	Financial Accounting/Integrated Business Concepts, 3 hrs.

Without thesis option:

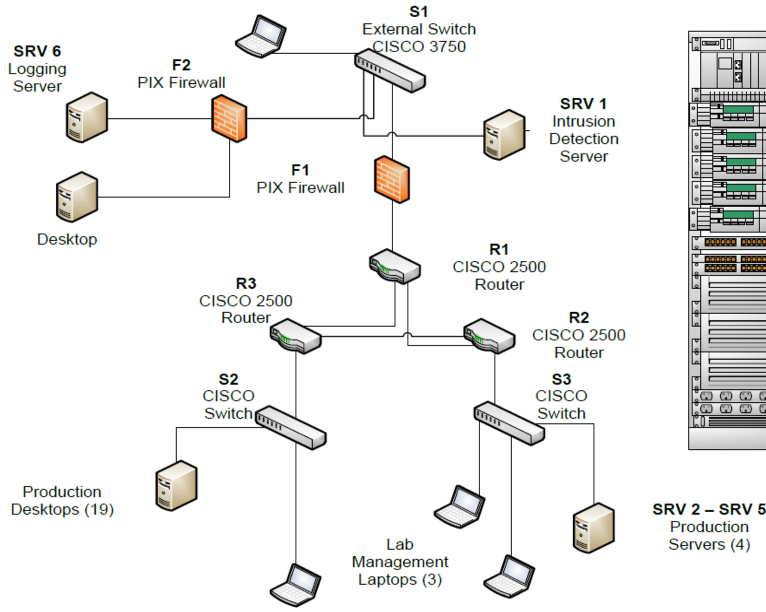
QMTD 6750:	Operations Research, 3 hrs.
CSIS 6912:	Supervised Practicum with Cyber-Industry Experience, 3 hrs.
CSIS: 6952:	Security Policy Seminar: Healthcare, Finance, Business, or Government, 3 hrs.

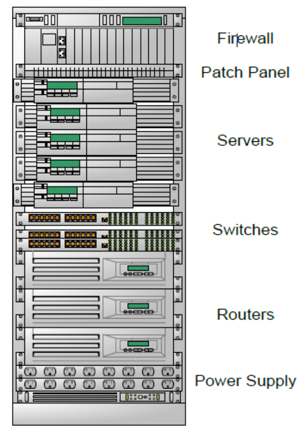
With thesis option:

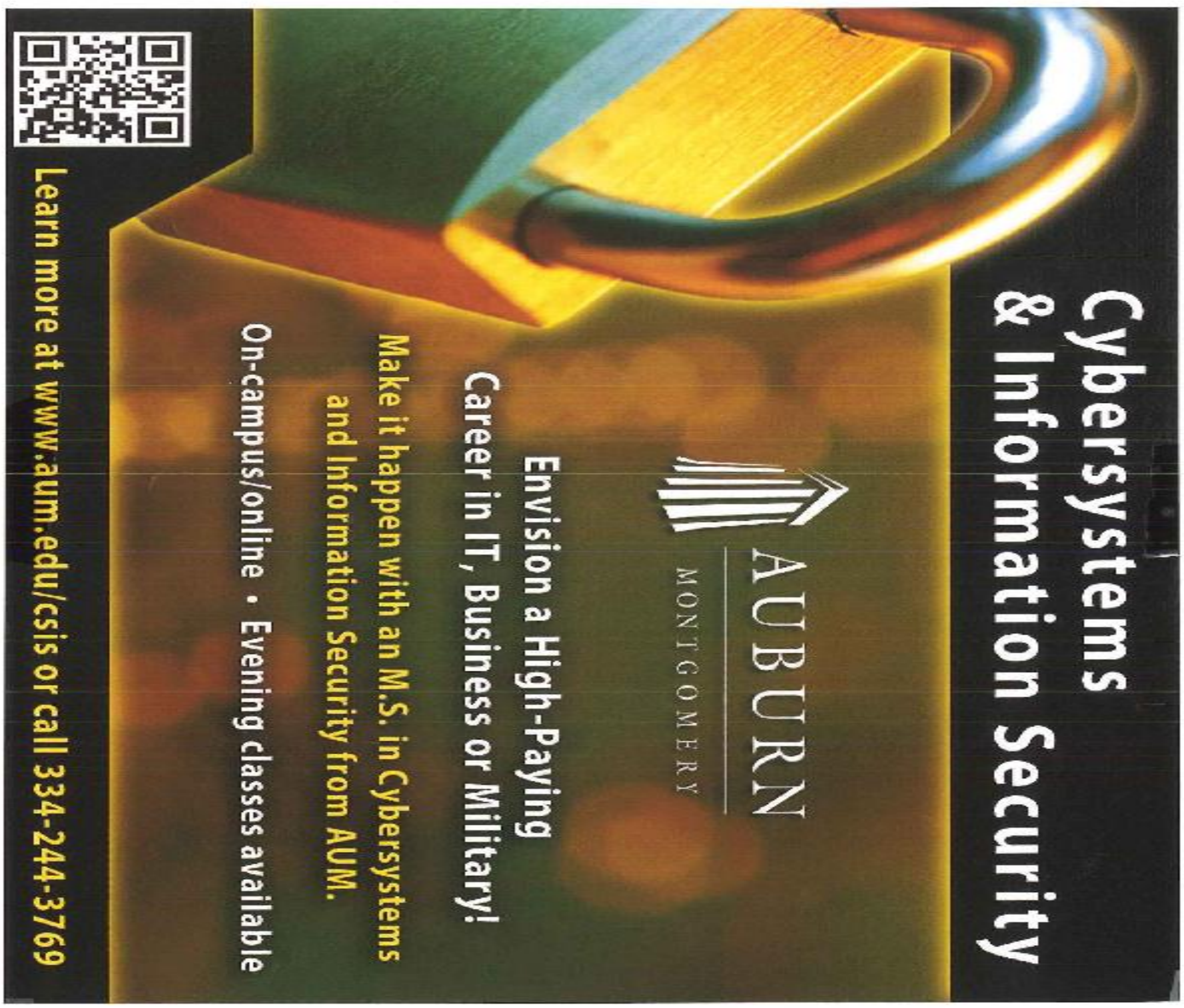
CSIS 6992:	MS Research Thesis, 9 hrs.

Program Director: Mehmet Sahinoglu, Ph.D., 334-244-3769, msahinog@aum.edu

AUBURN MONTGOMERY


S1
External Switch
CISCO 3750
SRV 6
Logging
Server
F2
PIX Firewall
SRV 1
Intrusion
Detection
Server
F1
PIX Firewall
Desktop
R1
CISCO 2500
Router
R3
CISCO 2500
Router
R2
CISCO 2500
Router
S2
CISCO
Switch
S3
CISCO
Switch
Production
Desktops (19)
Lab
Management
Laptops (3)
SRV 2 – SRV 5
Production
Servers (4)


Firewall
Patch Panel
Servers
Switches
Routers
Power Supply


Cybersystems
& Information Security
AUBURN
MONTGOMERY
Envision a High-Paying
Career in IT, Business or Military!
Make it happen with an M.S. in Cybersystems
and Information Security from AUM.
On-campus/online • Evening classes available
Learn more at www.aum.edu/csis or call 334-244-3769

Committee on National Security Systems

and

The National Security Agency

hereby certify that

AUBURN UNIVERSITY at MONTGOMERY

offers a set of courseware that has been reviewed by National Level Information Assurance Subject Matter Experts and determined to meet the National Training Standard for

Information Systems Security Professionals, NSTISSI No. 4011

for

June 2013 - June 2018

Teresa M. Takai
Chair, Committee on National Security Systems

Debora A. Plunkett
Information Assurance
Director

NIETP
National IA Education and Training Program

April 16, 2013

Dr. Mehmet Sahinoglu
Cybersystems and Information Security
Auburn University at Montgomery
P.O. Box 244023
Montgomery, AL 36124-3127

Dr. Sahinoglu:

The Information Assurance Courseware Evaluation (IACE) Program has evaluated your certification application and validated that Auburn University at Montgomery courseware meets all of the elements of the Committee on National Security Systems (CNSS) National Training Standard for:

Information Systems Security (INFOSEC) Professionals, NSTISSI No. 4011

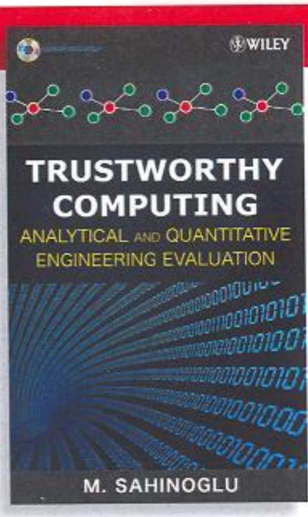
You will receive recognition and an official certificate during the June 2013 CNSS Ceremony, which will be held at the 17th Colloquium for Information Systems Security Education (CISSE).

The IACE Program provides consistency in training and education for the information assurance skills that are critical to our nation. We appreciate your participation in this program, and look forward to seeing you in June.

Lynn Hathaway

Lynn Hathaway
IACE Program Manager

National Information Assurance Education and Training Program (NIETP)
National Security Agency ~ 9800 Savage Road ~ Ft. Meade, MD 20755-6744 ~ ATTN: I084, Suite 6744
(410) 854-6206 ~ FAX (410) 854-4668
askIACE@nsa.gov



TRUSTWORTHY COMPUTING

ANALYTICAL AND QUANTITATIVE ENGINEERING EVALUATION

M. Sahinoglu

ISBN: 978-0-470-08512-7
$110.00 US • $131.99 CAN • £61.50 UK
320 pp.• Includes CD-ROM • September 2007

"The book itself is a commendable achievement, and it deals with the security and software reliability theory in an integrated fashion with emphasis on practical applications to software engineering and information technology. It is an excellent and unique book and definitely a seminal contribution and first of its kind." — C.V. Ramamoorthy

Trustworthy Computing: Analytical and Quantitative Engineering Evaluation presents an index-based, quantitative approach to advances in reliability and security engineering. Objective, metric-oriented, and data-driven, its goal is to establish metrics to quantify risk and mitigate risk through risk management. Based on the author's class-tested curriculum, it covers:

- Fundamentals of component and system reliability and a review of software reliability
- Software reliability modeling using effort-based and clustered failure data and stochastic comparative measures
- Quantitative modeling for security and privacy risk assessment
- Cost-effective stopping rules in software reliability testing
- Availablility modeling using Sahinoglu-Libby (S-L) Probability Distribution
- Reliability block diagramming for Simple and Complex Embedded Systems

Complete with a CD-ROM containing case histories and projects that give readers hands-on experience, this is a great text for students in courses on security, reliability, and trustworthiness, as well as a reference for practicing software designers and developers, computer reliability and security specialists, and network administrators who work with data.

M. Sahinoglu, PhD, is Chair-Professor of the Computer Science Department at Troy University in Montgomery, Alabama. After teaching twenty years at his alma mater (BSEE) Middle East Technical University in Ankara, Turkey, he served as founding dean and department chair in the College of Arts and Sciences at Dokuz Eylül University in Izmir, Turkey. More recently, Dr. Sahinoglu taught at Purdue University, Indiana, and Case Western University, Ohio, before joining Troy University as the university's first Eminent Scholar in Computer Science.

CONTENTS

Preface
Forewords
Chapter 1. Fundamentals of Component and System Reliability, and Review of Software Reliability
Chapter 2. Software Reliability Modeling with Clustered Failure Data and Stochastic Measures to Compare Predictive Accuracy of Failure-Count Models
Chapter 3. Quantitative Modeling for Security Risk Assessment
Chapter 4. Stopping Rules in Software Testing
Chapter 5. Availability Modeling using Sahinoglu-Libby Probability Distribution Function
Chapter 6. Reliability Block Diagramming in Complex Systems

ORDER YOUR COPY TODAY!

Phone
In North America:
1-877-762-2974
In rest of the world:
+44 (0) 1243 779 777

Fax
U.S. Customers:
1-800-597-3299
Outside the U.S.:
+44 (0) 1243 843 296

Mail
John Wiley & Sons, Inc.
Customer Care Center
10475 Crosspoint Blvd.,
Indianapolis, IN 46256

E-Mail
U.S. Customers:
custserv@wiley.com
Outside the U.S.:
csbooks@wiley.co.uk

IEEE   WILEY InterScience® DISCOVER SOMETHING GREAT   1807 WILEY 2007

Subscribe to our FREE Engineering eNewsletter at **www.wiley.com/enewsletters** • **Visit www.wiley.com/engineering**

The Messenger
SERVING TROY & PIKE COUNTY SINCE 1866
Troy, Alabama
Tuesday March 21, 2006

Published Mar 20, 2006 - 22:43:08 CST.

Troy University gets $50,000 grant

By Matt Clower, The Messenger

Troy University has been awarded a $50, 000 grant from Microsoft that will be used to fund courses on information system reliability and security and a cyber-security laboratory.

The grant is one of only 15 awarded by Microsoft to universities through an international competition of 114 other proposals.

The university's Computer Sciences Department submitted a proposal aimed at strengthening and validating an already existing university course on reliability and security, said Mehmet Sahinoglu, Troy eminent scholar and professor of computer science on the Montgomery Campus.

Sahinoglu said the grant puts Troy in an elite class of universities.

"I think this sort of research makes us recognized around the world and really puts us on the map, Sahinoglu said. "This is a big step forward for Troy and truly could not be any better."

The project, funded by a grant from the Microsoft Research Trustworthy Computing Curriculum 2005 Awards, will benefit the university's computer users on the four Alabama campuses, its 62 out-of-state sites and the University's eCampus.

Through the project, a cyber-security laboratory will be developed in collaboration with the Montgomery-based Integrated Computer Solutions, who is partnering with Troy to create a working example of how to create a problem-solving team between the information technology industry and academia.

"We aim to provide our students with collaborative guidance by a local IT firm for hands-on-training through the creation of a cyber-security lab," Sahinoglu said. "This brave endeavor will eventually take Troy University to the establishment of a center of advanced research in computer security and reliability."

Search
Search our archived stories.
(past two weeks)

Go!

Advanced Search
(for stories older than two weeks)

Montgomery Advertiser

David Irvin
Business writer
one (334) 956-0258
((334) 261-1521
Molton St.
ntgomery, AL 36104

Business

8(
Satur
March 1

STOCK REPORT:

Dow Jones:		Nasdaq:		S&P 500:		New York Stock Exchange:		Nasdaq:	
11,076.34	+104.06	2,262.04	+12.32	1,281.58	+9.35	Gainers	2,362	Gainers	1,960
						Losers	952	Losers	1,030

Com
repo

Bottomline

bama honors xporting firms

v. Bob Riley has recog- d eight Alabama firms xcellence in exporting. e value of exports from ama grew by 19 per- in 2005, surpassing the nal growth rate of 10.6 nt, the governor's of- aid in a statement.
e total value of manu- red goods shipped Alabama companies to ountries during 2005 d $10.8 billion, up $9.1 billion in 2004 and illion in 2003.
eight companies:

Troy lab scores Microsoft awa

Troy University will use $50,000 award to create a cyber-security lab

By Erica Pippins
Montgomery Advertiser
epippins@gannett.com

Troy University is among 14 universities from around the world that have earned a prestigious $50,000 Microsoft computing curriculum award for internal and external research.

Troy, along with 114 other institutions, submitted proposals to Microsoft detailing projects in the areas of security, reliability, privacy, business integrity and secure software engineering.

The university will use its award to create a cyber-security lab where computer science majors learn to develop secure and reliable information technology systems, said grant writer Mehmet Sahinoglu.

"This brave endeavor will eventually and gradually take us to the establishment of a center of advanced research in computer security and reliability at Troy University," said Sahinoglu, who heads up the computer science department at Troy's Montgomery campus.

"It will create a future powerhouse for our academia and greater community," Sahinoglu said.

Stephen Goldsby, CEO of Integrated Computer Solutions Inc. in Montgomery, is collaborating with the university to develop the cyber-security lab.

ICS provides operations support for mainframe, midtier and enterprise networks.

"It's not surprising that this grant was awarded in Montgomery," Goldsby said. "We have a strong university system and a strong information technology base because of the work done at Maxwell-Gunter Air Force Base. All the necessary tools are in place for a top-notch research project in this area."

Goldsby's company is donating equipment for the hands-on troubleshooting lab.

It will be used to simulate complex networks where security and privacy are essential, including those found in banks ment and law agencies.

The group a vide technical s
"I really bel project because search could ha ty to aid us i ness," Goldsby s
Sahinoglu ag
"This is the an even harder execute the pr noglu said. "Bu we can carry greater heights.

Merger marks Internet era

Analyst believes all media will come through Web

Montgomery Advertiser
6B
Monday
Jan. 17, 2000

By Denise Barkhalter
Montgomery Advertiser

The Jan. 10 marriage of the youthful and stock market energetic America Online Inc. and the staid but sound Time Warner Inc. may have put a sense of wonder in the hearts of many PC users.

The merger jolted the stock market when AOL Chief Executive Officer Steve Case and Gerald Levin, chief executive of Time Warner Inc., made the announcement.

AOL's stock was down 13 percent, while Time Warner's stock rose more than $25 the first day. Thursday, AOL and Time Warner each rose more than $1.

This past week has raised questions — among AOL's 20 million subscribers and Time Warner's millions who subscribe to its magazines and cable service — about whether the same to compete and succeed in emerging media can be kept.

Troy State University Montgomery Eminent Scholar Mehmet Sahinoglu of the computer and information science department gives us his analysis of the merger, expected to close in a year.

Q. How long have you been at TSUM?

A. Four months.

I understand you've done an interview with National Public Radio?

Yes. I was interviewed about AOL-Time Warner. It will air Jan. 19 on NPR 89.9 at 12:20 p.m.

What is so sensational about the AOL-Time Warner merger?

It's the largest Internet mediamerger of all time. The second largest was MCI World Com-Sprint merger, and that was $115 billion. Third in line was Exxon-Mobil, which was $79 billion. Other hits were Travelers-Citicorp, $73 billion and Bell-Atlantic, $55 billion, to name a few. AOL paid $183 billion to buy out Time-Warner and recently $10 billion to acquire Compuserve. CEO of AOL Steve Case owns 9 million AOL shares worth $650 million.

What's your interpretation of what the AOL/Time Warner marriage means?

First, it means the future belongs to Internet, that is, all media broadcasting will be conducted on the Internet. Secondly, the traditional hardware-dominated media, like television and the press, accepts the superiority of the software-dominated net. Finally, the Internet is being seen as a lucrative platform to conduct business on. No one expected Internet to buy out the media this fast.

But what can Time-Warner, with its media-focus, do for AOL, with its focus on the Internet?

They will continue to advertise each other's products. For example, AOL users will hear free music at least in the beginning for promotional reasons by Time Warner networks. AOL will, for example, popularize Time Warner products like Roadrunner, and Time Warner will promote AOL's own Digital City, Instant Messenger. Also, CNN news will be broadcast in the AOL news channel.

We're talking about healthy, robust companies

scribers, 2 million of which was from their newly acquired asset, Compuserve. AOL made the headlines when they distributed to every household in the USA their AOL subscription disks for a comical $19.95 each for unlimited use. They also had previously bought Netscape and ICQ. AOL had $4.8 billion in revenue and 12,000 employees. Profits were $760 million.

On the other hand, Time Warner has assets like the news channel CNN and cable channels, HBO, TNT, Cartoon Network, and with magazines like *Time, People, Sports Illustrated, Fortune, (Southern Living* in Alabama). Last but not least is TW's entertainment industry, such as Warner Music, WB network, Looney Tunes. It had 68,000 employees with revenues amounting to $14.6 billion but only a $168 million profit.

AOL is the new kid on the block and Time Warner has an established history. Was Time Warner losing ground in today's market?

Time was first established by Luce and Britton Hadden brothers in 1923. They sold 1 million *Time* magazines in 1940 and 4.5 million in 1980. When Jack Warner, a film production company giant, joined or bought Time in 1989, most of the corporate energy is said to have been consumed for resolving internal problems Warner created. Hence the profit share dropped drastically. However, this is refuted by Gerald Levin, ex-CEO of Time Warner. He said they simply had to change with the changing times to be more efficient.

What will this merger mean for PC users?

An Internet user nowadays with the existing technology uses a maximum of 56 kilobytes per second to get a one page per second transmission. Now, you normally can't get cable TV or musical programs over the Internet that fast. Therefore, with the merger, one will be able to get, in one second, not only the information, but also the audio-visual entertainment or communication. I even suspect that the telephone companies will not know what to do with themselves if such mergers can incorporate the visual telephone conversations on their Internet frame. You know, electronics engineers as early as 1990s did foresee a multimedia revolution happening soon, where the subscriber will receive everything from TV to radio to audio-video communications, such as visual teleconferencing, by plugging into the wall only once.

So, students, for example, could not only watch professors on real-time television, but they could also e-mail or have audio-communications with that professor, as well?

Yes. Distance learning is going to be fortified and strengthened and will also become faster and better if AOL-Time Warner can make this happen.

Before, distance learning was watching a professor lecture on a television screen or reading material online. With the two combined, a student can listen to the professor and send an e-mail if a ques-

The Associated Press

Steve Case, America Online's chairman and CEO, left, Time Warner's chairman and CEO, Gerald Levin, and vice chairman of Time Warner, Ted Turner, applaud Robert Pittman, president and chief operating officer of America Online, not shown, during a Jan. 10 news conference after the AOL, Time Warner merger announcement.

Todd Van Emst/Staff

Troy State University Montgomery Eminent Scholar Mehmet Sahinoglu has been with the computer and information science department for four months.

cally be there, but will instead be in a virtual classroom.

Of course, no matter how many of these new advances we have in technology, the most efficient medium for instruction is the university itself.

You've coined a phrase in all of this?

Yes. Net wars. You've heard of Star Wars, these are the Net wars.

So what's next in the Net wars?

Of course, the competition has heated up profoundly. Microsoft, with 3 million subscribers to Internet, has already entered into a ...

in the range of $3 million.

However, the AOL merger is facing up front with the latest move. AOL and Microsoft were already rivals. So were and still be Steve Case and Bill Gates. Please do not forget the restless Yahoo with 35 percent of the Internet market who is looking for a merger. There aren't a few TV giants still left.

If Microsoft is such a monopoly, why is the government allowing this merger to take place?

That's a legal question, and I would be afraid to try to answer that. I know the Microsoft monopoly ruling came from a court case. This is a merger, and as of yet, there's

EMINENT SCHOLAR

- **Name:** Mehmet Sahinoglu
- **Title:** Serving as Troy State University Montgomery's first eminent scholar of computer and information science.
- **Age:** 48
- **Education:** bachelor's from Middle East Technical University, master's from University of Manchester England, ph.D from Texas A&M
- **Born:** Izmir, Turkey
- **Family:** Suna, wife, and sons Hankan, 4, Efe, 13, and Turk, 15

...ing times for PC and Internet consumers?

And frightening times. We're relying more and more on a single source of communication, our computers. Because power companies in the USA have done a superb job in providing continuous and reliable energy to their customers, subscribers can utilize this blessing in software and telecommunications cheaply.

Without electric power, no matter how much you can endure for a few hours with uninterrupted power supply, you cannot continue to do so indefinitely. No power means no Internet, no TV or software or hardware.

I also wish these Internet companies can spend some effort on reliability and security questions, such as: What do I do when my power is cut off due to a blackout? How can I be 100 percent certain that a hacker will not confiscate my credit card number?

Do you have other concerns about the promise of one communications device?

Yes, concerns about bodily and mental health. More suffering from necessarily sitting in front of terminals leading to severe spinal and arthritis or weight problems due to lack of correct posture in part and also to lack of exercise. These major corpor-

Turner

"This will be exciting and challenging and a lot of fun. I did it with as much excitement as I did when I first made love some 42 years ago."

—Ted Turner, Time Warner vice chairman

Levin

"This really completes the digital transformation of Time Warner. These two companies are a natural fit."

—Gerald Levin, Time Warner chairman

Parsons

"This is a defining event for Time Warner and America Online as well as a pivotal moment in the unfolding of the Internet age."

—Richard Parson...

TROY STATE UNIVERSITY MONTGOMERY

MEMORANDUM

TO:	Mr. Bob McGough Education Services Officer
FROM:	Chuck Durham Interim Dean, Business
SUBJ:	CIS Eminent Scholar
DATE:	August 11, 1999

TSUM names eminent scholar

Troy State University Montgomery recently named Mehmet Sahinoglu as its first Eminent Scholar of Computer Information Science.

His career includes the reputation as one of the world's leading authorities on power system reliability and computer software reliability and dependability engineering.

Sahinoglu has also been recognized as the founding dean of the college of arts and sciences and head of the department of statistics at Dokuz Eylul University in Turkey. He has recently taught at Case Western Reserve and Purdue universities.

This is follow-up to our discussion last week. Dr. Mahmet Sahinoglu will become our CIS Eminent Scholar/Department Chair on September 1, 1999. He is extremely qualified to assume this position and will continue to move the CIS program forward. With his contacts and experience, we look forward to filling other CIS positions in the not too distant future.

As soon as Dr. Sahinoglu settles in, we will get on your calendar for an introduction. I agree that we should have a formal reception for him - and we'll seek input from you on appropriate Maxwell/Gunter invitees.

Thanks for your support and effort in our behalf, Bob.. I look forward to seeing you again soon.

cc: Dr. Jim Sutton

montgomeryadvertiser.com

August 19, 2008

AUM names Informatics Institute director

Mehmet Sahinoglu has been named distinguished professor and director of Auburn Montgomery's Informatics Institute.

As director, Sahinoglu will develop and manage new undergraduate and graduate programs in information science and establish the institute as a focal point for research in information technology, according to a news release from AUM.

"The institute provides a tangible way the university can support the mission of the 754th Electronic Systems Group and Alabama's bid to make Montgomery the home of the U.S. Air Force Cyber Command," said AUM Chancellor John Veres.

Sahinoglu comes to Auburn Montgomery from Troy University, where he served as eminent scholar and chairman of the Computer Science Department on Troy's Montgomery campus, the release states. He holds a bachelor's degree in electrical and computer engineering from Middle East Technical University, a master's degree in electrical engineering from the Institute of Science and Technology -- University of Manchester, and a doctorate in electrical engineering and statistics from Texas A&M University.

-- *Staff report*

OPERATING CONSIDERATIONS IN GENERATION RELIABILITY MODELING-AN ANALYTICAL APPROACH

A. D. Patton C. Singh M. Sahinoglu
Electric Power Institute
Texas A&M University
College Station, Texas

Abstract - The paper presents a new analytical approach to the calculation of generating system reliability indices. The new approach makes it possible to relax idealizing assumptions and to explicitly model the effects of operating considerations such as: (1) unit duty cycles reflecting load cycle shape, reliability performance of other units, unit commitment policy, and operating reserve-policy; (2) start-up failures; (3) start-up times; and (4) outage postponability. The models presented can also be used to consider the effects of basic energy limitations and to give production cost estimates.

INTRODUCTION

Analytical methods for generation reliability modeling generally assume the generating units independent of each other and the load. This means that the generating units are assumed to run continuously unless on forced or scheduled outage. Also the conventional methods and models do not recognize operating considerations and constraints such as spinning reserve policy, generator start up time and outage postponability. Recent simulation studies [1], however, indicate that these factors have considerable effect on computed reliability indices. It is, therefore, important that operating considerations and constraints be incorporated into analytical modeling to more closely reflect physical reality. Some attempts [2, 3] have been made in this direction by including start up failure probabilities and recognizing that except for the base-loaded units, other generators do not run continuously. These models, however, assume *a priori* a fixed duty cycle for peaking and cycling units which is not directly a function of the system being studied. Thus, existing models cannot reflect the effects of changes in unit duty cycles due to changes in: operating reserve policy, unit commitment priority, load cycle shape, and reliability characteristics of other system units. Further, existing models do not include the effects of start-up delays and outage postponability.

This paper presents improved models and methodology to reflect the individual duty cycle of each unit and also represent the effect of start up delays and outage postponability. The results obtained by these models for an EPRI synthetic system have been compared with those using Monte Carlo simulation and good agreement has been obtained.

The expected operating hours of each generating unit can be found using the methodology outlined in this paper. The approach, therefore, appears useful as a production cost model and also provides a means of considering basic energy limitations for each unit.

Paper A 80 082-3, recommended and approved by the Power System Engineering Committee of the IEEE Power Engineering Society for presentation at the IEEE/PES 1980 Winter Meeting, February 3-8, New York, NY. This paper was recommended for TRANSACTIONS status F 80 SM 690 8, and presentation by title for written discussion at the IEEE/PES 1980 Summer Meeting, July 13-18, Minneapolis, MN. Manuscript submitted August 28, 1979; made available for preprinting May 1, 1980. This paper has been published in 1980 Winter Meeting Text of Abstract Papers. Discussion and closure for A 80 082-3 have been published in 1980 Winter Meeting Bound Volume of Discussion and Closures.

GENERATION RELIABILITY MODELING

A brief review of generation reliability modeling concepts is presented as these concepts are essential for the understanding of the new material described in the paper. Traditionally, generating capacity reliability studies are performed by building generating capacity and load models and then combining them to calculate the probability and frequency of capacity deficiency. The relevant expressions [4] for the indices relating to margin M are given by (1)-(3).

$$P(M) = \sum_{X} p_g(X)\, P_\ell\,(C-X-M) \tag{1}$$

$$f(M) = \sum_{X} p_g(X)\, \{[\rho_{C+}(X) - \rho_{C-}(X)]\, P_\ell\,(C-X-M) + f_\ell\,(C-X-M)\} \tag{2}$$

and

$$D(M) = P(M)/f(M) \tag{3}$$

where

- $P(M)$, $f(M)$, $D(M)$ = probability, frequency and mean duration of margin less than or equal to M.
- $p_g(X)$ = probability of capacity outage equal to X.
- $P_\ell(C-X-M)$, $f_\ell(C-X-M)$ = probability and frequency of load greater than or equal to (C-X-M).
- C = installed capacity minus capacity on scheduled outage.
- $\rho_{C+}(X)$, $\rho_{C-}(X)$ = departure rates from capacity outage state X to states with more or less available capacity respectively.
- $\sum_X$ = summation over exact capacity outage states X.

The cumulative characteristics of load, $P_\ell(\cdot)$ and $f_\ell(\cdot)$ are derived by scanning the hourly load values. The generation system values of $p_g(X)$ and $\rho_{C\pm}(X)$ are determined by successively adding the generating units and utilizing relationships (4)-(6). The expressions (4)-(6) are for a three-state model shown in Figure 1, in which the transition rates between the derated and failed states are ignored for simplicity.

$$p_g(X) = p_g'(X)\ AV + p_g'(X - C_T)FOR + p_g'(X - C_D)DFOR \tag{4}$$

PROBABILITY DISTRIBUTION FUNCTIONS FOR GENERATION RELIABILITY INDICES - ANALYTICAL APPROACH

Mehmet Sahinoglu
Department of Applied Statistics
Middle East Technical University, Turkey

M. T. Longnecker L. J. Ringer
The Institute of Statistics

C. Singh A.K. Ayoub
Electrical Engineering

Texas A&M University, College Station, Texas

Abstract - The primary objective of this research is to analytically develop probability density functions (p.d.f.) for the widely used power generation reliability indices, Loss of Load and Unserved Energy. The equations to calculate the parameters of the distributions of these indices upon a prescribed load plan are derived. In order to develop the theoretical structure for the problem stated, classical and decision theoretic (Bayesian) statistical inference are used as major tools along with the univariate and multivariate asymptotic theory. Consequently, an approximate numerical multiple integration scheme is employed to compute the parameters of the asymptotic normal densities of the reliability indices for the sample power networks. The authors believe that this statistical approach offers a more realistic alternative to the conventional reliability evaluation in generation systems; that is, to the calculation of an averaged value for the Loss of Load and Unserved Energy where outage data is traditionally assumed to be deterministic with certainty.

INTRODUCTION

In the past decade or two, a number of techniques have been developed [2-9] for calculating the various measures of the reliability performance of the generating systems in power networks. In all these methods, invariably outage data are presupposed to be deterministic, and thus the reliability index calculated is quoted as one number. The past history collected for a generating unit is often inadequate, and is a mixture of accurate and inaccurate data. Thus any computational scheme based on such a historical record is subject to error propagation in the computation of reliability indices. The awareness of the need for information related to the variation of the reliability index around its mean has been recently investigated [10-18], by primarily employing various algebraic expansion techniques such as Taylor's series to approximate the expected value and variance of the index without any statistical (analytical) closed-form representation. This paper, however, is an endeavor to extend the work in this area by obtaining the asymptotic distributions of the two well-known reliability indices so as to more realistically represent the behavior of the system reliability performance.

The contribution of this paper is in developing a statistical closed-form density function for the random variables of interest, Loss of Load index (in hours) and Unserved Energy index (in Megawatt-Hour). The paper also establishes a theoretical frame work which may be used in similar analysis. This paper, however, is not concerned with analyzing the data of any particular system. The paper also presents a computerized algorithm in FORTRAN IV digital programming language for estimating the parameters of these distributions.

Uni- and multivariate distribution theory, in terms of both classical and Bayesian inferences are the basic tools in building the theoretical structure for the probability density functions of the Loss of Load and Unserved Energy indices. Appropriate limiting arguments inherent in most power networks are utilized. As a computational method to implement the developed algorithm, a numerical multiple integration technique is applied for satisfactory convergence. The algorithm is exemplified by applying it to several generation networks.

82 JPGC 603-9 A paper recommended and approved by the IEEE Power System Engineering Committee of the IEEE Power Engineering Society for presentation at the 1982 IEEE/ASME/ASCE Joint Power Generation Conference, October 17-21, 1982, Hilton Hotel, Denver, Colorado. Manuscript submitted December 10, 1981; made available for printing August 30, 1982.

WHY DENSITY FUNCTIONS?

Though the mean and variance of indices provide useful information, the density function completely characterizes the behavior of these indices. The density functions are especially useful when the effects of Loss of Load and Unserved Energy index are nonlinear.

Error propagation in reliability computations because of outage data uncertainty can be indicated by quoting confidence intervals for the indices. These intervals can be obtained by appropriate manipulations of the distribution functions. Furthermore, in power generation planning, the comparison of several alternatives can be made by examining the average value of reliability indices. The distribution of the indices must be known in order to conduct statistical tests of hypothesis concerning the average value of the indices.

LOSS OF LOAD AND UNSERVED ENERGY

The well-accepted Loss of Load Probability (L.O.L.P.) index expresses the probability of the capacity on forced outage exceeding the reserve capacity in the generation system for a defined period of study. The L.O.L.P., multiplied by the period of study gives the expected number of hours in which capacity deficiencies exist in a single area network (not interconnected with others). As a useful complementary measure to L.O.L.P., the Unserved Energy indicates the expected magnitude of loss of energy in Mw-hr for the given period of study. The following notation will be used throughout, for which reader is referred to Fig. 1.

TOTCAP $\triangleq$ the total installed capacity of the generating system

$L_j \triangleq$ the peak system load forecast constant for hour j. (No forecast errors assumed)

$M_j \triangleq$ sum of capacities for generating units on planned outage (maintenance and/or shut down) for hour j.

$R_j \triangleq$ the system reserve capacity for hour j $\triangleq [(\text{TOTCAP} - M_j) - L_j]$,

$X \triangleq$ system capacity or forced outage (ignoring maintenance and shutdown hours) where outage cannot be postponed beyond the next weekend.

$e_j(x) \triangleq$ Energy in Mw not supplied given capacity on forced outage is x at hour j.
$\triangleq [L_j - (\text{TOTCAP} - M_j - X)]$

[23] J.O. Berger, Statistical Decision Theory, Springer-Verlag, New York, Heidelberg, Berlin, 1979.

[24] C.R. Rao, Linear Statistical Inference and Its Applications, John Wiley & Sons, Inc., New York, New York, 1973.

[25] R.J. Serfling, Approximation Theorems of Mathematical Statistics, John Wiley & Sons, Inc., New York, New York, 1980.

Mehmet Sahinoglu was born on June 23, 1951 in Izmir, Turkey. He received a B.S. degree in Electrical Engineering from Middle East Technical University (M.E.T.U.) in Ankara, Turkey in 1973. He then completed his M.Sc. degree in Power Systems Engineering at U.M.I.S.T., in Manchester, England in 1975 on British Council Scholarship. Upon his return to Ankara, he worked as a Reliability Engineer in the Turkish Electricity Authorities (T.E.K.) and taught in the Department of Applied Statistics at M.E.T.U. in Ankara. He joined the Institute of Statistics of Texas A&M University in August of 1977, and worked as a research assistant on Reliability Projects with Electric Power Institute and taught statistics. Mr. Sahinoglu, who is on leave of absence from M.E.T.U., Ankara, and a member of IEEE, recently received a Ph.D. degree in Statistics in December of 1981.

Michael Longnecker is an assistant professor of Statistics at Texas A&M University. Prior to joining the Institute of Statistics in 1977, he taught for one year in the Department of Statistics, Florida State University. He obtained his B.S. in Mechanical Engineering in 1968 and then worked as a pipeline engineer for Shell Oil Company prior to obtaining his M.S. and Ph.D. in statistics in 1976. He has written several papers in which the effects of dependent data on the strong law of large numbers and optimal stopping rules were studied. He currently is working on the analysis of survival curves from paired data and the modeling of power systems in which there is dependency between individual generator failures.

Larry J. Ringer was born in Cedar Rapids, Iowa, on September 24, 1937. He received a B.S. in Math (1959) and M.S. in Statistics (1962) from Iowa State University and a Ph.D. in Statistics (1966) from Texas A&M University. He is currently a Professor and Associate Director of the Institute of Statistics, Texas A&M University. His research interests are in applied statistics and reliability. Dr. Ringer is a member of the American Statistical Association, American Society of Quality Control and Sigma Xi.

Chanan Singh is an associate professor of Electrical Engineering at Texas A&M University. He has been active in the reliability field, primarily in areas of electric power systems and urban transportation systems (conventional and advanced technology), for several years. He has published numerous papers and is a coauthor of the book "System Reliability Modelling and Evaluation", with Dr. R. Billinton and of "Engineering Reliability: New Techniques and Applications", with Dr. B.S. Dhillon. He is on the editorial advisory board of Microelectronics and Reliability and is a registered professional engineer with the province of Ontario.

A.K. Ayoub (SM'79) was born in Kom-Hamada, Egypt, on September 3, 1927. He received the B.Sc. degree in electrical engineering from the University of Alexandria, Egypt, in 1948, and the M.Sc. and Ph.D. degrees from the University of Texas, Austin, 1952 and 1955, respectively. He attended the Kurchatov Atomic Energy Institute, Moscow, in 1963 and the Reactor School at the Harwell Atomic Energy Research Establishment, United Kingdom, in 1965.

From 1955 to 1962 he was with the Ministry of Public Works, Cairo, Egypt. In 1962 he joined the U.A.R. Atomic Energy Establishment and was Deputy Director of their Nuclear Power Division until 1968. Since then he has been with the Electric Power Institute of Texas A&M University, College Station. His field of research is power system security.

Dr. Ayoub is a member of Eta Kappa Nu and Tau Beta Pi and Sigma Xi. He is a registered professional engineer in the State of Texas.

The Limit of Sum of Markov Bernoulli Variables in System Reliability Evaluation

Mehmet Sahinoglu, Member IEEE
Middle East Technical University, Ankara

Key Words — **Markov Bernoulli variable, Compound Poisson Process, System reliability**

Reader Aids —
Purpose: Widen the state of art
Special math needed for derivations: Probability, Stochastic processes
Special math needed to use results: Same
Results useful to: Theoreticians, Reliability analysts

Summary & Conclusions — **For 2-state maintainable and repairable systems modeled by nonstationary Markov chains, a limiting compound Poisson distribution is derived for the sum of Markov Bernoulli random variables. The result is useful for estimating the distribution of the sum of negative-margin hours in a boundary-crossing scenario regarding any physical system with inter-arrival times of system failures that are negative-exponentially distributed, where the positive- and negative-margin states denote desirable and undesirable operating conditions. Three test cases from the IEEE Reliability Test system are analyzed.**

The mean and variance/mean ratio are generated for each case (the unity ratio denotes a pure Poisson process). The basic result of compound Poisson distribution estimation for the sum of Markov Bernoulli random variables with varying probabilities contributes to solving the problem of estimating the distribution of the popular reliability index (cumulated loss-of-load hours) in large electric-power generation systems, where the hourly load demand varies. The compound Poisson process is a consequence of the counting process for the negative-margin hours accumulated at each system-breakdown. The Markov (non-ageing) property of the compound geometric distribution confirms the initial Markov Bernoulli assumption as well as the Markov property of the inter-arrival times of the system breakdown or failure. Thus, it is no coincidence that the limiting distribution is a sum of Markov Bernoulli variables resulting in a geometric Poisson distribution.

The derivation of the mean and variance of the compound Poisson distribution, in a physical 2-state maintainable and repairable system with the defined boundary-crossing scenario, for the limiting sum of Markov Bernoulli r.v.'s, contrary to a previous Markov binomial assumption is new. The capacity to infer the proposed compound Poisson distribution through the mean and variance/mean ratio and using the compound Poisson tables is an additional convenience. Such a procedure is necessary in large asymptotic system studies, such as in the electric power networks with variable success probabilities for the Markov Bernoulli random variable.

1. INTRODUCTION

The sum of a Markov Bernoulli sequence with non-constant probability of success is studied. The result is a compound Poisson distribution where the compounding distribution is geometric. The motivation lies in the derivation of the compound Poisson parameters for the sum of Markov Bernoulli variables in the event of non-constant success probabilities rather than in the Markov binomial assumption of constant success probability [3]. Such properties are inherent in some large systems with asymptotic solution, as in electric-power generation systems investigated for a long period, eg, one year. An IEEE Reliability Test System [6] is used as an example implementation.

2. NOTATION

- Y_i — Non-independent (nonstationary) and non-identical Markov Bernoulli r.v.; $i = 1, \ldots, n, \ldots, N$; 0 = success, 1 = failure
- P_i, Q_i — success, failure probability of Y_i
- $\bar{\ }$ — implies an average over $i = 1, \ldots, N$
- P — success probability for Markov binomial r.v. in stationary case
- Q — failure probability for Markov binomial and/or geometric r.v.
- π — auto-correlation coefficient of Y_i, Y_{i+1}
- P_{jk} — probability of being in state k, given that the Markov chain started at state j
- S_n — sum of Y_i over $i = 1, n$; it is a compound Poisson r.v.
- q — variance/mean for S_n
- x, or x_n, x_n — number of demands by customer n or the number of cars involved in car accident n; geometric r.v.'s
- Ω — arrival rate for geometric Poisson r.v. x; mean of x.
- pgf — probability generating function
- s — Laplace (dummy) variable for pgf
- $f^{W*}(x)$ — W-fold convolution of $\{f(x)\}$; eg, probability of W customers placing a total of x demands. $f^{W*}(1) = 1$.
- $0(1/n)$, $0''(1/n)$ — zero functions that go to zero as n goes to infinity
- TOTCAP — installed total capacity for an isolated electric-power generation system
- L_i — load forecast at each discrete hour i
- X — unplanned forced outage, r.v.
- m_i — power margin at hour i; TOTCAP-X-L_i
- U_N — unavailability index, sum of negative margin hours in the power system; S_n for $n = N$
- MTTF, MTTR — Mean time to failure, repair for a generating unit

Other, standard notation is given in "Information for Readers & Authors" at the rear of each issue.

0018-9529/90/1000-0046$01.00©1990 IEEE

REFERENCES

[Bie 89] J. M. Bieman, J. L. Schultz: "Estimating the number of test cases required to satisfy the All-du-paths testing criterion", *3rd IEEE Symposium on Software Testing, Analysis and Verification*, Key West, USA, December 1989, pp. 179-186.

[Cla 89] L. A. Clarke et al.: "A formal evaluation of data flow path selection", *IEEE Transactions on Software Engineering*, Vol. SE-15, No. 11, November 1989, pp. 1318-1331.

[Cur 86] P. A. Currit, M. Dyer, H. D. Mills: "Certifying the reliability of software", *IEEE Transactions on Software Engineering*, Vol. SE-12, No. 1, January 1986, pp. 3-11.

[DeM 87] R. A. DeMillo et al.: "Software testing and evaluation", *The Benjamin/Cummings Publishing Company, Inc.*, Menlo Park (CA), USA, 1987.

[Dur 84] J. W. Duran, S. C. Ntafos: "An evaluation of random testing", *IEEE Transactions on Software Engineering*, Vol. SE-10, No. 4, July 1984, pp. 438-444.

[Fra 88] P. G. Frankl, E. J. Weyuker: "An applicable family of data flow testing criteria", *IEEE Transactions on Software Engineering*, Vol. SE-14, No. 10, October 1988, pp. 1483-1498.

[Gad 89] J-Y. Gadeau: "Analyse des performances du test statistique de logiciel", *Student Project*, Laboratoire d'Automatique et d'Analyse des Systèmes, Toulouse, France, June 1989.

[Gir 73] E. Girard, J-C. Rault: "A programming technique for software reliability", *1st IEEE Symposium on Computer Software Reliability*, New York, USA, 1973, pp. 44-50..

[Gir 86] M. R. Girgis, M. R. Woodward: "An experimental comparison of the error exposing ability of program testing criteria", *1st Workshop Soft.Testing*, Banff, Canada, July 1986, pp. 64-73.

[Gou 83] J. S. Gourlay: "A mathematical framework for the investigation of testing", *IEEE Transactions on Software Engineering*, Vol. SE-9, No. 6, November 1983, pp. 686-709.

[Ham 86] D. Hamlet: "Testing for probable correctness", *1st IEEE Workshop on Software Testing*, Banff, Canada, July 1986, pp. 92-97.

[Ham 89] R. Hamlet: "Theoretical comparison of testing methods", *3rd IEEE Symposium on Software Testing, Analysis and Verification*, Key West, USA, December 1989, pp. 28-37.

[Her 76] P. M. Herman: "A data flow analysis approach to program testing", *Australian Comput. Journal*, Vol. 8, No. 3, November 1976, pp. 92-96.

[How 75] W. E. Howden: "Methodology for the generation of program test data", *IEEE Transactions on Computers*, Vol. C-24, No. 5, May 1975, pp. 554-559.

[How 77] W. E. Howden: "Symbolic testing-design techniques, costs and effectiveness", *NTIS PB-268518*, May 1977.

[Lap 89] J-C. Laprie: "Dependability: a unifying concept for reliable computing and fault tolerance", Chapter 1 in "Dependability of resilient computers" (Ed. T. Anderson), *BSP Professional Books*, UK, 1989, pp. 1-28.

[Lap 90] J-C. Laprie: "Dependability: basic concepts and associated terminology", *PDCS Project First Year Report (ESPRIT Project 3092)*, Volume 1, Chapter 1, May 1990.

[Mor 78] P. B. Moranda: "Limits to program testing with random number inputs", *COMPSAC'78*, Chicago, USA, November 1978, pp. 521-526.

[Nta 84] S. C. Ntafos: "On required element testing", *IEEE Transactions on Software Engineering*, Vol. SE-10, No. 6, November 1984, pp. 795-803.

[Nta 88] S. C. Ntafos: "A comparison of some structural testing strategies", *IEEE Transactions on Software Engineering*, Vol. SE-14, No. 6, June 1988, pp. 868-874.

[Rap 85] S. Rapps, E. J. Weyuker: "Selecting software test data using data flow information", *IEEE Transactions on Software Engineering*, Vol. SE-11, No. 4, April 1985, pp. 367-375.

[The 89] P. Thévenod-Fosse: "Software validation by means of statistical testing: retrospect and future direction", *Int. Working Conference on Dependable Computing For Critical Applications*, Santa Barbara, USA, August 1989, pp. 15-22.

[Wey 90] E. J. Weyuker: "The cost of data flow testing: an empirical study", *IEEE Transactions on Software Engineering*, Vol. SE-16, No. 2, February 1990, pp. 121-128.

[Zei 88] S. J. Zeil: "Selectivity of data-flow and control-flow path criteria", *2nd IEEE Workshop on Software Testing, Verification and Analysis*, Banff, Canada, July 1988, pp. 216-222.

A Bayes Sequential Statistical Procedure for Approving Products in Mutation-Based Softwar Testing

Mehmet Şahinoğlu *

Department of Statistics

Mathematical Sciences Building

Purdue University

West Lafayette, Indiana 47907

xnse@vm.cc.purdue.edu

Eugene H. Spafford

Software Engineering Research Center

Department of Computer Science

Purdue University

West Lafayette, Indiana 47907

spaf@cs.purdue.edu

Abstract

Mutation analysis is a well-studied method of measuring test-case adequacy. Mutation analysis involves the *mutation* of a program by introduction of a small syntactic change in the software. Existing test data sets are then executed against all these *mutant programs*. If the test data set is adequate for testing the original program, it will distinguish all of the incorrect mutant programs from the original program. As an ad-hoc procedure, a stopping criterion is conventionally based on a given "Y% of the mutants to be distinguished" with a certain "confidence level of X%" over a multiplicity of random test cases.

Alternatively, we propose a Bayes sequential procedure for testing $H_0 : p = p_1$ (acceptable fraction of live mutants to demonstrate good quality) vs. $H_A : p = p_2$ (unacceptable fraction of live mutants to demonstrate bad quality). This derives a sequential probability ratio testing (SPRT) that is the most economical sampling scheme with given prior probabilities, decision and sampling cost functions. The implementation of our proposed method on a sample program shows the cost effectiveness of the new technique as compared to the current, deterministic approach, which was not structured by statistical hypothesis testing.

Currently visiting Purdue University from Middle East Technical University (METU), Ank Turkey on a Fulbright Scholarship, support which is gratefully acknowledged.

PD-Vol. 47-1, Engineering Systems Design and Analysis
Volume 1
ASME 1992

ESTIMATION OF TOTAL GOOD OPERATING-LIFE IN k-out-of-n PARAMETER DEPENDENT NETWORKS

Mehmet Şahinoğlu
Department of Statistics
Middle East Technical University
Ankara, Turkey

Derya Güven
Department of Statistics
Texas A&M University
College Station, Texas

ABSTRACT

The reliability estimation of a k-out-of-n network is analytically derived, and satisfactorily supported by Monte Carlo Simulation in a situation when the constituting units are not independent but parameter-dependent like in a computer networks. A (k+1)-parameter version of the MVE distribution is used for the parameter-dependent failures of k-units with unequal failure rates α_i and $(k+1)^{th}$ dependency rate α_0. The primary concern is to transform a k-out-of-n PD network into an equivalent 1-out-of-n:G PD network by enumerating the success paths or tie-sets, and then, to determine the reliability function by employing the principles of a parallel redundant (standby) network.

NOTATION AND BASIC ASSUMPTIONS

I input (stimulus)

O output (response)

n number of units (components)

k number of units in each success path (tie-set)

N Total number of simulations

$m \begin{pmatrix} n \\ m \end{pmatrix}$ number of success paths

α_{ji} rates of independently distributed exponential random variables

U_{ji} an independent shock *i.e.*, time to failure for unit located on the path $j = 1, .., m$ for serial $i = 1, ..., k$ destroying unit ji which is exponentially distributed with parameter α_{ji}, α_{j0}, α_0 rates of failure for the dependency relation, assuming:

$\alpha_{j0} = \sum \alpha_{ji}/k$, $i = 1, ..., k$ for k-out-of-n

$\alpha_0 = \sum \alpha_j/n$, $j = 1, ..., n$ for 1-out-of-n

U_{j0} an independent shock, *i.e.*, time to failure to destroy all units, with rate α_{j0} assumed $\sum \alpha_{ji}/k$, $j = 1, .., m$ for k-out-of-n

$T_{ji} = \min(U_{ji}, U_{j0})$ time to failure for failure-dependent units

$S_j = \min(T_{j1}, .., T_{ji}, .., T_{jk})$, operating-life for path $j = 1, ..., m$

r critical system operating-life

θ_j representative rate of failure for each success - path (tie-set)

Ω_j representative failure rate for each unit in 1-out-of-n network

$T = \sum S_j$ network good operating-life

CE(T) an indicator function for system success counter CE=1 for $T > t$ at E^{th} simulation.

R(T) system reliability function

1-out-of-n:G MODELLING

In many network reliability problems, it is appropriate to assume some form of dependence among component life lengths as a result of common-mode failures, such as in microprocessor or electric power networks. Common-mode (interdependent) failures occur in standby or redundant systems or interactive systems which respond to a common environmental shock [1,11,12]. The joint-density-function approach is one way to proceed, as investigated by Bazovsky [3] in 1961 and Shooman [4] in 1968 in order to estimate the system survival distribution , where the survival or reliability is defined as the probability of the total good operating-life T (system time to failure), in a standby group of n-components with one operating and

Compound-Poisson Software Reliability Model

Mehmet Sahinoglu, *Member, IEEE*

Abstract— **The probability density estimation of the number of software failures in the event of clustering or clumping of the software failures is the subject of this paper. A discrete compound Poisson (CP) prediction model, as opposed to a Poisson (P) process, is proposed for the random variable (rv) X_{rem}, which is the remaining number of software failures. The compounding distributions, which are assumed to govern the failure sizes at Poisson arrivals, are respectively taken to be geometric when failures are forgetful and logarithmic-series (LSD) when failures are contagious. The expected value (μ) of X_{rem} of CP is calculated as a function of the time-dependent Poisson and compounding distribution based on the failures experienced. Also, the q (variance/mean) parameter for the remaining number of failures, q_{rem} is best estimated by q_{past} from the failures already experienced. Then, one obtains the pdf of the remaining number of failures estimated by CP(μ,q). The CP model suggests that the CP is superior to Poisson where clumping of failures exists. Its predictive validity is comparable to Musa-Okumoto's (MO) Log-Poisson Model for certain software failure data with q>1 when software failures clump within the same CPU second or unit time.**

Index Terms— **Compounding density, failure batch size, geometric, logarithmic-series, Poisson process, software reliability.**

I. Introduction

The ESTIMATION of the probability distribution functions (pdf) of software reliability indexes is currently a research topic of considerable interest to software engineers and statisticians. The notion of software reliability, the probability that the software will work without a failure for a specified period of time under specified conditions, is an important measure of software quality. In addition to the "times-between-failures" models, a number of "failure-count" models has been proposed where the interest is in the prediction of the number of residual failures in a future time interval rather than in the mean times to failures (MTTF) [5], [6], [11]. For a survey of other statistical procedures, the interested reader should see Ramamoorthy and Bastani [27]. The homogeneous or nonhomogeneous Poisson process (NHPP) alone does not statistically satisfy the requirements of a certain counting process at those epochs of failures that occur in bunches within the specified CPU second or time-unit.

The Poisson approach must possess the "orderliness" property, which dictates that the jumps of the counting process *N(t)* should be of strictly unit magnitude with probability one (w.p.1) [3], [4], [8]. Some other types are said to belong to a class of complex stochastic-state systems in which software failures will tend to occur in clusters in a software operational environment [2]. The sum of multiple counts in the discrete time domain is known to be distributed as compound Poisson (CP), where the mean differs from the variance [1], [3], [4], [8]–[11], [14], [15], [19]–[22].

The compounding pdf, as assumed in this paper, is twofold. It is either the geometric density with its forgetfulness property, to govern the failure-size ($x > 1$) distribution. A Poisson process is only a special case of the generalized CP, i.e., q(variance/mean)=1. Note, the symbol ^ denotes that the parent distribution to the left of ^ is compounded by the compounding distribution to the right of ^ [14]. Similarly, a publication on the Poisson^Geometric distribution of the loss of load hours in electric power systems, has studied the limiting sum of Markov Bernoulli variables [10]. Otherwise, one uses a logarithmic-series distribution (LSD), for the jump sizes, with its true contagion property. The sum of LSD rv's governed by a Poisson counting process produces a generalized CP, which is simply a negative binomial distribution (NBD) [1], [14]–[18], [22].

Manuscript received July 5, 1990; revised February 24, 1992. This work was supported by a Fulbright scholarship and by the Science and Engineering Research Council. Recommended by F. Bastani.

The author is with the Middle East Technical University (METU), Ankara, Turkey 06531.

IEEE Log Number 9201500.

II. Generalizations Of The Poisson Model

The Poisson theorem [3]–[5], [13], [21], [22] asserts that a counting process is Poisson if the jumps in all intervals of the same length are identically distributed and independent of the past jumps (stationary and independent increments) and the events occur one at a time (orderliness). However, interarrival times may be exponentially distributed, but this is not sufficient to prove the process is Poisson. The point of the preceeding discussion is to show that the interrenewal times must be independent in order to establish that a counting process is indeed a Poisson process [12, p. 434].

Let us observe two generalizations of the Poisson process [28]: The first is the CP process, which is the process obtained if the orderliness property is dropped from the Poisson theorem and replaced with the following.

Stationary Jumps: Let Z_n be the size of the *n*th jump, where $\{Z_n, n = 1, 2...\}$ are i.i.d. rv's. Let J(t) be the number of jumps that occur during (0,t]; then, N(t) is a Compound Poisson process where, $N(t) = Z_1 + Z_2 + \ldots + Z_{J(t)}, t \geq 0$.

The second generalization is the NHPP [3], [4], obtained by dropping the stationary increments property in Poisson theorem and replacing it with the "time-dependent increments" property, where the Poisson arrival rate β varies with time *t*, e.g., in software testing [23]–[25] or ambulance calls during an ordinary day.

III. Truncated Poisson^Geometric Model

A CP process with a specific compounding distribution in mind has interarrival times as negative exponentially dis-

0162–8828/92$03.00 © 1992 IEEE

Doğa - Tr. J. of. Engineering and Environmental Sciences
17 (1993), 157-163

Application of Monte Carlo Simulation Method for the Estimation of Reliability Indices in Electric Power Generation Systems

Mehmet ŞAHİNOĞLU, Ayşe Sevtap SELÇUK
Department of Statistics, Middle East Technical University, 06530, Ankara-Türkiye

Received 3/10/1990

Abstract: The aim of this study is to calculate the indices which describe the reliability of power generating systems by using Monte Carlo Simulation Method. The reliability indices obtained from the proposed method are compared with 32 generators where the units functionally depend on each other and fail with respect to a Multivariate Exponential Distribution (MVE). Further, the model is to be generalized for larger electric power systems.

Key Words: Monte Carlo simulation, multivariate exponential distribution, electric power system reliability indices.

Monte Carlo Benzetim Yöntemiyle Elektrik Enerji Üretim Sisteminde Güvenilirlik Endekslerinin Tahmini

Özet: Elektrik enerji şebekesi, yüksek düzeyde güvenilirlik beklenen sistemlerin başında gelir. Bu çalışmanın amacı Monte Carlo Benzetim yöntemini kullanarak enerji üretim sistemlerinin güvenirliliğini tanımlayan endeksleri hesaplamaktır. Birbirleriyle fonksiyonel olarak bağımlı olup çok değişkenli üstel dağılım kuralına göre arıza yapan 32 jeneratörlük bir üretim sisteminde Monte Carlo Benzetim yöntemiyle elde edilen endeksler yine aynı sistemde elde edilen analitik çözümlerle karşılaştırılmıştır ve yöntem daha geniş sistemler için genelleştirilmiştir.

Anahtar Kelimeler: Monte Carlo benzetimi, çok değişkenli üstel dağılım, sistem güvenilirlik endeksleri.

Introduction

The system reliability problems arise in areas such as communication networks- electrical power systems, transportation systems or manufacturing systems. A very important element in the design and operation of a system is the estimation of the impact of the unreliability measure which must be quantitatively defined for improvement purposes.

The reliability of an electric supply system is defined as the probability of providing users with continuous service of satisfactory quality within prescribed tolerances for the time period envisaged under the conditions encountered. The objective of this study is to calculate the indices which describe the reliability of power generating systems by Monte Carlo Simulation method and then to compare it with those of the established analytical results which are described in Patton et al., (1962) [6]. The proposed model, simulates the occurring random events and the operational decisions taken. Thus, the generating system is operated and planned through a model in a manner which closely simulates the reality. The actual system events are simulated hour after hour. If a digital computer is used, this simulation is accomplished at a relatively high speed. The simuation model is performed for a sample system having 32 generators for a study period covering 28 hours. Further, it is to be generalized for larger systems.

The problem considered in this study can be outlined as follows: A forced outage describes the state of a component when it is not available to perform its intended function due to some chance event Directly associated with that component to be taken out of service immediately. A system comprising such indivi-

APPLIED STOCHASTIC MODELS AND DATA ANALYSIS, VOL. 11, 135–143 (1995)

A STOPPING RULE FOR A COMPOUND POISSON RANDOM VARIABLE

PAUL RANDOLPH

Information Systems and Quantitative Sciences, Texas Tech University, Lubbock, TX 79409-2101, U.S.A.

AND

MEHMET ŞAHINOĞLU

Department of Statistics, Middle East Technical University, Ankara, and Dokuz Eylul University, Izmir, Turkey

SUMMARY

An optimal empirical Bayesian stopping rule for the Poisson compounded with the geometric distribution is developed and applied to the problem of the sequential testing of computer software. For each checkpoint in time, either the software satisfies a desired economic criterion, or else the software testing is continued.

KEY WORDS compound Poisson; Bayesian analysis; stopping rules

1. INTRODUCTION

There are many examples in which events occur according to the Poisson distribution, and, furthermore, for each of these Poisson events one or more other events can occur. For example, accidents of automobiles on a given highway might follow a Poisson, but the number of injuries follows a compound Poisson. In another example, if the jobs in a manufacturing firm come off the line according to a Poisson distribution, then the number of defects is distributed according to the compound Poisson.[1] In this paper the application will be the testing of software. If an interruption that occurs during the testing of a software program is assumed to be due to one or more software failures in a clump, and if the distribution of the number of interruptions is Poisson, then the distribution of the number of clumped failures is compound Poisson.[2]

When a new computer software package is written and all obvious software faults removed, a testing program is usually initiated to eliminate the remaining faults. The common procedure is to use the software package on a set of problems, and whenever the testing is interrupted because of one or more programming failures, the faults are corrected, the software recompiled, and computation is re-started. This testing can continue for several days or weeks, with the number of failures per unit time becoming fewer and fewer. Finally, a point is reached when it seems that all the software faults surely have been removed, at which time the software can be released to the end user.

However, when testing is stopped and the software released, one is never completely certain that all software faults have been found. Most likely there may be still a very small

CCC 8755–0024/95/020135–09

Received 18 May 1993
Revised 4 January 1995

SOFTWARE TESTING, VERIFICATION AND RELIABILITY, VOL. 7, 35–57 (1997)

Alternative Parameter Estimation Methods for the Compound Poisson Software Reliability Model with Clustered Failure Data

MEHMET SAHINOGLU[1]* AND ÜNAL CAN[2]

[1] *Department of Statistics, Dokuz Eylül University, Izmir, Turkey*
[2] *State Institute of Statistics (D.I.E.), Istanbul, Turkey*

SUMMARY

The 'compound Poisson' (CP) software reliability model was proposed previously by the first named author for time-between-failure data in terms of CPU seconds, using the 'maximum likelihood estimation' (MLE) method to estimate unknown parameters; hence, CPMLE. However, another parameter estimation technique is proposed under 'nonlinear regression analysis' (NLR) for the compound Poisson reliability model, giving rise to the name CPNLR. It is observed that the CP model, with different parameter estimation methods, produces equally satisfactory or more favourable results as compared to the Musa–Okumoto (M–O) model, particularly in the event of grouped or clustered (clumped) software failure data. The sampling unit may be a week, day or month within which the failures are clumped, as the error recording facilities dictate in a software testing environment. The proposed CPNLR and CPMLE yield comparatively more favourable results for certain software failure data structures where the frequency distribution of the cluster (clump) size of the software failures per week displays a negative exponential behaviour. Average relative error (ARE), mean squared error (MSE) and average Kolmogorov–Smirnov (K–S Av.D_n) statistics are used as measures of forecast quality for the proposed and competing parameter-estimation techniques in predicting the number of remaining future failures expected to occur until a target stopping time. Comparisons on five different simulated data sets that contain weekly recorded software failures are made to emphasize the advantages and disadvantages of the competing methods by means of the chronological prediction plots around the true target value and zero per cent relative error line. The proposed generalized compound Poisson (MLE and NLR) methods consistently produce more favourable predictions for those software failure data with negative exponential frequency distribution of the failure clump size versus number of weeks. Otherwise, the popularly used competing M–O log-Poisson model is a better fit for those data with a uniform clump size distribution to recognize the log-Poisson effect while the logarithm of the Poisson equation is a constant, hence uniform. The software analyst is urged to perform exploratory data analysis to recognize the nature of the software failure data before favouring a particular reliability estimation method. © **1997 by John Wiley & Sons, Ltd.**

Software Testing, Vol. 7, 35–57 (1997)

(No. of Figures: 10 No. of Tables: 3 No. of Refs: 31)

KEY WORDS compound Poisson (CP); maximum likelihood estimation (MLE); nonlinear regression (NLR); Musa–Okumoto (M–O); clustered failures; average relative error (ARE); mean squared error (MSE); average Kolmogorov–Smirnov statistic (K–S Av.D_n)

* Corresponding author.

CCC 0960–0833/97/010035–23

Received 24 April 1994
Revised 28 December 1995

Stochastic Bayes Measures to Compare Forecast Accuracy of Software-Reliability Models

Mehmet Sahinoglu, *Senior Member, IEEE*, John J. Deely, and Sedat Capar

***Abstract*—ARE (absolute relative error) and SqRE (squared relative error), are random variables that are suggested as measurements of forecast accuracy of the total number of estimated software failures at the end of a mission time. The purpose is to compare the predictive merit of competing software reliability models, an important concern to software reliability analysts. This technique calculates the Bayes probability of how much better the prediction accuracy is for one method relative to a competitor. This novel approach is more realistic, in the assessment of predictive merit, than a) comparing merely the average values of ARE and SqRE as conventionally done; and b) Conducting statistical hypothesis tests of pair-wise means of ARE and SqRE, an approach somewhat more sensible than a), because b) incorporates variability of predicted values, which a) does not. To implement this technique, first noninformative (across the border) are used and then informative (specified) priors. For the informative case, half-normal priors are placed on the mean of the ARE or SqRE random variables, because these means are hypothesized to remain peaked around zero relative-error (ideal error percentage). This problem is related to the general problem of ranking usual means discussed in the literature by Berger and Deely (1988), and is a follow-up to an invited research paper presented at ISI-97 by Sahinoglu and Capar (1997).**

***Index Terms*—Bayes, forecast accuracy, informative, noninformative, pairwise comparison, relative error, software-reliability model.**

ACRONYMS[1]

pdf	probability density function
r.v.	random variable
MLE	maximum likelihood estimate
RE	relative error
Notation:	
k	checkpoint between 1 and n
y_k	true number of software failures over $k = 1, \ldots, n$
x_{true}	$\sum_{k=1}^{n} y_k$
$x_{\text{est}}(k)$	forecast value of the total number of software failures estimated at time point $1 \le k \le n$
X_j	error r.v., $j = 1, 2$ for the two methods being compared
ARE	absolute RE
AvRE	average RE: arithmetic average of ARE(k)
AvSqRE	average SqRE: arithmetic average of SqRE(k)
CPMLE	compound Poisson MLE
CPNLR	compound Poisson nonlinear regression
MO	Musa–Okumoto logarithmic Poisson (method)
SqRE	squared RE
SSqRE	sum of SqRE over n sampled checkpoints

Manuscript received February 28, 1998; revised July 28, 2000.

M. Sahinoglu is with the Department Computer and Information Science, Troy State University, Montgomery, AL 36103-4419 USA (e-mail: MeSa@tsum.edu).

J. J. Deely is with the Department of Statistics, Purdue University, W. Lafayette, IN 47907 USA (e-mail: JDeely@stat.purdue.edu).

S. Capar is with the Department of Statistics, Dokuz Eylul University, Kaynaklar Kampusu, Buca-Izmir Turkey.

Publisher Item Identifier S 0018-9529(01)06806-3.

[1] The singular and plural of an acronym are always spelled the same.

I. INTRODUCTION

THERE IS increasing pressure to develop and quantify measures of computer software reliability [8], [18]. With the ascent of software reliability models, there is even more pressure to assess the predictive quality of these measures, both in their "goodness of fit" and "pair wise comparisons" [6], [9], [14]–[17]. However, the current methods, to compare these software reliability models, use constant measures and hence their results do not reflect the variability inherent in the observations. In particular, forecast accuracy of various methods are compared through measures such as AvRE and MSE (mean square error), both of which are constant measures. These do not consider the effect of stochastic variability. An earlier suggestion was to devise and study more precise methods for choosing the best predictive procedure through frequentist methods, such as two sample t-tests of equality of means, which consider this inherent variability. In addition to assessing the quality of fit to zero RE of an individual model, comparisons between competing models were conducted by t-tests. Such research was necessary to choose between the many new and old reliability models [15]. The research in this paper proposes and studies several new and particularly, actual data-supported Bayes methods of assessment, which acknowledge the presence of stochastic variation in the observed sequence of failure data, assumed or selected to be s-independent [16], [17].

The authors have already compared pairs of certain reliability models' forecast accuracy using statistical hypothesis tests in the frequentist sense. It was observed that a constant difference between the means of r.v. ARE, i.e., the AvRE of any two methods did not necessarily prove s-significant as to which of two competing estimation procedures was better. An alternative way of measurement through a more severe squared penalty reflected in r.v., SqRE is also considered in all calculations in this study. This paper brings a new dimension to the comparative assessment of the predictive accuracy of two competing methods. In developing Bayes methods, an innovative new approach is proposed, not only to allow for deciding which method is better, but additionally to quantitatively describe how much one is better than the other. This is done by experimenting with

2002 Society for Design and Process Science
Printed in the United States of America

HIGH ASSURANCE SOFTWARE TESTING IN BUSINESS AND DOD

Mehmet Sahinoglu
Department of Computer and Information Science
Troy State University Montgomery
Montgomery, AL

Coskun Bayrak
Computer Science Department
Donaghey College of Information Science and Systems Engineering
University of Arkansas at Little Rock
Little Rock, AR

Timothy Cummings
HQ Standard Systems Group
Maxwell AFB – Gunter Annex
Montgomery, AL

This paper argues that software testing can be less thorough yet more efficient if applied in a well-managed, empirical manner across the entire Software Development Life Cycle (SDLC). To ensure success, testing must be planned and executed within an Earned Value Management (EVM) paradigm. A specific example of empirical software testing is given: the Empirical Bayesian Stopping Rule (EBSR). The Stopping Rule is applied to an actual Department of Defense (DoD) software development to show potential gains with respect to archaic testing methods that were used. The result is that a considerable percentage of the particular testing effort could have been saved under usual circumstances, had the testing been planned and executed under EVM with the Empirical Bayesian Stopping Rule algorithm.

1. Introduction

Across the DoD and the general software industry, there is a drastic disparity in SDLC test planning and management. Businesses waste tremendous resources by not planning, developing, or testing software in an efficient, scientific manner. EVM is misunderstood and misused, planning is not comprehensive, and testing is not pervasive throughout the SDLC. There are methods of efficiently managing an SDLC

Parity Bit Signature in Response Data Compaction and Built-In Self-Testing of VLSI Circuits With Nonexhaustive Test Sets

Sunil R. Das, *Fellow, IEEE*, Made Sudarma, Mansour H. Assaf, *Member, IEEE*, Emil M. Petriu, *Fellow, IEEE*, Wen-Ben Jone, *Senior Member, IEEE*, Krishnendu Chakrabarty, *Senior Member, IEEE*, and Mehmet Şahinoğlu, *Senior Member, IEEE*

***Abstract*—The design of efficient time compression support hardware for built-in self-testing (BIST) is of great importance in the design and manufacture of VLSI circuits. The test data outputs in BIST are ultimately compressed by the time compaction hardware, commonly called a response analyzer, into signatures. Several output response compaction techniques to aid in the synthesis of such support circuits already exist in literature, and parity bit signature coupled with exhaustive testing is already well known to have certain very desirable properties in this context. This paper reports new time compaction techniques utilizing the concept of parity bit signature that facilitates implementing such support circuits using nonexhaustive or compact test sets, with the primary objective of minimizing the storage requirements for the circuit under test (CUT) while maintaining the fault coverage information as best as possible. Recently, Jone and Das proposed a multiple-output parity bit signature generation method extending the basic idea of Akers, for exhaustive testing of digital combinational circuits, where, given a multiple-output circuit, a parity bit signature is generated by first XORing all the outputs to produce a new output function and then feeding this resulting function to a single-output parity bit signature generator. The method, as shown by the authors, preserves all the desirable properties of the conventional single-output response analyzers and can also be easily implemented by using the current VLSI technology. The subject paper further augments the aforesaid concepts of Jone and Das, and proposes a multiple-output parity bit signature for nonexhaustive testing of VLSI circuits. Design algorithms are proposed in the paper, and the simplicity and ease of their implementations are demonstrated with examples. Extensive simulation experiments on ISCAS 85 combinational benchmark circuits using FSIM, ATALANTA, and COMPACTEST programs demonstrate that the proposed signature generation method achieves high fault coverage for single stuck-line faults, with low CPU simulation time, and acceptable area overhead. A performance comparison of the designed time compactors with conventional space-time compaction is also presented to demonstrate improved tradeoff for the new circuits in terms of fault coverage and the CUT resources consumed contrasted with existing designs, and to appreciate the resulting performance enhancements.**

Manuscript received December 15, 2002; revised June 29, 2003. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada under Grant A 4750.

S. R. Das, M. Sudarma, M. H. Assaf, and E. M. Petriu are with the School of Information Technology and Engineering, Faculty of Engineering, University of Ottawa, Ottawa, ON K1N 6N5, Canada.

W.-B. Jone is with the Department of Electrical and Computer Engineering and Computer Science, University of Cincinnati, Cincinnati, OH 45221 USA.

K. Chakrabarty is with the Department of Electrical and Computer Engineering, Duke University, Durham, NC 27708 USA.

M. Şahinoglu is with the Department of Computer and Information Science, Troy State University Montgomery, Montgomery, AL 36103 USA.

Digital Object Identifier 10.1109/TIM.2003.818547

***Index Terms*—Built-in self-test (BIST), circuit under test (CUT), multiple-output parity bit signature generation, nonexhaustive or compact test sets, parity testing, space-time compaction, stuck-line faults, time compaction.**

I. Introduction

As the digital design moves through increased levels of integration densities, it is desirable that better and effective methods of testing be made available to ensure reliable systems operation. Frankly speaking, the concept of testing has broad applicability, and as such, finding efficient testing techniques that guarantee correct systems performance has attracted considerable attention of the testing community for quite sometime [1]–[32]. The conventional testing techniques of digital systems require application of test stimuli generated by a test pattern generator (TPG) to the circuit under test (CUT) and subsequent comparison of the produced responses with known correct responses. However, for large circuits, because of higher storage requirements for the fault-free responses, the procedure turns out to be rather expensive, and hence alternative approaches are sought. Built-in self-testing (BIST) is a design approach that can significantly improve the testability of digital circuits and save testing time. It combines concepts of both built-in test (BIT) and self-test (ST) in one termed built-in self-test (BIST). In BIST, test generation, test application, and response verification are all done through built-in hardware, which allows different parts of a chip to be tested in parallel, reducing the required testing time, besides eliminating the necessity for external test equipments. A typical BIST environment, as shown in Fig. 1, uses a test pattern generator (TPG) that sends its outputs to a circuit under test (CUT), and the resulting output streams from the CUT are fed into a response data analyzer. A fault is detected if the CUT response is shown to be different from that of the fault-free circuit. The test data analyzer is comprised of a response compaction unit (RCU), a storage for the fault-free responses of the CUT, and a comparator.

In order to reduce the amount of data represented by the fault-free and the faulty CUT responses, data compression is used to create signatures from the CUT and its corresponding fault-free circuit. BIST techniques use pseudorandom, pseudoexhaustive, and exhaustive test patterns, or even sometimes on-chip storing of reduced test sets. The standard response compaction unit is comprised of a space compression unit and

Fault Simulation and Response Compaction in Full Scan Circuits Using HOPE

Sunil R. Das, *Life Fellow, IEEE*, Chittoor V. Ramamoorthy, *Life Fellow, IEEE*, Mansour H. Assaf, *Member, IEEE*, Emil M. Petriu, *Fellow, IEEE*, Wen-Ben Jone, *Senior Member, IEEE*, and Mehmet Sahinoglu, *Senior Member, IEEE*

***Abstract*—This paper presents results on fault simulation and response compaction on ISCAS 89 full scan sequential benchmark circuits using HOPE—a fault simulator developed for synchronous sequential circuits that employs parallel fault simulation with heuristics to reduce simulation time in the context of designing space-efficient support hardware for built-in self-testing of very large-scale integrated circuits. The techniques realized in this paper take advantage of the basic ideas of sequence characterization previously developed and utilized by the authors for response data compaction in the case of ISCAS 85 combinational benchmark circuits, using simulation programs ATALANTA, FSIM, and COMPACTEST, under conditions of both stochastic independence and dependence of single and double line errors in the selection of specific gates for merger of a pair of output bit streams from a circuit under test (CUT). These concepts are then applied to designing efficient space compression networks in the case of full scan sequential benchmark circuits using the fault simulator HOPE.**

***Index Terms*—Built-in self-test (BIST), circuit under test (CUT), detectable error probability estimates, fault simulation using HOPE, Hamming distance, optimal sequence mergeability, response compaction, sequence weights, single stuck-line faults, space compactor.**

I. Introduction

With continued growth in semiconductor industries and development of extremely complex systems with higher levels of integration densities, the real urge to find better and more efficient methods of testing that ensure reliable operations of chips, a mainstay of today's many sophisticated digital systems, has become the single most pressing issue to design and test engineers. The very concept of testing has a broad applicability, and finding highly effective test techniques that

Manuscript received November 11, 2003; revised December 7, 2004. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada under Grant A 4750.

S. R. Das is with the School of Information Technology and Engineering, University of Ottawa, Ottawa, ON K1N 6N5, Canada, and with the Department of Computer and Information Science, Troy State University-Montgomery, Montgomery, AL 36103 USA.

C. V. Ramamoorthy is with the Department of Electrical Engineering and Computer Sciences, Computer Science Division, University of California, Berkeley, CA 94720 USA.

M. H. Assaf and E. M. Petriu are with the School of Information Technology and Engineering, University of Ottawa, Ottawa, ON K1N 6N5, Canada.

W.-B. Jone is with the Department of Electrical and Computer Engineering and Computer Science, University of Cincinnati, Cincinnati, OH 45221 USA.

M. Sahinoglu is with the Department of Computer and Information Science, Troy State University-Montgomery, Montgomery, AL 36103 USA.

Digital Object Identifier 10.1109/TIM.2005.858102

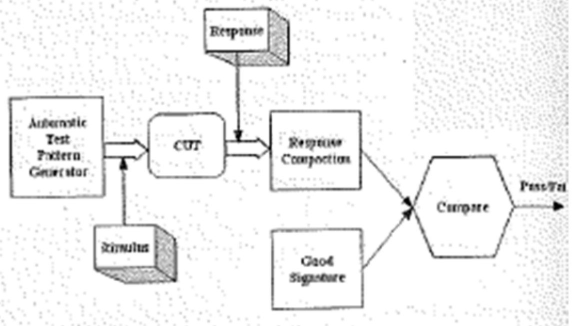


Fig. 1. Block diagram of the BIST environment.

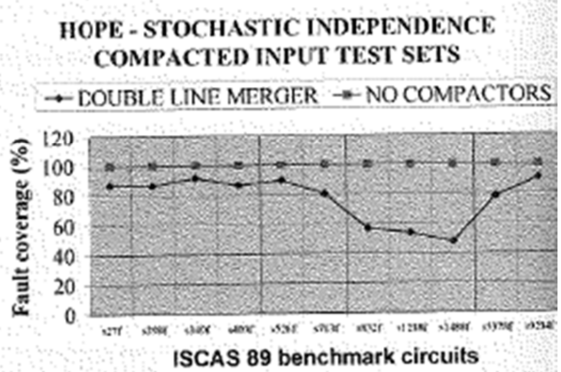


Fig. 2. Simulation results of the ISCAS 89 full scan sequential benchma circuits using HOPE under stochastic independence of single and double li errors using compacted input test sets.

guarantee correct system performance has been gaining impo tance [1]–[57]. Consider, for example, medical test and dia nostic instruments, airplane controllers, and other safety-cr ical systems that have to be tested before (off-line testing) a during use (on-line testing). Another application where failu can have severe economic consequences is real-time transa tions processing. The testing process in all these circumstanc must be fast and effective to make sure that such systems opera correctly. In general, the cost of testing integrated circuits (IC is rather prohibitive; it ranges from 35% to 55% of their to manufacturing cost [7]. Besides, testing a chip is also time co suming, taking up to about one-half of the total design cycle ti [8]. The amount of time available for manufacturing, testi and marketing a product, on the other hand, continues to d crease. Moreover, as a result of global competition, custom demand lower cost and better quality products. Therefore,

An Empirical Bayesian Stopping Rule in Testing and Verification of Behavioral Models

Mehmet Şahinoğlu, *Senior Member, IEEE*

***Abstract*—Software stopping rules are tools to effectively minimize the time and cost involved in software testing. The algorithms serve to guide the testing process such that if a certain level of branch or fault (or failure) coverage is obtained without the expectation of further significant coverage, then the testing strategy can be stopped or changed to accommodate further, more advanced testing strategies. By combining cost analysis with a variety of stopping-rule algorithms, a comparison can be made to determine an optimally cost-effective stopping point. A novel cost-effective stopping rule using empirical Bayesian principles for a nonhomogeneous Poisson counting process compounded with logarithmic-series distribution (LSD) is derived and satisfactorily applied to digital software testing and verification. It is assumed that the software failures or branches covered, whichever the case may be, clustered at the application of a given test-case are positively correlated, i.e., contagious, implying that the occurrence of one software failure (or coverage of a branch) positively influences the occurrence of the next. This phenomenon of clustering of software failures or branch coverage is often observed in software testing practice. The r.v. w_i of the failure-clump size of the interval is assumed to have LSD(θ) and justified on the data sets by employing a chi-square goodness of fit testing while the distribution of the number of test cases is Poisson(λ). Then, the distribution of the total number of observed failures, or similarly covered branches, X is a compound Poisson ^ LSD, i.e., negative binomial distribution, given that a certain mathematical identity holds. For each checkpoint in time, either the software satisfies a desired reliability attached to an economic criterion, or else the software testing is allowed to continue. By using a one-step-look-ahead formula derived for the model, the proposed stopping rule is applied to five test case-based data sets acquired by testing embedded chips through the complex VHDL models. Further, multistrategy testing is conducted to show its superiority to single-stage testing. Results are satisfactorily interpreted from a practitioner's viewpoint as an innovative alternative to the ubiquitous test-it-to-death approach, which is known to waste billions of test cases in a tedious process of finding more bugs. Moreover, the proposed dynamic stopping-rule algorithm can validly be employed as an alternative paradigm to the existing on-line statistical process control methods static in nature for the manufacturing industry, provided that underlying statistical assumptions hold. A detailed comparative literature survey of stopping-rule methods is also included in terms of pros and cons, and cost effectiveness.**

***Index Terms*—Bernoulli process, cluster effect, compound Poisson process, cost effective, effort domain, empirical Bayesian analysis, failure or branch coverage, logarithmic-series distribution (LSD), negative binomial distribution (NBD), positive autocorrelation, stopping rule.**

Manuscript received December 15, 2002; revised July 9, 2003.
The author is with the Department of Computer and Information Science, Troy State University Montgomery, Montgomery, AL 36103-4419 USA (e-mail: mesa@tsum.edu).
Digital Object Identifier 10.1109/TIM.2003.818548

I. Introduction and Motivation

THIS PAPER describes a statistical model to devise a stopping criterion for random testing in VHDL based hardware verification. The method is based on statistical estimation of branching coverage and will flag the stopping criteria to halt the verification process or to switch to a different verification strategy. The paper gives some results on some VHDL descriptions. This paper builds upon the statistical behavior of failure (or fault) or branch coverage described in Section II. Applying empirical Bayesian and other statistical methods to problems in hardware verification, such as better stopping rules, should be a fruitful area of research where improvements in the state of the art would be very valuable. Technically, the general concept is questionable. However, the stopping-rule idea is generally accepted to be more rational than having no value-engineering judgment to stop testing, as often dictated by a commercially tight time-to-market approach [41]. There is actually a large number of research and practical results available in statistically analyzing hardware verification processes. All major microprocessor companies heavily rely on such concepts. Note, faults and failures are taken to be synonymous here for convenience.

When designing a VLSI system in the behavioral level, one of the most important steps to be taken is verifying its functionality before it is released to the logic/PD design phase. It is widely believed that the quality of a behavioral model is correlated to the experienced branch or fault coverage during its verification process [17]–[19], [31], [51]. However, measuring coverage is just a small part of ensuring that a behavioral model meets the desired quality goal. A more important question is how to increase the coverage during verification to a certain level with a given time-to-market constraint. Current methods use brute force where billions of test cases were applied without knowing the effectiveness of the techniques used to generate these test cases [17]–[19], [32], [46]. One may consider behavioral models as oracles in industries to test against when the final chip is produced. In this work, in experimental sets involved, branch coverage (in five data sets of DR1 to DR5) is used as a measure for the quality of verifying and testing behavioral models. Minimum effort for achieving a given quality level can be realized by using the above proposed empirical Bayesian stopping rule. The stopping rule guides the process to switch to a different testing strategy using different types of patterns, i.e., random versus functional, or using different set of parameters to generate patterns or test cases or test vectors when the current strategy is expected not to increase the coverage. This leads to

ALIASING-FREE COMPACTION IN TESTING CORES-BASED SYSTEM-ON-CHIP (SOC) USING COMPATIBILITY OF RESPONSE DATA OUTPUTS

Sunil R. Das
School of Information Technology and Engineering, Faculty of Engineering, University of Ottawa, Ottawa, Ontario K1N 6N5, Canada, and
Department of Computer and Information Science, Troy State University Montgomery, Montgomery, AL 36103, U.S.A.

Mansour H. Assaf
Emil M. Petriu
School of Information Technology and Engineering, Faculty of Engineering, University of Ottawa, Ottawa, Ontario K1N 6N5, Canada

Mehmet Sahinoglu
Department of Computer and Information Science, Troy State University Montgomery, Montgomery, AL 36103, U.S.A.

The realization of space-efficient support hardware for built-in self-testing (BIST) is of great importance in the design and manufacture of VLSI circuits. Novel approaches to designing aliasing-free space compaction hardware were recently proposed in the context of testing cores-based system-on-chip (SOC) for single stuck-line faults, extending the well-known concepts of conventional switching theory, specifically those of cover table and frequency ordering commonly utilized in the simplification of switching functions, and of compatibility relation as used in the minimization of incomplete sequential machines, based on optimal generalized sequence mergeability, as developed and utilized by the authors in earlier works. The advantages of these aliasing-free compaction methods over earlier techniques are quite obvious, since zero-aliasing is achieved without any modifications of the module under test (MUT), while keeping the area overhead and signal propagation delay relatively low as contrasted with the conventional parity tree linear compactors. Besides, the approaches could be applied with both deterministic compacted and pseudorandom test patterns. The subject paper, without furnishing details of the different algorithms developed in the implementation of these approaches to designing zero-aliasing space compactors, provides the mathematical basis of selection criteria for merger of an optimal number of outputs of the MUT to achieve maximum compaction ratio in the design, along with some results from simulation experiments conducted on ISCAS 85 combinational and ISCAS 89 full-scan sequential benchmark circuits, with simulation programs ATALANTA, FSIM, and HOPE.

Keywords: *Aliasing-free (zero-aliasing) space compaction, built-in self-testing (BIST) in VLSI, compatibility of response data outputs, cores-based system-on-chip (SOC), module under test (MUT).*

Revisiting Response Compaction in Space for Full-Scan Circuits With Nonexhaustive Test Sets Using Concept of Sequence Characterization

Sunil R. Das, *Life Fellow, IEEE*, Chittoor V. Ramamoorthy, *Life Fellow, IEEE*, Mansour H. Assaf, *Member, IEEE*, Emil M. Petriu, *Fellow, IEEE*, Wen-Ben Jone, *Senior Member, IEEE*, and Mehmet Sahinoglu, *Senior Member, IEEE*

***Abstract*—This paper revisits response compaction in space and reports results on simulation experiments on ISCAS 89 full-scan sequential benchmark circuits using nonexhaustive (deterministic compact and pseudorandom) test sets in the design of space-efficient support hardware in the context of built-in self-testing (BIST) of VLSI circuits. The techniques used herein take advantage of sequence characterization as utilized by the authors earlier in response data compaction in the case of ISCAS 85 combinational benchmark circuits using ATALANTA, FSIM, and COMPACTEST, to realize space compression of ISCAS 89 full-scan sequential benchmark circuits using simulation programs ATALANTA, FSIM, and MinTest, under conditions of both stochastic independence and dependence of single and double line errors.**

***Index Terms*—ATALANTA, built-in self-test (BIST), COMPACTEST, FSIM, full-scan circuits, MinTest, nonexhaustive (deterministic compact and pseudorandom) test sets, sequence characterization, space compaction, VLSI circuits.**

I. Introduction

As THE electronics industry continues to grow, integration densities and system complexities continue to increase, and the necessity for better and more efficient methods of testing to ensure reliable operations of chips, the mainstay of today's many sophisticated devices and products, is being increasingly realized [1]–[57]. The very concept of testing has a relatively broad applicability, and finding the most effective testing techniques that can guarantee correct system performance is of immense practical significance. Generally, the price of testing integrated circuits (ICs) is rather prohibitive, accounting for 35% to 55% of their total manufacturing cost. Besides, testing a chip is also time-consuming, taking up to about one-half of the total design cycle time. The amount of time available for manufacturing, testing, and marketing a product, on the other hand, is on the decline. Moreover, as a result of diminishing trade barriers and global competition, customers now demand products of better quality at lower cost. In order to achieve this higher quality at lower cost, evidently testing methods need to be improved. The conventional testing techniques of digital circuits require application of test patterns generated by a test pattern generator (TPG) to the circuit under test (CUT) and comparing the responses with known correct responses. For large circuits, because of higher storage requirements for the fault-free responses, the customary test procedures, thus, become very expensive, and, hence, alternative approaches are required to minimize the amount of needed storage [45].

Built-in self-testing (BIST) is a design process that provides the capability of solving many of the problems otherwise encountered in testing digital systems. It combines the concepts of both built-in test (BIT) and self-test (ST) in one termed built-in self-test (BIST). In BIST, test generation, test application, and response verification are all accomplished through built-in hardware, which allows different parts of a chip to be tested in parallel, reducing thereby the required testing time, besides eliminating the necessity for external test equipment. As the cost of testing is becoming the single major component of the manufacturing expense of a new product, BIST, thus, tends to reduce manufacturing and maintenance costs through improved diagnosis [1]–[53]. Several companies such as Motorola, AT&T, IBM, and Intel have incorporated BIST in many of their products [6], [8], [14]–[16]. AT&T, for example, has incorporated BIST into more than 200 of their IC chips. The three large programmable logic arrays (PLAs) and microcode ROM in the Intel 80386 microprocessor were built-in self-tested [52]. The general-purpose microprocessor chip, Alpha AXP21164, and Motorola microprocessor 68020, were also tested using BIST techniques [8], [52]. More recently, Intel, for its Pentium Pro architecture microprocessor, with its unique requirements of meeting very high production goals, superior performance standards, and impeccable test quality put strong emphasis on its design-for-test (DFT) direction [16]. A set of constraints, however, limits Intel's ability to tenaciously explore DFT and test generation techniques, *viz*. full or partial scan or scan-based BIST [2]. AMD's K6 processor is a reduced instruction set computer (RISC) core named enhanced RISC86 microarchitecture [15]. K6 processor incorporates BIST into its DFT process. Each RAM array of K6 processor

Manuscript received October 23, 2003; revised May 9, 2005. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada under Grant A 4750.

S. R. Das is with the School of Information Technology and Engineering, Faculty of Engineering, University of Ottawa, Ottawa, ON K1N 6N5, Canada, and also with the Department of Computer and Information Science, Troy State University, Montgomery, AL 36103 USA.

C. V. Ramamoorthy is with the Department of Electrical Engineering and Computer Sciences, Computer Science Division, University of California, Berkeley, CA 94720 USA (e-mail: ram@csce.berkeley.edu).

M. H. Assaf and E. M. Petriu are with the School of Information Technology and Engineering, Faculty of Engineering, University of Ottawa, Ottawa, ON K1N 6N5, Canada.

W.-B. Jone is with the Department of Electrical and Computer Engineering and Computer Science, University of Cincinnati, Cincinnati, OH 45221 USA.

M. Sahinoglu is with the Department of Computer and Information Science, Troy State University, Montgomery, AL 36103 USA (e-mail: mesa@troy.edu).

Digital Object Identifier 10.1109/TIM.2005.855085

Measuring Availability Indexes With Small Samples for Component and Network Reliability Using the Sahinoglu–Libby Probability Model

Mehmet Sahinoglu, *Senior Member, IEEE*, David L. Libby, and Sunil R. Das, *Life Fellow, IEEE*

***Abstract*—With the advances in pervasive computing and wireless networks, the quantitative measurements of component and network availability have become a challenging task, especially in the event of often encountered insufficient failure and repair data. It is well recognized that the Forced Outage Ratio (FOR) of an embedded hardware component is defined as the failure rate divided by the sum of the failure and the repair rates; or FOR is the operating time divided by the total exposure time. However, it is also well documented that FOR is not a constant but is a random variable. The probability density function (pdf) of the FOR is the Sahinoglu–Libby (SL) probability model, named after the originators if certain underlying assumptions hold. The SL pdf is the generalized three-parameter Beta distribution (G3B). The failure and repair rates are taken to be the generalized Gamma variables where the corresponding shape and scale parameters, respectively, are not identical. The SL model is shown to default to that of a standard two-parameter Beta pdf when the shape parameters are identical. Decision Theoretic (Bayesian) solutions are employed to compute small-sample Bayesian estimators by using informative and noninformative priors for the component failure and repair rates with respect to three definitions of loss functions. These estimators for component availability are then propagated to calculate the network expected input–output or source–target (s–t) availability for four different fundamental networks given as examples. The proposed method is superior to using a deterministic way of estimating availability simply by dividing total up-time by exposure time. Various examples will illustrate the validity of this technique to avoid over- or underestimation of availability when only small samples or insufficient data exist for the historical lifecycles of components and networks.**

***Index Terms*—Bayes, beta, gamma, generalized three-parameter Beta distribution (G3B), informative, loss, Sahinoglu–Libby (SL), source–target (s–t) availability.**

NOMENCLATURE

FOR	Forced outage rate or unavailability index of a hardware or software component.
G3B	Generalized three-parameter beta RV.
MLE	Maximum likelihood estimate.
Q:Unavailability	RV for FOR, the probability that an item is inoperative at any point in time where q is a realization $q = 1 - r$.
R:Availability	Probability that an item is up (operating) at any point in time, where r is a realization. $r = 1 - q$.
RV	Random variable.
SL	Sahinoglu–Libby RV (same as G3B RV).
cdf	Cumulative probability density function of a given RV.
pdf	Probability density function of a given RV.
a	Number of occurrences of operative (up) times sampled.
b	Number of occurrences of debugging (down) times sampled.
c	Shape parameter of gamma prior for component failure rate λ.
d	Shape parameter of gamma prior for component recovery rate μ.
$E(q)$	Expected unavailability (= FOR) Estimator with informative prior using squared error loss.
$E(r)$	Expected availability ($= 1 -$ FOR) estimator with an informative prior using squared error loss.
$Q_{\rm sys}$	System unavailability random variable.
$\hat{q} = q_{\rm Est}$	Estimator of RV q using a specified estimation method.
q^*	Expected unavailability (= FOR) estimator with informative prior using weighted squared error loss.
q^{**}	Expected unavailability (= FOR) estimator with noninformative prior when $\xi = \eta = 0, c = d = 1$ using weighted squared error loss.
$q^{**}_{\rm large-sample}$	Unavailability (= FOR) large-sample asymptotic estimator of q^{**} if $a, b \to \infty$ where $(a/b) \approx 1$.
q_M	Median or Bayes estimator with informative prior for an absolute error loss function.
$R_{\rm sys}$	System availability random variable.
$\sum_i$	Summation notation.

Manuscript received April 11, 2004; revised November 12, 2004.

M. Sahinoglu is with Troy University, Montgomery, AL 36081 USA (e-mail: mesa@tsum.edu).

D. L. Libby is with IS Leaders, Shorewood, MN 55311-8125 USA (e-mail: David.Libby@ISLeaders.com).

S. R. Das is with the School of Information Technology and Engineering, Faculty of Engineering, University of Ottawa, Ottawa, ON K1N 6N5, Canada, and also with Troy University, Montgomery, AL 36703 USA.

Digital Object Identifier 10.1109/TIM.2005.847239

REFERENCES

[1] N. L. Johnson and S. Kotz, *Continuous Univariate Distributions*, 1st ed: Wiley, 1970, vol. 2.

[2] ——, *Continuous Univariate Distributions*, 2nd ed: Wiley, 1995, vol. 2.

[3] M. Sahinoglu, "Statistical inference on the reliability performance index for electric power generation systems," Ph.D. dissertation, Institute of Statistics, College Station, Texas A&M Univ., 1981.

[4] M. Sahinoglu, L. J. Ringer, M. T. Longnecker, C. Singh, and A. K. Ayoub, "Probability distribution functions for generation reliability indices—analytical approach," presented at the 1982 IEE/ASME/ASCE Joint Power Generation Conf., Denver, CO, Oct. 17–21, 1982.

[5] M. Sahinoglu, M. T. Longnecker, L. J. Ringer, C. Singh, and A. K. Ayoub, "Probability distribution functions for generation reliability indices—Analytical approach," *IEEE Trans. Power App. Syst.*, vol. PAS-102, no. 6, pp. 1486–1493, Dec. 1983.

[6] M. Sahinoglu and E. Chow, "Empirical-bayesian availability index of safety & time critical software systems with corrective maintenance," in *Proc. Pacific Rim Int. Symp. Dependable Computing*, Hong Kong, 1999, pp. 84–91.

[7] M. Sahinoglu, "Reliability index evaluations of integrated software systems (INTERNET) for insufficient software failure and recovery data," in *Lecture Notes Springer-Verlag 1st Int. Conf. ADVIS-2000*, Izmir, Turkey, Oct. 2000, pp. 25–27.

[8] M. Sahinoglu and W. Munns, "Availability indices of a software network," in *Proc. IX Brazilian Symp. Fault Tolerant Computing*, 2001, pp. 123–131.

Mehmet Sahinoglu (SM'93) received the B.S. degree from METU, Ankara, Turkey, and the M.S. degree from UMIST, England, both in electrical and computer engineering, and the Ph.D. degree from Texas A&M University, College Station, in electrical engineering and statistics.

He is the Eminent Scholar for the Endowed Chair of the Alabama Commission of Higher Education and Chairman of the Computer and Information Science Department at Troy University, Montgomery Campus since 1999. Following his 20-year-long tenure at METU, he was the first Dean and the founding Department Chair in the College of Arts and Sciences, DEU, Izmir, Turkey (1992–1997). He was a Chief Reliability Consultant to the Turkish Electricity Authority from 1982 to 1997. He became an Emeritus Professor at METU and DEU in 2000. He has taught at Purdue University, West Lafayette, IN (1989–1990, 1997–1998) and Case Western Reserve University, Cleveland, OH (1998–1999) as a Fulbright and a NATO scholar, respectively. He is accredited for the Compound Poisson Software Reliability Model to account for the multiple (clumped) failures in predicting the total number of failures at the end of a mission time, and the "MESAT: Compound Poisson Stopping Rule Algorithm" in cost-effective digital software testing. He is also jointly responsible with Dr. D. Libby for the original derivation of the "G3B (Generalized Three-Parameter Beta) pdf in 1981, also known as the Sahinoglu–Libby pdf in 1999.

He is a Fellow of the Society of Design and Process Science, a member of ACM, AFCEA, and ASA, and an elected member of ISI.

David L. Libby received the B.A. degree in mathematics from Carleton College, Northfield, MN, and the M.S. and Ph.D. degrees in statistics from The University of Iowa, Iowa City.

He has worked in computer software development for 23 years. Currently, he is a Consultant with IS Leaders, Minneapolis, MN, specializing in business architectures and project management.

Sunil R. Das (M'70–SM'90–F'94–LF'04) received the B.Sc. (Honors) degree in physics and the M.Sc. (Tech.) and Ph.D. degrees in radiophysics and electronics from the University of Calcutta, Calcutta, West Bengal, India.

He is an Emeritus Professor of Electrical and Computer Engineering with the School of Information Technology and Engineering, University of Ottawa, Ottawa, ON, Canada, and a Professor of Computer and Information Science, Troy University, Montgomery, AL. He previously held academic and research positions with the Department of Electrical Engineering and Computer Sciences, Computer Science Division, University of California, Berkeley, the Center for Reliable Computing (CRC), Computer Systems Laboratory, Department of Electrical Engineering, Stanford University, Stanford, CA (on sabbatical leave), the Institute of Computer Engineering, National Chiao Tung University, Hsinchu, Taiwan, R.O.C., and the Center of Advanced Study (CAS), Institute of Radiophysics and Electronics, University of Calcutta. He has published approximately 300 papers in the areas of switching and automata theory, digital logic design, threshold logic, fault-tolerant computing, BIST with emphasis on embedded cores-based system-on-chip (SOC), microprogramming and microarchitecture, microcode optimization, applied theory of graphs, and combinatorics. He has edited jointly with P. K. Srimani a book entitled, *Distributed Mutual Exclusion Algorithms* (Los Alamitos, CA: IEEE Computer Society Press, 1992) in its Technology Series. He is also the author jointly with C. L. Sheng of a text on digital logic design to be published by Ablex Publishing Corporation.

and a Regional Editor for Canada of the *VLSI Design: An International Journal of Custom-Chip Design, Simulation and Testing* (New York: Gordon and Breach). He is a former Administrative Committee (ADCOM) Member of the IEEE Systems, Man, and Cybernetics Society, a former Associate Editor of the IEEE TRANSACTIONS ON VLSI SYSTEMS (for two consecutive terms), a former Associate Editor of the *SIGDA Newsletter*, the publication of the ACM Special Interest Group on Design Automation, a former Associate Editor of the *International Journal of Computer Aided VLSI Design* (Norwood, NJ: Ablex), and a former Associate Editor of the *International Journal of Parallel and Distributed Systems and Networks* (Calgary, AB: Acta). He also served as the Co-Chair of the IEEE Computer Society Students Activities Committee from Region 7 (Canada). He was the Associate Guest Editor of the IEEE JOURNAL OF SOLID-STATE CIRCUITS Special Issues on Microelectronic Systems (Third and Fourth Special Issues), and Guest Editor of the *International Journal of Computer Aided VLSI Design* (September 1991), as well as *VLSI Design: An International Journal of Custom-Chip Design, Simulation and Testing* (March 1993, September 1996, and December 2001), Special Issues on VLSI Testing. He also Guest Edited jointly with Rochit Rajsuman a Special Section of the IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT in the area of VLSI Testing (Innovations in VLSI Test Equipments) published in October 2003. He is currently Guest Editing, jointly with R. Rajsuman, another Special Section of the IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT in the area of VLSI Testing (Future of Semiconductor Test) scheduled for October 2005. Dr. Das was elected a Fellow of the IEEE (with separate membership in the IEEE Computer Society, IEEE Systems, Man, and Cybernetics Society, IEEE Circuits and Systems Society, and IEEE Instrumentation and Measurement Society) for contributions to switching theory and computer design. He is a Member of the Association for Computing Machinery (ACM), USA. He is the 1996 recipient of the IEEE Computer Society's highly esteemed Technical Achievement Award for his pioneering contributions in the fields of switching theory and modern digital design, digital circuits testing, microarchitecture and microprogram optimization, and combinatorics and graph theory. He is also the 1997 recipient of the IEEE Computer Society's Meritorious Service Award for excellent service contributions to IEEE TRANSACTIONS ON VLSI SYSTEMS and the Society, and was elected a Fellow of the Society for Design and Process Science in 1998 for his accomplishments in integration of disciplines, theories and methodologies, development of scientific principles and methods for design and process science as applied to traditional disciplines of engineering, industrial leadership and innovation, and educational leadership and creativity. In recognition as one of the distinguished core of dedicated volunteers and staff whose leadership and services made the IEEE Computer Society the world's preeminent association of computing professionals, he was made a Golden Core Member of the Computer Society in 1998. Also, he is the recipient of the IEEE Circuit and Systems

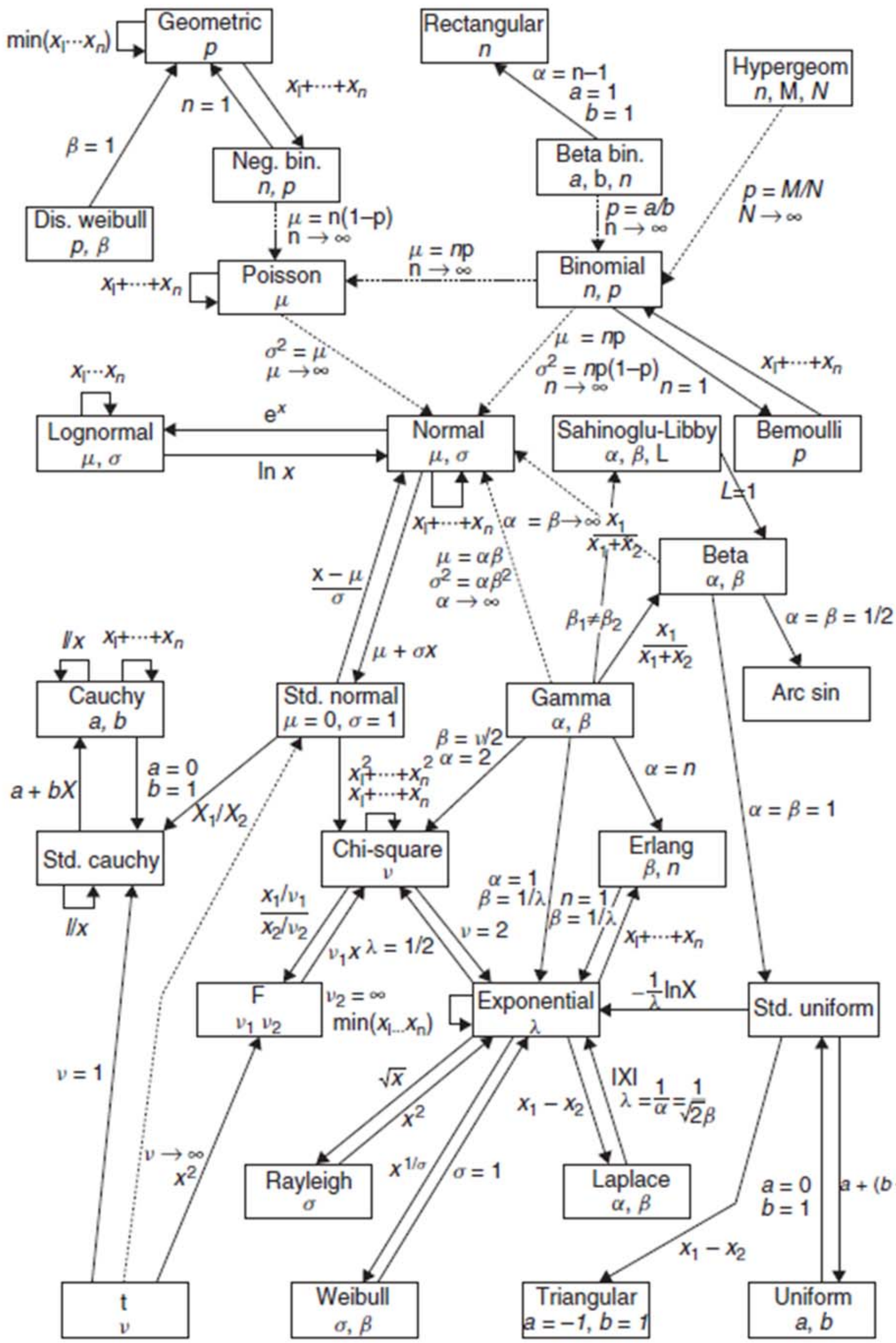


FIGURE 11 | Relationships for distributions in statistical simulation where $\alpha_1 = \alpha_2$ or $\alpha_1 \neq \alpha_2$, and $L = (\beta_1/\beta_2)$ for SL (α, β, L). (Dashed arrows indicate $\rightarrow \infty$ Reprinted with permission from Ref 20 Copyright 2007, Wiley & Sons, Inc)

RBD Tools Using Compression, Decompression, Hybrid Techniques to Code, Decode, and Compute Reliability in Simple and Complex Embedded Systems

Mehmet Sahinoglu, *Senior Member, IEEE*, and Chittoor V. Ramamoorthy, *Life Fellow, IEEE*

***Abstract*—A large amount of work is in progress on reliability block diagramming (RBD) techniques. Another body of dynamic research is in digital testing of embedded systems with very large scale integration (VLSI) circuits. Each embedded system, whether simple or complex, can be decomposed to consist of components (blocks) and interconnections or transmissions (links) within an s-source (input) and t-target (output) setup. There will be three tools proposed in this study. The first tool, using a novel "compression algorithm" is capable of reducing any complicated series-parallel system (not complex) to a visibly easy sequence of series and parallel blocks in a reliability block diagram by first finding all existing paths, then algorithmically compressing all redundant component duplications, and finally calculating an exact reliability and creating an encoding of the topology. A second tool is to decode and retrieve an already coded $s-t$ dependency relationship using post-fix notation for series-parallel or complex systems. A third tool is an approximate fast upper-bound (FUB) $s-t$ reliability computing algorithm designed for series–parallel systems, to perform state enumeration in a *hybrid* form assisted by the Polish encoding approach on non-series-parallel complex systems to compute the exact s (source)—t (target) reliability. Various examples illustrate how these tools work satisfactorily in unison. Further research with the OVERLAP method is in progress to reduce the computation speed by a thousand fold for a grid of 19 nodes without sacrificing any accuracy.**

***Index Terms*—Code–decode, complex, compression, hybrid, reliability block diagramming (RBD), series-parallel, $s-t$ reliability.**

I. Introduction and Motivation

RELIABILITY block diagramming (RBD) has been an active area of research for decades, even more so now with the advent of the embedded systems [1]–[11]. This paper explores to describe and compute the $s-t$ reliability in such (embedded) systems through an RBD approach. It is assumed that the input data required, such as reliability or availability including the aspect of security for each component and link in the RBD approach, is correctly facilitated by improving the very large scale integration (VLSI) testing techniques [24]–[30]. Earlier, simple or complicated series–parallel systems are studied to demonstrate that these networks can be encoded using a modified Polish notation employing postfixes [12], [17], [19]–[22]. The "compression" algorithm through a user-friendly and graphical Java application computes the reliability of any series–parallel network, no matter how large or complicated it is. Furthermore, the encoded topology can be transmitted remotely and then reverse-coded to reconstruct the original network diagram for purposes of securing classified information and saving space, a project which is also in progress nearing completion.

Interest in considering reliability during design of computer communications networks with a large number of nodes and connecting links, such as those found in hospitals, universities, electricity distribution, gas pipelines, military, or internet has increased in recent years. Due to geographical and physical constraints in such critical systems, designers at the initial or improvement stages usually base their decisions on approximate or upper-bound estimates of reliability to compute a given ingress (source) to egress (target) reliability. This practice may be deceptive, erroneous and overly optimistic due to computational complexity when reliability remains of a crucial importance that means human life and health.

The graphical screening ease and convenience of this algorithm are advantageous for planners and designers trying to improve system reliability by allowing a quick and efficient intervention that may be required at a dispatch center to observe routine operations and/or identify solution alternatives in case of a crisis.

The Boolean decomposition and binary enumeration algorithms or BDD [13]–[16] are outside the scope of this work, although it illustrates a new hybrid solution with the Polish notation. The proposed algorithm, through a user-friendly and graphical Java applet, computes the reliability of any complex series-parallel network. Furthermore, the coded topology can be transmitted remotely and then reverse-engineered to reconstruct the original network diagram for purposes of securing classified information and saving space.

All current exact computational algorithms for general networks are based on enumeration of states, minpaths, or mincuts [2], [3]. Network reliability estimation has been used successfully for nontrivial-sized networks using neural networks and heuristic algorithms in [7] and [8] as well as employing a "concurrent error detection" approach by the coauthor of this research as in [18]. Other researchers have used efficient Monte

Manuscript received August 12, 2004; revised July 8, 2005.
M. Sahinoglu is with the Department of Computer Sciences, Troy University, Montgomery, AL 36103 USA (e-mail: mesa@troy.edu).
C. V. Ramamoorthy is with the Department of Electrical Engineering and Computer Sciences, Computer Science Division, University of California, Berkeley, CA 94720 USA (e-mail: ram@csce.berkeley.edu).
Digital Object Identifier 10.1109/TIM.2005.855103

System for Insufficient Software Failure and Recovery Data. Izmir, Turkey: Springer-Verlag, Oct. 2000, pp. 25–27.
[10] K. E. Murphy and C. M. Carter, "Reliability block diagram construction techniques: Secrets to real-life diagramming woes," in *Proc. Ann. Reliability and Maintainability Symp.—Tutorial Notes RAMS03*, Tampa, FL, Jan. 2003.
[11] L. C. Woltenshome, *Reliability Modeling—A Statistical Approach*. London, U.K.: Chapman & Hall/CRC, 1999, pp. 106–107.
[12] M. Sahinoglu, J. Larson, and B. Rice, "An exact reliability calculation tool to improve large safety-critical computer networks," in *Proc. DSN2003*. San Francisco, CA, Jun. 22–25, 2003, pp. B-38–B-39.
[13] T. Luo and K. S. Trivedi, "An improved algorithm for coherent system reliability," *IEEE Trans. Rel.*, vol. 47, no. 1, pp. 73–78, Mar. 1998.
[14] S. Rai, M. Veeraraghavan, and K. S. Trivedi, "A survey on efficient computation of reliability using disjoint products approach," *Networks*, vol. 25, no. 3, pp. 174–163, 1995.
[15] X. Zang, H. R. Sun, and K. S. Trivedi, "A BDD approach to dependable analysis of distributed computer systems with imperfect coverage," in *Dependable Network Computing*, D. Avresky, Ed. Amsterdam, The Netherlands: Kluwer, 1999, pp. 167–190.
[16] H. Sun, X. Zang, and K. S. Trivedi, "A BDD based algorithm for reliability analysis of phase mission systems," *IEEE Trans. Rel.*, vol. 48, no. 1, pp. 50–60, Mar. 1999.
[17] M. Sahinoglu, "An exact RBD calculation tool to design very complex systems," in *Proc. 1st ACIS Int. Conf. Software Engineering Research Applications*, San Francisco, CA, Jun. 25–27, 2003. Invited talk.
[18] C. V. Ramamoorthy and Y. W. Han, "Reliability analysis of systems with concurrent error detection," *IEEE Trans. Comput.*, vol. 26, pp. 868–878, Sep. 1975.

Mehmet Sahinoglu (S'78–M'81–SM'93) received the B.S. degree from the Middle East Technical University (METU), Ankara, Turkey, and the M.S. degree from the University of Manchester Institute of Science and Technology (UMIST), Manchester, U.K., both in electrical and computer engineering, and the Ph.D. degree in electrical engineering and statistics from Texas A&M, College Station.

He is the Eminent Scholar for the Endowed Chair of the Alabama Commission of Higher Education (ACHE) and Chairman of the Computer and Information Science (CIS) at Troy State University, Montgomery, AL, since 1999. Following his 20-year-long tenure at METU as an Assistant/Associate/Full Professor, he served as the First Dean, and the Founding Department Chair in the College of Arts and Sciences at DEU, Izmir, Turkey, from 1992 to 1997. He was a Chief Reliability Consultant to the Turkish Electricity Authority (TEK) from 1982 to 1997. He became an Emeritus Professor at METU and DEU in 2000. He lectured at Purdue University, West Lafayette, IN (1989–1990, 1997–1998) and Case Western Reserve University, Cleveland, OH (1998–1999) in the capacity of a Fullbright, and a NATO Scholar, respectively.

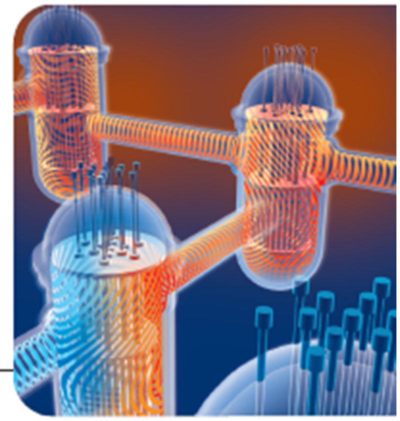
Dr. Sahinoglu is a Fellow of the Society of Design and Process Science (SDPS), a Member of ACM, AFCEA, and ASA and an Elected Member of ISI. He is accredited for the "Compound Poisson Software Reliability Model" to account for the multiple (clumped) failures in predicting the total number of failures at the end of a mission time, and the "MESAT: Compound Poisson Stopping Rule Algorithm" in cost-effective digital software testing. He is also jointly responsible with Dr. D. Libby for the original derivation of the Generalized Three-Parameter Beta (G3B) pdf in 1981, also known as Sahinoglu and Libby (SL) pdf in 1999.

Chittoor V. Ramamoorthy (M'57–SM'76–F'78–LF'93) received degrees in physics and technology from the University of Madras, Madras, India, two graduate degrees in mechanical engineering from the University of California, Berkeley, and the A.M. and Ph.D. degrees in electrical engineering and computer science (applied mathematics) from Harvard University, Cambridge, MA, in1964. His education at Harvard was supported by Honeywell Inc. with whom he was associated last as a Senior Staff Scientist.

He later joined the University of Texas, Austin, as a Professor in the Department of Electrical Engineering and Computer Science. After serving as Chairman of the Department, he joined the University of California, Berkeley, in 1972 as Professor of Electrical Engineering and Computer Sciences, Computer Science Division, a position that he still holds as Professor Emeritus. He has supervised more than 70 doctoral students in his career. He has held the Control Data Distinguished Professorship at the University of Minnesota, Minneapolis, and Grace Hopper Chair at the U.S. Naval Postgraduate School, Monterey, CA. He was also a Visiting Professor at Northwestern University, Evanston, IL, and a Visiting Research Professor at the University of Illinois, Urbana-Champaign. He is a Senior Research Fellow at the ICC Institute of the University of Texas. He has published more than 200 papers and has also coedited three books. He has worked on and holds patent in computer architecture, software engineering, computer testing and diagnosis, and in databases. He is currently involved in research on models and methods to assess the evolutionary trends in information technology. He is also the founding Co-Editor-in-Chief of the *International Journal of Systems Integration* and the *Journal for Design and Process Science*.

Dr. Ramamoorthy received the Group Award and Taylor Booth Award for education from the IEEE Computer Society, the Richard Merwin Award for outstanding professional contributions, and the Golden Core Recognition, and is the recipient of the IEEE Centennial Medal and the IEEE Millennium Medal. He also received the Computer Society's Kanai–Hitachi Award for the year 2000 for pioneering and fundamental contributions in parallel and distributed computing and the Best Paper Award in 1987. He was the cowinner (with Prof S. Das of Troy State University) of the IEEE's Best Paper Award—the Donald Fink Prize Paper Award for 2003 for their paper published in the December 2001 issue of the IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT. He is a Fellow of the Society of Design and Process Science from which he received the R. T. Yeh Distinguished Achievement Award in 1997. He also received the Best Paper Award from the IEEE Computer Society in 1987. Three international conferences were organized in his honor, and one UC Berkeley Graduate Student Research Award, and two International Conferences/Society Awards have been established in his name. and in 2002, he received its Gold Medal of Honor. He served as the Editor-in-Chief of the IEEE TRANSACTIONS ON SOFTWARE ENGINEERING. He is the founding Editor-in-Chief of the IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, which recently published a Special Issue in his honor. He served in various capacities in the IEEE Computer Society including its First Vice President, and a Governing Board Member. He served on several Advisory Boards of the Federal Government and of the Academia that include the United States Army, Navy, Air Force, DOEs, Los Alamos Lab, University of Texas, and State University System of Florida. He is one of the founding Directors of the International Institute of Systems Integration in Campinas, Brazil, supported by the Federal Government of Brazil, and for several years, was a Member of the International Board of Advisors of

Security Meter: A Practical Decision-Tree Model to Quantify Risk



Several security risk templates employ nonquantitative attributes to express a risk's severity, which is subjective and void of actual figures. The author's design provides a quantitative technique with an updated repository on vulnerabilities, threats, and countermeasures to calculate risk.

Mehmet Sahinoglu
Troy University

As part of my research to quantify risk in security risk assessment, I've devised and proposed Security Meter, a model that provides a purely quantitative and semiquantitative (hybrid) alternative to frequently used qualitative models,[1] such as Symantec's Enterprise Security Architecture (www.symantec.com). The proposed approach is a quick, bird's-eye-view way of calculating a system's information security risk (http://socrates.tsum.du/~mesa).

In this article, I also propose a modification of some of the decision-tree-based model's qualitative attributes, in case the quantitative data are unavailable. The proposed model is practical and simple to use for beginners in the field, but it also provides a mathematical–statistical foundation on which strategists or practitioners can construct a practical risk valuation. The probabilistic assumptions, such as using a uniformly distributed random variable for the input variables, can be improved by using other statistical distributions. Other techniques used hitherto within a nonprobabilistic frame, such as attack trees, don't provide an accurate overall picture of the risk to the system that's being protected.[2–4]

Risk scenarios

Conventionally, risk scenarios involve possible chance-based catastrophic failures with scarce modeling of maliciously designed human interventions that threaten inherent system vulnerabilities. Risk scenarios concerning critical computer communication networks are now more pervasive and severe than ever before because of the cost of nonmalicious chance failures that occur due to insufficient testing and lack of adequate reliability. We can use software reliability modeling and testing techniques to examine these chance failures in more detail.[5–8] However, for the intentional failures or malicious activities that critically increase the risk of ill-defined attacks, no one has ever thoroughly modeled a physical scenario, at least not one that considers a unified consistent scheme of vulnerabilities, threats, and countermeasures. A quantitative risk assessment provides results in numbers that management can understand, whereas a qualitative approach, although easier to implement, makes it difficult to trace generalized results. My proposed security-meter design fills a void in the arena of much-sought quantitative risk evaluation favorably compared to most current assessments that provide qualitative results. This is achieved by a probabilistically accurate quantitative model that measures security risk. The design's concrete numerical approach, which always works for all systems, can further facilitate security risk management and security testing. This means that the final risk measure calculated as a percentage can be tested, improved, compared, and budgeted as opposed to attributes such as high, medium, or low, which cannot be managed or quantified numerically for an objective assessment.[9]

Banks and other financial institutions, for example, employ several commercially available security risk templates, mostly in verbal or qualitative form, that express the severity of a risk by classifying them as low, medium, or high. This approach is not only highly subjective, but it also lacks any actual risk figures. Quantitative risk figures help mitigate or avoid future errors by allowing risk managers to objectively compare project alternatives and identify priorities for software maintenance. In existing analyses that favor a quantitative study, either a probabilis-

Testing Analog and Mixed-Signal Circuits With Built-In Hardware—A New Approach

Sunil R. Das, *Life Fellow, IEEE*, Jila Zakizadeh, Satyendra Biswas, *Member, IEEE*, Mansour H. Assaf, *Member, IEEE*, Amiya R. Nayak, *Senior Member, IEEE*, Emil M. Petriu, *Fellow, IEEE*, Wen-Ben Jone, *Senior Member, IEEE*, and Mehmet Sahinoglu, *Senior Member, IEEE*

***Abstract*—This paper aims to develop an approach to test analog and mixed-signal embedded-core-based system-on-chips (SOCs) with built-in hardware. In particular, oscillation-based built-in self-test (OBIST) methodology for testing analog components in mixed-signal circuits is implemented in this paper. The proposed OBIST structure is utilized for on-chip generation of oscillatory responses corresponding to the analog-circuit components. A major advantage of the OBIST method is that it does not require stimulus generators or complex response analyzers, which makes it suitable for testing analog circuits in mixed-signal SOC environments. Extensive simulation results on sample analog and mixed-signal benchmark circuits and other circuits described by netlist in HSPICE format are provided to demonstrate the feasibility, usefulness, and relevance of the proposed implementations.**

***Index Terms*—Built-in self-test (BIST), circuit under test (CUT), design-for-testability (DFT), mixed-signal test, oscillation-based BIST (OBIST), system-on-chip (SOC), test-pattern generator (TPG).**

I. Introduction

EVER-INCREASING applications of the analog and mixed-signal embedded-core-based system-on-chips (SOCs) [1], in recent years, have motivated system designers and test engineers to shift their research direction to embrace this particular area of very large-scale integrated circuits and systems to develop specifically their effective test strategies. The modern technology of manufacturing high-volume products demands that substantial efforts be directed toward the design, test, and evaluation of the prototypes before the start of the actual production cycle. An important objective to realize through detailed testing is to ensure that the manufactured products are free from defects and to simultaneously guarantee that they meet all the required specifications. Besides, the information that may be acquired through the process may ultimately help in increasing the product yield, thereby reducing the product cost. The integrated-circuit (IC) fabrication process involves photolithography, printing, etching, and doping steps. In the real-world situations, none of these steps is ever perfect, and the resulting imperfections may eventually lead to failures in the operation of the individual ICs. Specifically, the performance of mixed-signal ICs will be greatly degraded, since these circuits are very sensitive to even small imperfections in any step of the fabrication process. In the digital-circuit domain, however, some of these may be rather unimportant, but in mixed-signal circuits, imperfection in the form of small capacitance between the traces can present a significant circuit-parameter variation, thereby changing the circuit behavior drastically. Because of the shrinking of the circuit geometry, the circuit performance sensitivity is also enhanced. That is why every IC must be very rigorously tested before being shipped to their customers. The testing improves the overall quality of the final product, although it has no effect on the ICs' manufacturing excellence. Furthermore, the testing assures the product flawlessness when implemented during the key phases of a product development. Besides, it can also be a strategy for validating the design and checking processes. The high sensitivity of mixed-signal circuits to very small imperfections during process implementations and their broad specifications necessitate detailed and long performance tests as well. All these requirements eventually result in high test cost, thus forcing research efforts to be directed in the domain of mixed-signal testability [1]–[26]. Researchers are now seeking to combine both the analog- and the digital-circuits testing either by applying digital signals, such as serial bit streams to drive analog circuits, or by using analog signals to drive digital circuits.

The test methodologies for digital devices are already pretty well developed [27]–[34]. In contrast, analog-test methods are still so underdeveloped that analog test becomes a bottleneck in mixed-signal-test environment, particularly with the developments of semiconductor technology with high integration densities and shrinking sizes. Although analog and mixed-signal-test approach takes benefit from the digital-test development and experience, analog and mixed-signal tests are still

Manuscript received June 15, 2005; revised December 4, 2006. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada under Grant A 4750.

S. R. Das is with the Faculty of Engineering, School of Information Technology and Engineering, University of Ottawa, Ottawa, ON K1N 6N5, Canada, and also with the Department of Computer and Information Science, College of Arts and Sciences, Troy University, Montgomery, AL 36103 USA.

J. Zakizadeh, A. R. Nayak, and E. M. Petriu are with the Faculty of Engineering, School of Information Technology and Engineering, University of Ottawa, Ottawa, ON K1N 6N5, Canada.

S. Biswas is with the Department of Electrical Engineering Technology, Georgia Southern University, Statesboro, GA 30458 USA.

M. H. Assaf is with the University of Trinidad and Tobago, O'Meara Campus, O'Meara Industrial Park, Arima, Trinidad and Tobago.

W.-B. Jone is with the Department of Electrical and Computer Engineering, University of Cincinnati, Cincinnati, OH 45221 USA.

M. Sahinoglu is with the Department of Computer and Information Science, College of Arts and Sciences, Troy University, Montgomery, AL 36103 USA.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIM.2007.894223

An Input–Output Measurable Design for the Security Meter Model to Quantify and Manage Software Security Risk

Mehmet Sahinoglu, *Senior Member, IEEE*

***Abstract*—The need for information security is self-evident. The pervasiveness of this critical topic requires primarily risk assessment and management through quantitative means. To do an assessment, repeated security probes, surveys, and input data measurements must be taken and verified toward the goal of risk mitigation. One can evaluate risk using a probabilistically accurate statistical estimation scheme in a quantitative security meter (SM) model that mimics the events of the breach of security. An empirical study is presented and verified by discrete-event and Monte Carlo simulations. The design improves as more data are collected and updated. Practical aspects of the SM are presented with a real-world example and a risk-management scenario.**

***Index Terms*—Assessment, cost, countermeasure, data, management, probability, quantity, reliability, risk, security, simulation, statistics, threat, vulnerability.**

I. Introduction—Why Measure and Estimate the Inputs in the SM Model

QUANTITATIVE risk measurements are needed to objectively compare alternatives and calculate monetary figures for budgeting and for reducing or minimizing the existing risk. Security meter (SM) design provides these conveniences in a quantitative manner that is much desired in the security world [1], [7]–[11]. This is a follow up to [1] to create a simple statistical input–output design to estimate the risk model's parameters in terms of probabilities. In pursuit of a practical and accurate statistical design, security breaches will be recorded, and then, the model's input probabilities will be estimated using the equations that were developed. Undesirable threats that take advantage of hardware and software weaknesses or vulnerabilities can impact the violation and breakdown of availability (readiness for usage), integrity (accuracy), confidentiality, and nonrepudiation, as well as other aspects of software security such as authentication, privacy, and encryption [2]. Other methods such as Attack Trees [3], [4], Time-to-Defeat [5], and qualitative models [6] are only deterministic. Therefore, we must collect data for malicious attacks that have been prevented or not prevented [7]–[9]. Fig. 1 shows that the constants are the utility cost (asset) and criticality constant (between 0 and 1), whereas the probabilistic inputs are vulnerability, threat, and lack of countermeasure (LCM) of all risks between 0 and 1. The residual risk (RR: as in Fig. 2) and expected cost of loss (ECL) are the outputs obtained using (1)–(3). Fig. 3 will illustrate a software solution.

The black box in Fig. 1 leads to the probabilistic tree diagram of Fig. 2 to do the calculations.

Equations (1)–(3) summarize Figs. 1 and 2 from input to output. Suppose an attack occurs, and it is recorded. At the very least, we need to come up with a percentage of nonattacks and successful (from the adversary's viewpoint) attacks. Out of 100 such attempts, the number of successful attacks will yield the estimate for the percentage of LCM. We can then trace the root of the cause to the threat level backward in the tree diagram. Let us imagine that the anti-virus software did not catch it, and a virus attack occurs, which reveals the threat exactly. As a result of this attack, whose root threat is known, the e-mail system may be disabled. Then, the vulnerability comes from the e-mail itself. This way, we have completed the "line of attack" on the tree diagram, as illustrated in Fig. 2. Out of 100 such cyberattacks, which maliciously harmed the target cyberoperation in some manner, how many of them were not prevented or countermeasured by, e.g., smoke detectors or generators or antivirus software or firewalls installed? Out of those that are not prevented by a certain CM device, how many of them were caused by threat 1 or 2, etc., of certain vulnerability? We can then calculate the percentage of vulnerability A, B, or C. The only way wherein we can calculate the count of CM preventions is by doing either of the following: a) guessing a healthy estimator of an attack ratio, like 2% of all attacks are prevented by CM devices or b) using a countermeasuring device to detect a probable attack prematurely. The following equation computes the RRs for each activity in Table II for each leg:

$$\mathrm{RR} = \mathrm{Vulnerability} \times \mathrm{Threat} \times \mathrm{LCM}. \qquad (1)$$

II. Simple Case Study for the Proposed SM

The suggested vulnerability (weakness) values vary between 0.0 and 1.0 (or between 0% and 100%) to add up to one. In a probabilistic sample space of feasible outcomes of the random variable of "vulnerability," the sum of probabilities adds up to one. This is like the probabilities of the faces of a die, such as 1 to 6, totaling to one. If a cited vulnerability is not exploited in reality, then it cannot be included in the model or Monte Carlo (MC) simulation study. Vulnerability has from one to several threats to trigger the existing vulnerability. A threat is defined

Manuscript received April 27, 2007; revised August 17, 2007.
The author is with the Department of Computer Science, Troy University, Montgomery, AL 36103 USA (e-mail: mesa@troy.edu).
Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.
Digital Object Identifier 10.1109/TIM.2007.915139

On a New Graph Theory Approach to Designing Zero-Aliasing Space Compressors for Built-In Self-Testing

Sunil R. Das, *Life Fellow, IEEE*, Altaf Hossain, *Member, IEEE*, Satyendra Biswas, *Member, IEEE*, Emil M. Petriu, *Fellow, IEEE*, Mansour H. Assaf, *Member, IEEE*, Wen-Ben Jone, *Senior Member, IEEE*, and Mehmet Sahinoglu, *Senior Member, IEEE*

***Abstract*—The realization of space-efficient support hardware for built-in self-testing (BIST) is of great significance in the design of present-day very large scale integration (VLSI) circuits and systems, particularly in the context of the recent paradigm shift from system-on-board to system-on-chip (SOC). A new approach in designing zero-aliasing space-compaction hardware, specifically in relation to embedded core-based SOC, is proposed in this paper for single stuck-line faults, extending the well-known concepts of conventional switching theory and of incompatibility relation to generate the maximal compatibility classes using graph theoretic concepts, based on optimal generalized sequence mergeability, as developed and applied by the authors in earlier works. This is novel in the sense that zero-aliasing is obtained without any modification of the original module under test, while a maximal compaction is achieved in almost all cases in reasonable time utilizing some simple heuristics. The method is illustrated with design details of space compactors for the International Symposium on Circuits and Systems (ISCAS) 85 combinational and ISCAS 89 full-scan sequential benchmark circuits using simulation programs ATALANTA and FSIM, attesting to the usefulness of the technique for its relative simplicity, resulting in low area overhead, and full fault coverage for single stuck-line faults, thus making it suitable in a VLSI synthesis environment. With advances in computational resources in the future, the heuristics applied in the design algorithm may be further improved upon to significantly lower the simulation CPU time and storage.**

***Index Terms*—Aliasing-free (zero-aliasing) space compression, built-in self-testing (BIST) in very large scale integration (VLSI), core-based system-on-chip (SOC), maximal compatibility classes (MCCs), maximal minimally strongly connected (MMSC) subgraphs, nonminimally strongly connected (NSC) pairs of vertices.**

Manuscript received July 15, 2006; revised September 20, 2007. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada under Grant A 4750. A preliminary version of this paper was presented at the 23rd IEEE Instrumentation and Measurement Technology Conference, Sorrento, Italy, April 24–27, 2006.

S. R. Das is with the School of Information Technology and Engineering, Faculty of Engineering, University of Ottawa, Ottawa, ON K1N 6N5, Canada, and also with the Department of Computer and Information Science, College of Arts and Sciences, Troy University, Montgomery, AL 36103 USA (e-mail: das@site.uottawa.ca; sdas@troy.edu).

A. Hossain and E. M. Petriu are with the School of Information Technology and Engineering, Faculty of Engineering, University of Ottawa, Ottawa, ON K1N 6N5, Canada.

S. Biswas is with the Department of Electrical Engineering Technology, Georgia Southern University, Statesboro, GA 30460 USA.

M. H. Assaf is with the University of Trinidad and Tobago, Arima 7498, Trinidad and Tobago.

W.-B. Jone is with the Department of Electrical and Computer Engineering and Computer Science, University of Cincinnati, Cincinnati, OH 45221 USA.

M. Sahinoglu is with the Department of Computer and Information Science, College of Arts and Sciences, Troy University, Montgomery, AL 36103 USA.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIM.2007.910004

I. Introduction

An ENORMOUS amount of complexity has been brought about to the test-generation process of integrated circuits (ICs) due to very large scale integration. With the unprecedented growth of the electronics industry, the integration densities besides system complexities continued to increase, and hence, the need for better and more effective methods of testing to assure reliable operations of chips, which is the mainstay of today's many sophisticated devices and products, was intensely felt [1]–[56]. The concept of testing, in general, has a rather broad applicability and finding efficient testing techniques that can guarantee correct system performance is of huge practical significance. Generally, the cost of testing ICs is prohibitive, accounting for 35% to 55% of their total manufacturing expense. Furthermore, testing a chip is also time consuming, taking up to about one half of the total design-cycle time [4]. On the other hand, the amount of time available for manufacturing, testing, and marketing a product is constantly on the decline. Moreover, as a result of diminishing trade barriers and global competition, customers now demand products of superior quality at lower price. However, to achieve this better quality at relatively low cost, evidently, the testing strategies have to be improved. The conventional testing techniques of digital systems require application of test-input patterns generated by a test pattern generator (TPG) to the module under test (MUT) and comparing the responses with known correct responses. For large systems, because of higher storage requirements for the fault-free responses, the customary test procedures thus become highly expensive, and therefore, alternate approaches are aimed at minimizing the amount of needed storage [45], [52]–[54].

The testing techniques of ICs can be broadly classified into three main categories, viz., 1) testing of purely combinational circuits or full-scan synchronous sequential circuits using design-for-testability (DFT) techniques; 2) built-in self-testing (BIST) techniques that generate their own test vectors for circuits using built-in hardware; and 3) testing of general digital sequential circuits with test vectors that are externally generated and applied. For purely combinational circuits, there are available methods that can automatically generate tests with

International Journal of Computers, Information Technology and Engineering
Volume 4 • Number 2 • December 2010 • pp. 125-135

VALIDATION OF A SECURITY AND PRIVACY RISK METRIC USING TRIPLE UNIFORM PRODUCT RULE

Mehmet Sahinoglu

Director, Informatics Institute, Auburn University Montgomery, Montogomery

YanLing Yuan

Department of Computer Science, Troy University Montgomery

David Banks

Professory of Practice of Statistics, Department of Statistical Science, Duke University, Durhanm, USA

In the Security meter (SM) modeling for a quantitative risk assessment, about which a brief description is presented, one is required to take the product of three unidentical uniforms, U(a,b), which forms one leg of the many that constitute the total residual risk (TRR). The pdf of such a triple product of uniforms is certainly a challenge not encountered in the current literature. We have a complete agreement of the theoretical mean with the Monte Carlo Simulation average for large number of simulation runs. Variance from the summation of available legs will converge to simulation variance as the number of legs from TRR increases. However, variance for large number of runs from the simulations compares favorably with the analytical results so as to obtain a complete characterization for the Security Meter Quantitative Risk Probability Model. This work analytically (theoretically) validates the Monte Carlo simulation and vice versa. The same concept can be utilized for other applied fields where the triple product of uniforms is vitally needed. Authors will further find ways to improve this work by modifying the uniforms with triangular representations for the three random variables of interest.

Keywords: Statistical Analysis, Security Meter, CLT (Central Limit Theorem), Triple Uniform Product, Simulation, Risk

1. INTRODUCTION

In the security-meter modeling for quantitative risk assessment, one is required to take the product of three un-identical uniforms, U(a,b,c), which forms one leg of the many that constitute the total residual risk (TRR). Authors have studied a unique problem not challenged before. See Figure 1. Using the CLT, Central Limit Theorem, we sum the means and variances to find the approximate normal (Mean, Variance). We have a complete agreement of the theoretical mean with the Monte Carlo Simulation (MCSIM) average for large number of simulation runs using MAPLE software. Variance improves with the number of legs increasing and compares satisfactorily with the variance for large number of runs from the MCSIM results, such as n = 100,000. Therefore, the simulation mean and variance can be used to model the risk to imply that time-consuming and tedious MAPLE software calculations are not necessary every time results are sought (M. Sahinoglu, 2005, 2007, 2008; M. Sahinoglu, Yangling Yuan, David Banks, 2009. A brief description of the Security Meter (SM) method is illustrated below.

Figure 1 model illustrates the constants in the SM model as the utility cost (dollar asset) and criticality constant; the probabilistic inputs are vulnerability, threat, and lack of countermeasure all valued between 0 and 1. SM is described following the Figure 1 as follows (M. Sahinoglu, 2005, 2007):

Probabilistic Tree Diagram: Given that a simple sample system or component has two or more outcomes for each risk factor, vulnerability, threat, and countermeasure, the following

*Corresponding Author's: *msahinog@aum.edu*

Cybersystems and Information Security: Master of Science Program at Auburn University Montgomery

Mehmet Sahinoglu, *Senior Member, IEEE*

Abstract— Auburn University at Montgomery (AUM) proposed a Master of Science in Cybersystems and Information Security (CSIS) degree program, which was approved by ACHE (Alabama Commission on Higher Education) on December 4, 2009. AUM will be the first university in Alabama and Southeast to offer a program classified as 11.1003 by the Classification of Instructional Programs (CIP) coding system. The implementation date for this program will be the Fall Semester 2011 since the accreditation by SACS (Southern Association of Schools and Colleges) has been officially notified on December 14, 2010. The initial target audience for this program will be Air Force uniformed and civilian personnel located at Maxwell/Gunter AFB and related defense industry personnel associated with information technology (IT) contractors. IT community located in the AUM service area is included in this audience. This group is composed of employees of state/local governments, businesses, as well in- and out-of State graduate and undergraduate students. These projections are based on statitical surveys conducted by AUM to gauge interest. Course requirements will be listed for each semester and what makes this program unique will be discussed including resources. A conclusive summary of challenges since 2008 is presented at the end.

Index Terms- Cybersystems; ACHE; Information Security, SACS

I. Introduction

The Master of Science in Cybersystems and Information Security (CSIS) program will be a newly established graduate degree program designed to meet the security needs of national defense, government, and business sectors now, and in the future. Instructional delivery methods will utilize the latest technology already in place at AUM, both in the classroom and online. As the program begins, approximately 80% of classes will be taught in a traditional in-class lecture and/or laboratory setting with both day and (mostly) evening classes. Approximately 20% of classes will be taught through distance education formats. Distance education technology will be used in the delivery of courses and special topics presentations by experts in the field from across the nation. According to the U.S. Computer Emergency Readiness Team (US-CERT), Cybersecurity refers to the prevention, detection, and response to attacks on personal information that is stored within information systems [1].

Manuscript received on October 7, 2010. Mehmet Sahinoglu is the Director of Informatics Institute with Auburn University Montgomery in Montgomery Alabama 36124 USA. Tel: 334-244-3769, Fax: 334-244-3127. E-Mail: msahinog@aum.edu, URL:www.aum.edu/csis. This work was supported in part by the Ida Belle Young endowment toward academic research publications conducted by the AUM's Informatics Institute.

Potential attackers include "unfriendly governments and militaries, intelligence agencies, organized criminals, and hactivists" [2]. In April 2009, for example, news that cyberspies from hostile nations had disrupted the U.S. electrical grid caused a stir among intelligence and information security officials [3]. International events, such as enemy hackers' 2008 attack on the country of Georgia [4] and the 2007 attack on Estonia [5] suggest that cyberwarfare may in fact pose one of the greatest security threats to countries in the years to come.

Being located in the Alabama State capital, in close proximity to Maxwell/Gunter AFB (in particular the USAF 754th Electronic Systems Group), and centralized along the I-65 information technology corridor which is a hub to hundreds of technology-based contractual companies, the establishment of this program will fill a clearly identified societal need. The proposed program will not only prepare leaders who can implement, monitor, and respond to security issues, but will also train researchers who can develop original and innovative technologies to improve cybersystems security.

II. ASSESSMENT OF NEED AND PROGRAM PLANNING

There is an ever-increasing need in society for greater cyber systems and information security. This calls for the development of leaders who can implement, monitor, and respond to security issues, as well as researchers who can develop original and innovative technologies to improve cyber systems security. Within the last decade, cybersystems and information security have become increasingly significant priorities on the U.S. national political agenda. In the aftermath of September 11, and similar conflicts, and the subsequent political discourse on homeland security, this concern has been reflected in higher education, as colleges and universities began to introduce academic programs to provide specialized training in a brand new area.

To assess the educational need for a specialized program in Cybersystems and Information Security in the Southeast, Auburn University at Montgomery employed the Hanover Research Council to develop a research report on *The Viability of a New Master's Degree Program in Cybersystems and Information Security* [6]. The Hanover Research Council utilized the Integrated Postsecondary Education Data System (IPEDS) to identify a group of 24 institutions that offer graduate degree programs in Computer and Information Systems Security.

ACKNOWLEDGMENT

The author dutifully acknowledges his gratitude for many at AUM from Chancellor Dr. Veres with a clear "cyber vision" to its past and current Provost and Associate Provost as well its Dean of School of Science. Special thanks go to distinguished scientists and Informatics Institute Board Members who remotely supported, and/or assembled in November 2009 at Montgomery. They ranged from the University of California at Berkeley to Carnegie Melon University, and from the University of Pittsburgh, Purdue, and Integrated Computer Solutions, a local IT company and Maxwell AFB to the AUM's local Faculty and Staff. The author is also grateful to the Auburn University President Dr. Gouge, and Board of Trustees, as well as ACHE and SACS specialists during the course of 2009-2010 to elevate this program to its current completion in 2011. AUM Informatics Institute Board deserves a special recognition:

1) Prof. C.V. Ramamoorthy, CSE, Univ. of Cal., Berkeley, CA
2) Prof. Eugene H. Spafford, Dir., CERIAS-Purdue Univ., IN
3) Prof. James Joshi, Dir., LERSAIS- Univ. of Pittsburgh, PA
4) Prof. Kai Chang, Chair, CSSE, Auburn Univ., Auburn, AL
5) Stephen Goldsby, CEO, ICS, Montgomery, AL
6) Prof. Murat Tanik, ECE, UAB, Birmingham, AL
7) Col. Mary Griswold, HQ 754th ELSG, Maxwell AFB, AL
8) Dr. Karen Stine, Dean, School of Sciences, AUM, AL
9) Dr. Luis Cueva-Parra, School of Sciences, AUM, AL
10) Dr. Jeff Barksdale, Associate Provost, AUM, AL
11) Dr. Yaw-Chin Ho, Special Assistant to the Chancellor, AUM, AL
12) Dr. Bob Gehling, School of Business, AUM, AL
13) Dr. Jane Goodson, Dean, School of Business, AUM, AL
14) Dr. Jeffrey Elwell, Provost, AUM, AL
15) Dr. John Veres III, Chancellor, AUM, AL

REFERENCES

[1] US-CERT, "National Cyber Alert System," http://www.us-cert.gov/cas/tips/ST04-001.html. January 17, 2007.

[2] Jaikumar Vijayan, "Internet Warfare: Are We Focusing on the Wrong Things? A lack of vision and leadership have left the U.S. woefully unprepared for a cybercatastrophe," *ComputerWorld*, April 27, 2009.

[3] Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *The Wall Street Journal,* April 8, 2009 http://online.wsj.com/article/SB123914805204099085.html. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9131050.

[4] Brandon Griggs, "U.S. at Risk of Cyberattacks, Experts Say," *CNN.* http://www.cnn.com/2008/TECH/08/18/cyber.warfare/index.html.

[5] Joshua Davis, "Hackers Take Down the Most Wired Country in

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=338289.

[9] M. Sahinoglu, "A Case Study in Cyber Risk Education: Cybersystems and Information Security Graduate Degree Program at Auburn University Montgomery," Accepted for Presentation at CSEIT 2010, Hilton Phuket Arcadia Resort & Spa, Thailand, 6 - 7 December 2010.

[10] Siobhan Gorman, August Cole, and Yochi Dreazan, "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*. April 21, 2009. http://online.wsj.com/article/SB124027491029837401.html.

[11] Ben Bain, "Number of Reported Cyber Incidents Jumps," *Federal Computer Week.* February 17, 2009. http://www.fcw.com/Articles/2009/02/17/CERT-cyber-incidents.aspx.

[12] M. Sahinoglu, Trustworthy Computing: Analytical and Quantitative Engineering Evaluation. John Wiley & Sons, Hoboken, NJ. 2007.

Mehmet Sahinoglu (M'78–SM'93) is the founder Director of Informatics Institute in Auburn University at Montgomery. He obtained his Ph.D. from Texas A&M (1981) and his MS from UMIST, England (1975) both in EE. Following his 20 year-long tenure at METU (his alma mater, BS-ECE 1969-73) in Ankara as an Assistant-Associate-Full Professor, he served as the founding dean, and department chair in the College of Sciences at DEU in Izmir (1992-97). He taught at TAMU (1978-81) and Purdue (1989-90, 1997-98) and Case Western Reserve University (1998-99), as Fulbright fellow, and NATO research scholar respectively. He is a Fellow of Society of Design and Process Science www.sdpsnet.org and an elected member of International Statistical Institute.

Network reliability evaluation

Mehmet Sahinoglu[1]* and Benjamin Rice[2]

This article, beyond presenting a spectrum of network reliability methods studied in the past decades, describes a scalable innovative 'overlap technique' to tackle large complex networks' reliability evaluation difficulties, which cannot be handled by straightforward reliability block diagramming (RBD) techniques used for the simple parallel-series topologies. Examples are shown on how to apply the overlap algorithm to compute the ingress-egress reliability. Monte Carlo simulations demonstrate the methods discussed. (1) Static (time independent), (2) dynamic (time dependent) using a versatile Weibull distribution to represent the multiple stages of network components from infancy to useful life period and to wear-out, and (3) multistate versions to include derated behavior beyond conventional working and nonworking states, are illustrated for calculating the directional source-target (s-t) reliability of complex networks by using the Java software ERBDC: *Exact Reliability Block Diagramming Calculator*.
WIREs Comp Stat

Network reliability is the probability that a network with all its subnetworks and constituting components will successfully complete the task it is intended to perform under the conditions encountered for the specified period of time defined between a source and a target.[1–11] Reliability analysis is the process of quantifying a system's ingress–egress [or source–target (s–t) at will] serviceability by examining the dependency relationships between the components that comprise the system. Analysis is essential whenever the cost of failure is high.[12,13] Modeling and simulation allow analysts to determine weak spots in the systems so that the maintenance engineer can inventory a backup list of components. The reliability analysis focuses on the computer network components and the connections between them to determine the overall system reliability as well as the reliabilities between any two individual nodes in the network. Network reliability computations are similar to those developed for industrial applications, but there are a few exceptions. In industrial applications, all of the components in the system are usually considered critical to the overall function of the system. However, in network applications, the target communication between two nodes may select few components in the system due to redundancy.[11,14,15]

Currently, most published educational materials cover methods for determining system reliabilities in networks that can be expressed as pure parallel–series systems or reducing a complex topology to a parallel–series one using a conditional 'keystone' method.[10] However, as experience proves, these ready-to-cook networks with small sizes rarely occur outside textbooks and classrooms. These computations prove impossible or mathematically unwieldy when applied to real complex networks and are therefore useful only to teach basic reliability concepts.[11] The graphical screening ease and convenience of reliability block diagramming (RBD) algorithms[16] is advantageous for planners and designers trying to improve system reliability by allowing quick and efficient intervention that may be required at a dispatch center to observe routine operations and identify solution alternatives in case of a crisis. The Boolean decomposition and binary enumeration algorithms[17–19] are outside the practical scope of this article because of large networks we will work with. The algorithm through a user-friendly and graphical Java applet computes the reliability of any complex parallel–series network. Furthermore, the coded topology can be transmitted remotely and then reverse-engineered to reconstruct the original network diagram for purposes of securing classified information and saving space.[12,13,15,20–23,25] This, too, can be applied to security-related input for wired or wireless systems. All current exact

*Correspondence to: msahinog@aum.edu

[1]Informatics Institute, Auburn University, Montgomery, AL 36124, USA

[2]Computer Science Department, Troy University, Montgomery, AL 36104, USA

DOI: 10.1002/wics.81

I J C I T A E
© Serials Publications
6(1) 2012 : 9-15

COST-EFFECTIVE SECURITY TESTING OF CYBERSYSTEMSUSING COMBINED LGCP: LOGISTIC-GROWTH COMPOUND-POISSON

Mehmet Sahinoglu[1], Susan J. Simmons[2] and JamesH. Matis[3]

[1]*Auburn University Montgomery, Department of Cybersystems and Information Security, Montgomery, USA*
[2]*UNCW, Department of Mathematics and Statistics, Wilmington, USA*
[3]*Texas A & M University,Department of Statistics, College Station TX 77840, USA*

Abstract: A new challenge to software testing lies in the concept of a monitored security testing and most essentially in the determination of an epoch as to when to stop testing. Under minimum assumptions regarding growth of failures or breaches, due to chance (reliability) or malicious (security) reasons, we can objectively define an appropriate stopping rule to timely avoid further damage saving resources with a cost efficient plan. This research topic opens new avenues in a very critical area of cybersystems and information security defined to be "quantitative stopping rules in security testing" as compared to existing conventionally qualitative rules which do not lend themselves to probabilistic and cost-effective reasoning. We employ two probabilistic models to determine appropriate stopping rules and compare the approaches using two well-known data sets known as DR 4 and DR 5 (Sahinoglu, 2007).

1. INTRODUCTION

The damage inflicted by security breaches and software failures in computer and communication networks as experienced by related businesses or government entities is measured by multiples of billions of dollars. The analysis of such malicious activities as to when to act at the right moment to assure cost efficiency and maximum security are of a paramount interest to computer scientists and risk analysts, in addition to the business owners and their customers. In most situations, testing continues until the time-to-release date or the budget is depleted. This conventional subjective stopping decision inhibits the testers from understanding the extent of potential security breaches or failures when the product is released and can be extremely costly and inefficient. Herein, we consider two methods defining appropriate stopping rules in security testing, the logistic growth model (LGM) and the compound Poisson process model (CPM). These two methods model failure times based on probabilistic models and develop criteria-based stopping rules to support each other in synergy.

*Corresponding Author's: *msahinog@aum.edu*

There is another aspect of software security testing which deals with the functional testing of secure software (as in the metaphor of walking a high wire with a safety net), an entirely different domain and conceptually different than what this research paper addresses. The two common methods for testing whether software has met its security requirements are functional (Allen, Barnum, Ellison, McGraw, Mead, 2008) and risk-based security testing (McGraw, 2006). The methods proposed herein follow the latter risk-based testing derived from a risk analysis to encompass not only the high-level risks identified during the design process but also low-level risks derived from the software itself.

2. METHODS

The LGM was originally defined by Verhulst (1845) and used to model population growth of species for many years (Larralde-Corona et al., 1997; Matis *et al.*, 2009; Piegorsch and Bailer, 2005; Simmons *et al.*, 2009). The LGM has also been used to model software failures (Yamada *et*

Advanced Review

CLOUD computing

Mehmet Sahinoglu[1]* and Luis Cueva-Parra[2]

CLOUD computing (Grid or utility computing, computing on-demand) which was the talk of the computing circles at the end of 1990s has become once again a relevant computational topic. CLOUD computing, also considered as a fifth utility after water, electric power, gas, and telephony, is on the basis of the hosting of services on clusters of computers housed in server farms. This article reviews CLOUD computing fundamentals in general, its operational modeling and quantitative (statistical) risk assessment of its much neglected service quality issues. As an example of a CLOUD, a set of distributed parallel computers is considered to be working independently or dependently, but additively to serve the cumulative needs of a large number of customers requiring service. Quantitative methods of statistical inference on the quality of service (QoS) or conversely, loss of service (LoS), as commonly used customer satisfaction metrics of system reliability and security performance are reviewed. The goal of those methods is to optimize what must be planned about how to improve the quality of a CLOUD operation and what countermeasures to take. Also, a discrete event simulation is reviewed to estimate the risk indices in a large CLOUD computing environment favorably compared to the intractable and lengthy theoretical Markov solutions. *WIREs Comp Stat* 2011 3 47–68 DOI: 10.1002/wics.139

Keywords: CLOUD Computing; cyber-risk; security; reliability; discrete event simulation

INTRODUCTION AND MOTIVATION

CLOUD computing, an emerging form of computing using services provided through the largest network (Internet or CLOUD) is becoming a promising alternative to the traditional in-house IT computing services. CLOUD computing is a form of computing in which providers offer computing resources (software and hardware) on-demand. All of these resources are connected to the Internet and are provided dynamically to the users. Figure 1 shows a schematic representation of CLOUD computing. Here, CLOUD computing providers are connected to the Internet and able to provide computing services to both enterprise and personal users. Some companies envision this form of computing as a single major type of service which will be demanded extensively in the next decade. In fact, companies like Google, IBM, Microsoft, HP, Amazon, and Yahoo among others have already made investments not only in CLOUD research but also in establishing CLOUD computing infrastructure services (see Figure 1).

CLOUD computing services fall into three major categories[1]: (1) infrastructure as a service (IaaS), (2) software as a service (SaaS), and (3) platform as a service (PaaS). In IaaS virtualized servers, storage and networks are provided to the clients. SaaS is focused on allowing clients to use software applications through web-based interfaces. A service targeted to developers who focus primarily on application development only, without dealing with platform administration (operating system maintenance, load balancing, scaling, etc.), is called PaaS. Advances in virtualization, distributed computing, and high-speed network technologies have given further impetus to CLOUD computing. The major advantages of CLOUD computing are scalability, flexibility, resilience, and affordability. However, as users (companies, organizations, and individual persons) turn to CLOUD computing services for their businesses and commercial operations, there is a growing concern from the security and reliability perspectives as to how those services actually rate. The serviceability measurement can be categorized into three areas: performance, reliability, and security. Performance and reliability are two characteristics related to the condition of the providers' infrastructure and

*Correspondence to: msahinog@aum.edu

[1]Informatics Institute, Auburn University Montgomery, Montgomery, AL, USA

[2]Department of Mathematics, CS Option, Auburn University Montgomery, Montgomery, AL, USA

DOI: 10.1002/wics.139

IJCITAE
© Serials Publications
6(2) 2012 : 73-81

SOFTWARE ASSURANCE TESTING BEFORE RELEASING CLOUD FOR BUSINESS - A CASE STUDY ON A SUPERCOMPUTING GRID (XSEDE)

MEHMET SAHINOGLU[1], LUIS CUEVA-PARRA[2], SUSAN J. SIMMONS[3], SUNIL R. DAS[4]

[1]*Informatics Institute, Department of Cybersystems and Information Security, Auburn University Montgomery Montgomery, AL 36124*

[2]*Department of Mathematics - CS Option, Auburn University Montgomery, Montgomery, AL 36124*

[3]*Department of Mathematics and Statistics, University of North Carolina Wilmington, Wilmington, NC 28403*

[4]*Department of Computer Science, Troy University, Montgomery, AL 36103*

Abstract: There is a dire need to determine when best to release operations with respect to CLOUD computing to commercial use. CLOUD computing operations centers are multiplying rapidly and offering services to their clientele who believe that they are getting a good deal. However, "devil in the details" is the lack of an assumed reliability where customers soon discover that the services promised or claimed are not offering expected service reliability. This CLOUD reliability testing for assurance purposes opens new avenues in a very critical area of cybersystems and information security defined to be "quantitative stopping rules in reliability and security testing". This is a new research paradigm worth undertaking when compared to the existing and conventionally qualitative or rule-of-thumb rules which do not lend themselves to probabilistic and cost-effective reasoning. A case study on XSEDE, a continental supercomputing grid to be the world's largest, will be studied and discussed.

INTRODUCTION

Under minimum assumptions regarding growth of failures or breaches, due to chance (reliability) or malicious (security) reasons, we can objectively define an appropriate stopping rule to avoid further damage and save resources with a cost efficient plan. The stimulus behind this objective is that a new challenge existsto software testing for assurance lies in the concept of a monitored reliability testing and most essentially in the determination of an epoch as to when to stop testing.

We employ two probabilistic models combined to determine appropriate stopping rules and compare the approaches using historical failure and maintenance (interruption) data of the NSF supercomputing infrastructure XSEDE (akin to a super CLOUD) presented in part in Table 1 and Table 2 from March 2009 to March 2010, as well as in a popularly studied test data DR5. In general, the damage inflicted by reliability or security breaches and software failures in computer and communication networks, such as recently emerging.

CLOUD computing centers (Worthen *et al.*, 2009) experienced by related businesses or government entities is measured by multiples of billions of dollars (Sahinoglu *et al.*, 2011). See typical CLOUD representation in Figure 1. The analysis of such malicious and/or non-malicious activities as to when to act at the right moment to assure cost efficiency and maximum security are of a paramount interest to computer scientists and risk analysts, in addition to the business owners and their customers. In most situations, testing continues until the time-to-release date or the budget is depleted.

This conventional subjective stopping decision inhibits the testing company from understanding the extent of potential security breaches or reliability failures when the product is released, and can be extremely costly and inefficient. Herein, we consider comparing, and further merging the compound Poisson process model

significance
statistics making sense

Login | Register | Help?

WEB EXCLUSIVES MAGAZINE REVIEWS VIDEO EDUCATION SUBSCRIBE

HOME › WEB EXCLUSIVE ARTICLE

Search the site

A new metric for usability in trustworthy computing of cyber systems

Mehmet Sahinoglu, Scott Morton, Erman Samelo and Sukanta Ganguly

Recently, the concept of Usability Engineering (UE) is emerging to be a popular and pragmatic issue due to scarcity of resources. UE is generally concerned with human-computer interaction and specifically with making human-computer interfaces that have high usability or user friendliness. Usability is a science that deals with interaction between two end-points. One serves the interface and the other end consumes the information that can be presented via the interface. However we will add an original concept of quantification to the existing model through a designed algorithm by the author to calculate the usability (U) index. To accomplish this task owing to the field expertise of the corresponding author, numerical and/or cognitive data must be collected to supply the input parameters to calculate the quantitative risk index for Usability. A qualitative-input version of assessment will also be presented. This article will not only present a metric model but also generate a prototype numerical index, new in this field.

INTRODUCTION

Usability Engineering is regarded as one of the four pillars of the Trustworthy Computing, the others being Reliability, Security and Privacy[1]. Usability Engineering is a relatively new discipline, and was not even offered in computer science courses up to ten or fifteen years ago. Usability engineering is now central to proper software development. In this research paper, we will adopt a model of usability taking into account the task / user / user-interface variables, which have been inspired from Shackel, Nielsen and Eason[2]. Another strong source on Usability Engineering is by Nielsen[3]. Nielsen offers examples of measuring the Usability icons (such as ticket vending machines in Grand Central Stations or used by regular commuters, or stamp vending machines in Post Offices, or Personal Computers' usage of a certain piece of Software) and Usability testing as well as Usability Assessment methods beyond testing. Usability only becomes an issue when it is not present in an interface. In large part, an interface is usable when the user can accomplish their task smoothly without hindrance or frustration. Assessing the nature of usability quantitatively is the goal of this paper. To do so, a Usability Meter based on a series of questions designed to assess the user's perceptions of an interface's usability will be utilized. Based on the user's responses, a usability risk index will be calculated.

VULNERABILITIES

Inspired by Shackel, Nielsen and Eason[Ibid], three vulnerabilities are assessed: Task, User, and System Interface. Within each vulnerability category, questions pertain to specific threats and countermeasures. Within Task vulnerability, users are asked questions regarding Infrequency, Rigidity, and Unfavorable Situational Constraints threats and countermeasures. Within User vulnerability, users are asked questions regarding Lack of Knowledge, Lack of Motivation, and Lack of Choice threats and countermeasures. Within System Interface vulnerability, users are

Related Articles

- Turing test - the Loebner Prize
- Obama passes the Turing test
- Final Jeopardy: Man vs. Machine and the Quest to Know Everything
- Final Jeopardy: Man vs. Machine and the Quest to Know Everything
- IBM's Watson v Jennings and Rutter on Jeopardy!: was it a fair fight?
- How wise was Watson?
- IBM's Watson: wonder of the analytics age
- Privacy, data discs and realistic risk
- Digital doctoring: how to tell the real from the fake
- Bioinformatics: new science-new statistics?
- Does RIOT foretell the end of privacy?

Browse Categories

ENVIRONMENT & NATURE | SOCIAL SCIENCES | FINANCE & THE ECONOMY | FOOD & DRINK | OFFICIAL STATISTICS | HEALTH & MEDICINE | SCIENCE & TECHNOLOGY | SPORTS | HISTORY OF SCIENCE & STATISTICS

Are social networks risky? Assessing and mitigating risk

Mehmet Sahinoglu and Aysen Dener Akkaya

The number of Twitter users is growing quickly. Image: Wikimedia.

With the ever growing and unprecedented popularity of social networking sites such as Facebook, Google+, MySpace, Twitter etc. in the personal sphere, and others such as LinkedIn in business circles, undesirable security and privacy risk issues have emerged as a result of this extraordinary rapid ascent. The front ranking problems are mainly lack of trustworthiness; namely, those of breach of security and privacy. We employ a quantitative approach to assess security and privacy risks for social networks already under pressure by users and policymakers for breaches in both quality and sustainability, and will also demonstrate how to manage risk by using a cost-optimal game-theoretical solution. A number of real people (not simulated) were interviewed and the results are discussed. Ramifications of this quantitative risk assessment of privacy and security breaches in social networks will be summarized.

APPLICATION OF THE PROPOSED QUANTITATIVE RISK ASSESSMENT METHOD TO MEASURE AND MANAGE PRIVACY/SECURITY RISK IN SOCIAL NETWORKS

Fast Company reported that a Ph.D. candidate at Berkeley made headlines exposing a potentially devastating hole in the framework of Facebook's third-party application programming interface (API) which allows for easy theft of private information. This candidate and her co-researchers found that third-party platform applications for Facebook gave developers access to far more information (addresses, pictures, interests, etc.) than needed to run the app. A major reason social network security and privacy lapses exist simply results from the astronomical amounts of information the sites process each and every day. These flows of data make it much easier to exploit a single flaw in the system. Features that invite user participation such as messages, invitations, photos, open platform applications etc. are often the avenues used to gain access to private information.

The core of the matter, however, is to come up with a set of effective risk quantification and management techniques so as to help alleviate problems arising from lack of security and privacy due to the mushrooming social networks as well their connect services[1]. A well-known management proverb says, "what is measured is managed" and another says, "Yes, you can quantify risk" balanced against reasons such as the difficulty in collecting trustworthy data regarding security and privacy breaches[2]. The Security Meter technique provides a quantitative

Related Articles
- Analysing my Facebook friends
- Nowcasting the mood of the nation
- Unearthing the roots of riots
- Tweet de France - beware of the tweeting cyclist
- Facebook map of the world
- The emergence of digital governance
- Digital doctoring: how to tell the real from the fake
- Does RIOT foretell the end of privacy?

Browse Categories
ENVIRONMENT & NATURE | SOCIAL SCIENCES | FINANCE & THE ECONOMY | FOOD & DRINK | OFFICIAL STATISTICS | HEALTH & MEDICINE | SCIENCE & TECHNOLOGY | SPORTS | HISTORY OF SCIENCE & STATISTICS

Game-theoretic computing in risk analysis

Mehmet Sahinoglu,[1*] Luis Cueva-Parra[2] and David Ang[3]

Risk analysis, comprising risk assessment and risk management stages, is one of the most popular and challenging topics of our times because security and privacy, and availability and usability culminating at the trustworthiness of cybersystems and cyber information is at stake. The precautionary need derives from the existence of defenders versus adversaries, in an everlasting Darwinian scenario dating back to early human history of warriors fighting for their sustenance to survive. Fast forwarding to today's information warfare, whether in networks or healthcare or national security, the currently dire situation necessitates more than a hand calculator to optimize (maximize gains or minimize losses) risk due to prevailing scarce economic resources. This article reviews the previous works completed on this specialized topic of game-theoretic computing, its methods and applications toward the purpose of quantitative risk assessment and cost-optimal management in many diverse disciplines including entire range of informatics-related topics. Additionally, this review considers certain game-theoretic topics in depth historically, and those computationally resourceful such as Neumann's two-way zero-sum pure equilibrium and optimal mixed strategy solutions versus Nash equilibria with pure and mixed strategies. Computational examples are provided to highlight the significance of game-theoretic solutions used in risk assessment and management, particularly in reference to cybersystems and information security.

How to cite this article:
WIREs Comput Stat 2012. doi: 10.1002/wics.1205

Keywords: risk analysis; Nash equilibrium; game-theoretic; mixed strategy

INTRODUCTION TO GAMING AND HISTORICAL PERSPECTIVE TO GAME THEORY'S ORIGINS

Game playing is an unlimited topic in scope as old as the ancient human history. Although its first seeds were planted in the latter part of the 19th century, the popularity of game theory skyrocketed in the 20th century. This was a period of devastating wars and conflicts that needed urgently smart solutions with the advent of transistor-led electronics, and further, vast computer storage space and unprecedented computational speed. In the 21st century, the cyber wars brought forward a dire necessity to employ gaming solutions to outsmart the hostile hackers and adversaries, in lieu of former invading troops or bombarding warplanes. In retrospect, the first human hunters were involved in game solutions against their enemies, i.e., carnivorous animal world, who played the same game, all to quell hunger. Gaming may mean many things to different people, such as gambling or simulation or politics and warfare. According to Shubik,[1] the disciplines most heavily involved in the utilization of games have been management science and operations research, psychology, education, political science, sociology, engineering, computer and military science, and economics. The major expenditures, in terms of

*Correspondence to: msahinog@aum.edu

[1]Informatics Institute, 'Cybersystems and Information Security' graduate program, Auburn University at Montgomery, Montgomery, AL, USA

[2]Mathematics Department–CS Option, School of Sciences, Auburn University at Montgomery, Montgomery, AL, USA

[3]Information Systems and Decision Science, School of Business, Auburn University at Montgomery, Montgomery, AL, USA

Special Issue Paper **Environmetrics**

Received: 3 May 2012, Revised: 21 October 2012, Accepted: 27 October 2012, Published online in Wiley Online Library

(wileyonlinelibrary.com) DOI: 10.1002/env.2186

Ecological Risk-O-Meter: a risk assessor and manager software tool for better decision making in ecosystems†

Mehmet Sahinoglu[a]*, Susan J. Simmons[b], Lawrence B. Cahoon[c] and Scott Morton[a]

Increased awareness of environmental issues and their effects on ecological systems and human health drive an interest in developing computational methods to reduce detrimental consequences. For example, there are concerns regarding chlorofluorocarbons and their impact on stratospheric ozone, radon and its effect on human health, coal mining and effects on habitat loss, as well as numerous other issues. However, these issues do not exist in a vacuum nor occur just one at a time. There is a need to assess social and ecological risks comprehensively and account for numerous, inter-related potential risks. Given limited funds available for addressing these issues, how can spending for purposes of environmental and ecological mitigation be optimized? What is the magnitude of overall ecological risk for a given region? Novel software, the "Ecological Risk-o-Meter", addresses these questions and concerns. The software tool not only assesses the current environmental and ecological risks, but also takes into account potential solutions and provides guidance as to how spending can be optimized to reducing overall environmental risk. We demonstrate this new tool and show how to optimize the costs of risk reduction in recursive cycles based on feedbacks.

Keywords: ecological systems; vulnerability; threat; countermeasure; Risk-o-Meter

1. INTRODUCTION

There is not a day that passes when one does not hear or read about the adverse effects of climate change and consequent ecological damage occurring on our planet, which we have inherited and owe to the next generation to leave as well as or better than what we received. Recent events associated with global warming, such as record heat, drought, and more intense storms and hurricanes, have highlighted the continuing need to monitor, assess and mitigate ecological and environmental risks in a more holistic fashion. Traditional risk assessments were performed on a case by case basis rather than by using a systemic approach, as in the Ohio EPA DERR document (2008). It is rather a new trend to determine overall risk from a holistic viewpoint so that risk managers can take global, rather than incremental measures, as earth is connected through a common, freely circulating atmosphere and hydrosphere, and therefore, the communities exposed to risks are diverse. Such broad assessments of risk may be termed "ecological risk assessment" (ERA). According to Barnthouse and Suter (1986), ERA is the process of assigning magnitudes and probabilities of adverse effects of human activities or natural catastrophes. There are other resources where one can learn about ERA, such as the ones by Natural Resource Damages, http://www.epa.gov/superfund/programs/nrd/era.htm, and US Environmental Protection Agency http://www.epa.gov/oswer/riskassessment, as well as The Department of Energy & Environmental Protection in Canada, http://www.ct.gov/dep/cwp/view.asp?a=2715&depNav_GID=1626&q=325016.

"A Framework for Ecological Risk Assessment: General Guidance" by the Canadian Council of Ministers of the Environment defines ERA as a formal set of scientific methods for estimating the probabilities and magnitudes of undesired effects on plants, animals and ecosystems resulting from events in the environment, including the release of pollutants, physical modification of the environment and natural disasters. See a related website, http://www.ccme.ca/assets/pdf/pn_1195_e.pdf. In the same reference, a diagram from screening to preliminary and finally to a detailed quantitative ERA is illustrated in Figure 1. A detailed ERA as proposed is not only quantitative, dealing with a complex interaction, but it is also predictive and subject to statistical inference supported by expert field data rather than data obtained from hearsay through common literature.

* *Correspondence to: Dr. M. Sahinoglu, PO Box 244023, Informatics Institute, Auburn University at Montgomery, Montgomery, AL, 36124-4023, USA. E-mail: msa@aum.edu*

a *Informatics Institute, Auburn University at Montgomery, Montgomery, AL, 36124, USA*

b *Department of Mathematics and Statistics, University of North Carolina Wilmington, Wilmington, NC, 28403, USA*

c *Department of Biology and Marine Biology, University of North Carolina Wilmington, Wilmington, NC, 28403, USA*

† *This article is published in Environmetrics as a special issue on Modern quantitative methods for environmental risk assessment, edited by Lelys Bravo de Guenni, Cómputo Científico y Estadística, Universidad Simón Bolívar, Valle de Sartenejas. Carretera Baruta-Hoyo de La Puerta, Caracas, Miranda 1080-A, Venezuela, and Susan J. Simmons, Mathematics and Statistics, UNCW, 601 South College Road, Wilmington, NC 28403, U.S.A.*

Overview

Modeling and simulation in engineering

Mehmet Sahinoglu*

This review article will explore the innovative and popular theme of engineering modeling and simulation, predominantly in the manufacturing industry and cybersecurity world, citing severe challenges, advantages and time- and budget saving solutions and its future. The power of simulation is not an exaggeration but an understatement. The favorable outcomes since the advent of digital computers and software revolution could not have been achieved, especially without the multiple benefits of statistical simulation, which underlies the widespread use of modeling and simulation in engineering and sciences, stretching from A (Astronomy) to Z (Zoology). This refers not only to research findings in verifying a certain piece of theory, such as that of the recently discovered Higgs Boson, but in testing new products to innovate new discoveries so as to make our universe a more peaceful place by modeling and simulating the future projects and taking precautions before disasters occur. The review explores a cross section of engineering modeling and simulation practices illustrating a window of numerical examples.

How to cite this article:
WIREs Comput Stat 2013, 5:239–266. doi: 10.1002/wics.1254

Keywords: discrete event/Monte Carlo; modeling; production; cyber-security; Bayesian; multistate

INTRODUCTION AND BRIEF HISTORY TO SIMULATION AND MOTIVATION

Computer modeling and simulation (M&S), as programs or networks of computers mimicking the execution of an abstract model of many natural systems from physical and life sciences to social and managerial sciences, and primarily engineering, have become an integral part of digital experimentation. M&S proves useful to estimate the performance of complex engineering systems when too prohibitive for analytical solutions. A simulation is defined as the reproduction of an event with the use of scientific models. A model is a physical, mathematical, or other logical representation of a system, process, or phenomenon. Time-independent static Monte Carlo (MC) or conversely dynamic Discrete Event Simulation (DES) to manage events in real time for engineering applications will be reviewed. Taxonomy-wise, simulated computer models may be stochastic or deterministic, and dynamic or static, and discrete or continuous.

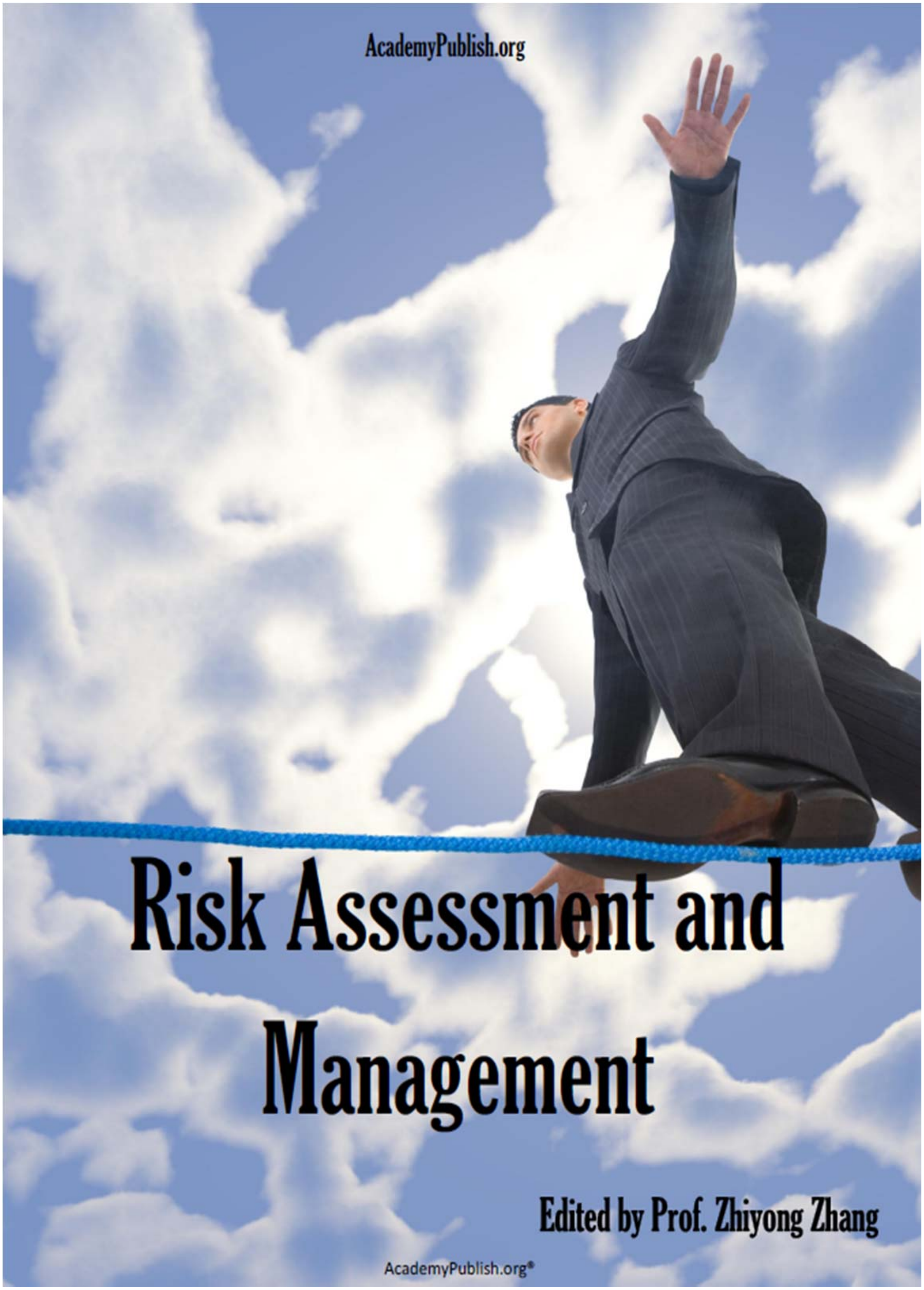
Modern computer simulation developed in parallel with the rapid-growth of computer use during the development of the Manhattan Project in WWII to nondestructively model and simulate the nuclear detonation before it was destructively dropped on Hiroshima and Nagasaki in Japan in 1945. Therefore, the history of simulation is interesting and intriguing. Some earliest pioneers can be observed in Ref. 1 Lord Rayleigh in 1899 showed that a one-dimensional random walk without absorbing barriers could provide an approximate solution to a parabolic differential equation. In 1908 W.S. Gosset (with a nickname, Student) used experimental sampling to

Additional Supporting Information may be found in the online version of this article.

*Correspondence to: msahinog@aum.edu

Informatics Institute, Cybersystems and Information Security, Auburn University at Montgomery, Montgomery, AL, USA

Conflict of interest: The author has declared no conflicts of interest for this article.


AcademyPublish.org
Risk Assessment and
Management
Edited by Prof. Zhiyong Zhang
AcademyPublish.org®

CLOUD Computing Risk Assessment and Management

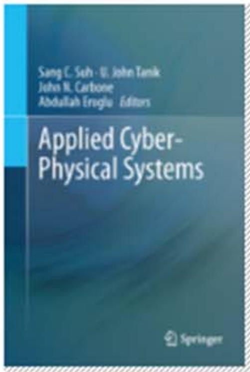
Mehmet Sahinoglu

ABSTRACT

CLOUD Computing is an emerging idea and technology with pros and cons, but the innovation definitely will leave its impact and footprints while facing new economic realities during the second decade of a new century. Rather than installing a series of commercial packages for each computer, including never ending security patches, users would only have to load one application. That application would allow workers to log on to a Web-based service which hosts all the programs the user would need for their job. Remote servers owned by the service provider would run everything from e-mail to word processing to complex data analysis programs. It's called CLOUD computing, the fifth utility (after electric power, gas, water and telephony) and it could change the way individuals and companies operate. However, as often apparent from the news media describing outages as simple glitches (usually downplayed by the CLOUD hosting companies and their providers or assigned responsible managers who boast about their 99.99% reliability), the crucial problem with CLOUD computing is its occasional, though dramatic lack of desired reliability and security. Both of these key features need to be duly and timely assessed in order to manage this new model of distributed computing, i.e. CLOUD. This chapter will examine methods and software programs that achieve these challenging goals, i.e. assessment and management hurdles from the CLOUD hosting (producer's risk) perspective in addition to the customer (consumer's risk) base, an avenue which has been examined before by the author. The purpose is to prioritize and cost-optimize the countermeasures needed to reach a desirable level of customer satisfaction as well as CLOUD hosting best practices. Quantitative methods of statistical inference on the Quality of Service (QoS) or conversely, Loss of Service (LoS), as commonly used customer satisfaction metrics of system reliability and security performance is reviewed. Subsequently, as an analytical alternative to the simulation practices, a CLOUD Risk-O-Meter approach is studied to assess risk and manage it cost optimally through an information gathering data-base type algorithm. The primary goal of those methods is to optimize plans to improve the quality of a CLOUD operation and what countermeasures to take. Among the simulation alternatives, a discrete event simulation (DES) is reviewed to estimate the risk indices in a large CLOUD computing environment to compare with the intractable and lengthy theoretical Markov solutions. In addition, Monte-Carlo VaR technique is introduced and summarized to compare and contrast with those of the DES.

INTRODUCTION

CLOUD computing services fall into three major categories (Leavitt, 2009): a) Infrastructure as a service (IaaS), b) Software as a service (SaaS) and c) Platform as a service (PaaS). These three structures are explained as follows. IaaS: Infrastructure-as-a-service products deliver a full computer infrastructure via the Internet through virtualized servers, storage and networks provided to clients. SaaS, the most popular of all, is focused on allowing clients to use software applications through web-based interfaces. The major idea behind SaaS is to lower costs to business and individuals from not having to purchase and maintain the software themselves. SaaS also assists with achieving standard product lines in lieu of encouraging organizations to adopt point solutions. Other advantages include increased uptime and shifting responsibility from administering and maintaining a network infrastructure out of the hands of organizations with other main purposes. SaaS in brief provides a complete, turnkey application - including complex programs. This software as a service in general is supposed to offer customers the overall benefits of CLOUD computing with enhanced information assurance. PaaS : Platform as-a-service products offer a full or partial application development environment that users can access and utilize on line, even in collaboration with others. The major advantages of CLOUD computing are scalability, flexibility, resilience, and affordability. However, as users (companies, organizations and individual persons) turn to CLOUD computing services for their businesses and commercial operations, there is a growing concern from the security and reliability perspectives as to how those services actually rate. Moreover, the federal government has approved commercial products to operate on a defense CLOUD, marking the first industry online offerings with this level of security accessible to the military via such an environment. As more clients migrate to the CLOUD and employ the technology, the cost of use will drop. This benefits anyone wishing to take advantage of offerings that include a suite of products designed to increase communications across the Web, social and contact center touch points (Boland, 2011). The absence of universal CLOUD standards to safeguard security can be a risky task; it is high time to do so. CLOUD computing diagrams are as follow:



Applied Cyber-Physical Systems

Suh, S.C.; Tanik, U.J.; Carbone, J.N.; Eroglu, A. (Eds.)

2014, XII, 253 p. 100 illus.

Available Formats:

eBook

Hardcover | **$199.00**
(net) price
ISBN 978-1-4614-7335-0
Usually dispatched within 3 to 5 business days.
» Add to marked items

Add to cart

Like 0 Tweet 0 +1 0

ABOUT THIS BOOK

Applied Cyber-Physical Systems presents the latest methods and technologies in the area of cyber-physical systems including medical and biological applications. Cyber-physical systems (CPS) integrate computing and communication capabilities by monitoring, and controlling the physical systems via embedded hardware and computers.

This book brings together unique contributions from renowned experts on cyber-physical systems research and education with applications. It also addresses the major challenges in CPS, and then provides a resolution with various diverse applications as examples.

Advanced-level students and researchers focused on computer science, engineering and biomedicine will find this to be a useful secondary text book or reference, as will professionals working in this field.

Content Level » Research

Keywords » CPS in Medical Systems - Critical Infrastructure - Cyberphysical systems (CPS) Research - High Integrity Systems

Related subjects » Communication Networks - Information Systems and Applications - Robotics - Signals & Communication

TABLE OF CONTENTS

Overview of Cyber-Physical Systems.- The Need for a Transdisciplinary Approach to Security of Cyber-Physical Infrastructure.- A Regional and Transdisciplinary Approach to Educating Secondary and College Students in Cyber-Physical Systems.- Cyber-Physical Systems and Stem Development: NASA Digital Astronaut Project- Radically Simplifying Cyber Security.- Cyber-Physical System Architectures for Dynamic, Real-Time "Need-to-Know" Authorization.- Cyber-Physical Systems Security.- Axiomatic Design Theory for Cyber-Physical Systems.- The Importance of Grain Size in Communication within Cyber-Physical Systems.- Focus, Salience, and Priming in Cyber-Physical Intelligence.- An Adaptive Cyber-Physical System Framework for Cyber-Physical Systems Design Automation.- Cyber-Physical Eco-Systems.- Risk Assessment and Management to Estimate Hospital Credibility Score of Patient Health Care Quality.- Use of Session Initiation Protocol in Multimedia Communications.- Principle of Active Condition Control.- Long Range Wireless Data Acquisition Sensor System for Health Care Applications.- Performance Improvement of RFID Systems.- Thinking Embedded, Designing Cyber-Physical.

Chapter 13
Risk Assessment and Management to Estimate and Improve Hospital Credibility Score of Patient Health Care Quality

Mehmet Sahinoglu and Kenneth Wool

Introduction

The purpose of this chapter is to study how to assess patient-centered health-care quality and as a follow-up, how to mitigate the unwanted risk to a tolerable level, through automated software utilizing game-theoretic risk computing. This chapter overall seeks methods about how to improve patient-centered quality of care in the light of uncertain nationwide health care quality mandate to disseminate and utilize results for the "most bang for the buck". A patient-centered composite 'credibility' or 'satisfaction' score is proposed for the mutual benefit of patients seeking quality care, and hospitals delivering the promised healthcare, and insurance companies facilitating a financially accountable healthcare. Patient-centered quality of care risk assessment and management are inseparable aspects of health care in a hospital, yet both are frequently overlooked. In Alabama State, a 2004 study by the Kaiser Family Foundation found substantial dissatisfaction with the quality of health care. In response to whether they were dissatisfied with the quality of healthcare, 44 % of Latinos, 73 % of Blacks, and 56 % of Whites said "Yes". When asked whether health care has gotten worse in the prior five years prior, 39 % of Latinos, 56 % of Blacks, and 38 % of Whites reported dissatisfaction [1].

Being overly optimistic, and not considering or preparing for possible detrimental events could be severely damaging to both the patient and hospital management. Characterizing and assessing the patient-centered quality of care

M. Sahinoglu (✉)
Informatics Institute, Cybersystems and Information Security, Auburn University at Montgomery(AUM), Montgomery, AL 36124, USA
e-mail: msahinog@aum.edu

K. Wool
Cardiology, Central Alabama Veterans Health Care System, 215 Perry Hill Road, Montgomery, AL, USA
e-mail: drwooke@yahoo.com

S. C. Suh et al. (eds.), *Applied Cyber-Physical Systems*, 149
DOI: 10.1007/978-1-4614-7336-7_13,

Informatics Institute

Home » Departments » Informatics Institute » Master of Science in Cybersystems & Information Security »

- Programs & Degrees
- Message from the Dean
- Advising
- Departments
- Biology
- Informatics Institute
- Master of Science in Cybersystems & Information Security
- SDPS Transdisciplinary Conference
- Informatics Institute
- Justice & Public Safety
- Mathematics
- Military Sciences/ROTC
- Physical Science
- Political Science & Public Administration
- Psychology
- Online Programs & Degrees
- Pre-professional programs
- Faculty Scholarship and Research
- Undergraduate Research
- Student internships
- Sciences To Go! SOS Speaker's Bureau
- Sciences To Do! Activities for Citizen Scientists
- Student FAQs
- Supporting the SOS mission
- Dean's Office Contacts

Graduate Assistantships Available for New and Current Graduate Students in Cybersystems and Information Security!

Application Deadline EXTENDED: **July 31, 2013**

Master of Science in Cybersystems & Information Security

You understand a world that most people don't even know exists: Security Informatics. Ask the average guy on the street what "Applied Cryptology" is and you'll get a blank stare. But for you, it's good news because it's the title of a core class you'll be taking if you enroll in AUM Graduate Studies for a master of science in cybersystems and information security.

This isn't just some fancy-sounding IT degree like you could get anywhere else. This is elevated instruction in an industry that in many ways runs the modern world. Companies depend on people like you to keep their business intact. AUM makes sure those people remain on the cutting edge.

Click here for complete details about the program's accreditation and other official documentation.

Upon graduation, a student in this program will be able to do the following with confidence:

- Identify and respond to information security challenges in distributed and embedded systems.
- Evaluate and recommend technological tools and protocols to protect against risks.
- Integrate the use of encryption technology in non-secure and non-private computers and systems.
- Design and conduct research in the area of cybersystems and information security.

This master's degree will arm you with the skills to develop original, innovative technologies that improve cybersystems security. You'll be ready to troubleshoot large-scale information networks and distributed systems. And you'll know exactly how to mitigate system vulnerabilities and restore compromised services.

Your program will include courses like:

- Network Security & Reliability-Quantitative Metrics
- Secure Software Systems
- Computer Systems Modeling & Simulation
- Financial Accounting/Integrated Business Concepts

Click here for the list of courses and more information on the curriculum.

Chances are, you've already discovered your interest and natural aptitude for this industry. AUM is here to help you develop that skill to a professional level that surpasses even your own expectations.

So, if you're ready to expand your capabilities and increase your earning potential, apply to AUM Graduate Studies M.S. in Cybersystems and Information Security. To learn more, contact us today.

Related careers/job titles: Homeland security, government and state agencies, private business, armed forces, information technology.

Approximate program length: Two years

To learn more, call **334-244-3769** or email **msahinog@aum.edu**

Home » Departments » Informatics Institute » Accreditation and Official Documents »

- Master of Science in Cybersystems & Information Security
- SDPS Transdisciplinary Conference
- Informatics Institute

Frequently Asked Questions about the CSIS Program and Curriculum

Graduate Assistantships Available for New and Current Graduate Students in Cybersystems and Information Security!

Application Deadline EXTENDED: **July 31, 2013**

Click here for complete details!

Accreditation, Foundational Documents, and Other Documentation

The Master of Science in Cybersystems and Information Security was the first of its kind in Alabama, having been approved by the Alabama Commission on Higher Education in 2009 and the Southern Association of Colleges and Schools in 2010. In 2011, the first students were enrolled.

See below for official documentation regarding the establishment, approval, and curriculum of the program.

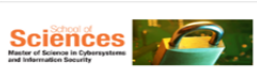
ACHE Approval: 2009

SACS Approval: 2010

Letters of Support

Notification from National Security Agency regarding NIEPT Certification

GSTF International Journal in Computing article detailing the process by which AUM's Cybersystems and Information Security master's degree was developed and introduced.



Download the M.S. in Cybersystems and Information Security brochure here.

Master of Science in Cybersystems & Information Security

SDPS Transdisciplinary Conference

Informatics Institute

New:
Graduate Assistantships Available for New and Current Graduate Students in Cybersystems and Information Security!

Application Deadline:
May 31, 2013

Click here for complete details!

Download the Cybersystems and Information Security brochure here.

Cybersystems and Information Security Courses

The Master of Science in Cybersystems and Information Security offers courses that provide you with the skills and knowledge to prepare for your career. Learn more about the curriculum and each course below.

Master of Cybersystems and Information Security: Semester-by-Semester Curriculum Model

Year 1 Fall Semester (9 credits)
CSIS 6003: Introduction to Computer Security - 3 credits
CSIS 6003: Introduction to Computer Security

CSIS 6010: Data Communications and Computer Networks- 3 credits
CSIS 6010: Data Communications and Computer Networks

CSIS 6020: Distributed Systems - 3 credits
CSIS 6020 COMP 7330: Advanced Parallel and Distribution Computing with Many-Core GPGPU

Year 1 Spring Semester (9 credits)
CSIS 6013: Network Security and Reliability - Quantitative Metrics – 3 credits
CSIS 6013: Network Security and Reliability - Quantitative Metrics

CSIS 6033: Secure Software Systems – 3 credits
CSIS 6033: COMP 6700: Software Process

CSIS 6040: Applied Cryptology – 3 credits
CSIS 6040: Applied Cryptology

Year 2 Fall Semester (9 credits)
CSIS 6053: Information Security Management – 3 credits
CSIS 6053: Information Security Management

CSIS 6403: Computer Systems Modeling and Simulation - 3 credits
CSIS 6403: Computer Systems Modeling and Simulation

ACCT 6180: Financial Accounting Integrated Business Concepts - 3 credits
ACCT 6180: Financial Accounting Integrated Business Concepts

Year 2 Spring Semester (9 credits)
Non-thesis option
QMTD 6750: Operations Research – 3 credits
QMTD 6750: Operations Research

CSIS 6912- Supervised Practicum with Cyber-Industry Experience – 3 credits
CSIS 6912: Supervised Practicum - Cyber-Industry Experience

CSIS 6952- Security Policy Seminar: Healthcare, Finance or Government – 3 credits***
CSIS 6952: Security Policy Seminars - Healthcare, Finance, or Government

April 16, 2013

AUM recently applied to the National Information Assurance Education and Training Program (NIETP) of the National Securit Agency for certification that the Cybersystems and Information Security degree meets the organization's stringent standards.

The application was a success. Information Assurance Courseware Evaluation (IACE) Program evaluators certified AUM course-ware as meeting all of the elements of the Committee o National Security Systems (CNSS) National Training Standard f information systems security professionals.

In June 2013, AUM will receive recognition and an official certificate. The IACE Program provides consistency in training and education for the information assurance skills that are critic to our nation's security.

AUM's CSIS graduate program reached this milestone after only two full academic years. In 2010, the program was first accredited and, in 2011, its first students enrolled.

Click here for the official memo regarding the certification from the National Security Agency.

Degree Program

The Informatics Institute offers the M.S. in Cybersystems and Information Security. Click the link to learn more about the program.

For information on graduate admissions, click here.

Cybersystems & Information Security Degree Brochure

Auburn University at Montgomery is Alabama's first program to offer a master's in cybersystems and information security to train future leaders in the field of information and network security. **more**

Internet Security Radio Clips

WSFA 12 Talk Appearance

WSFA talks with Program Director Dr. Sahinoglu and instructor Joel Junker about the Master of Science in Cybersystems and Information Security

Informatics Gets Donation

Integrated Computer Solutions, a Montgomery-based information security and technology consulting firm, recently donated approximately $70,000 in cutting-edge computer equipment to the Informatics Institute to help further the

Dr. Sahinoglu talks about CSIS at the Eisenhower Lecture Series

Informatics class at a panel discussion at the Eisenhowe National Security Lecture Series at AUM

News

First CSIS student graduates at fall commencement

by Buffy Lockette | Dec 16, 2013

More than 340 students graduated from Auburn University at Montgomery during its fall commencement exercises on Saturday. Among those receiving degrees was Erman E. Samelo, the university's first graduate from its Master of Science in Cybersystems and Information Security program.

Samelo enrolled at Auburn Montgomery in 2011 upon retiring from the U.S. Air Force as superintendent of the Education Support Squadron at the Spaatz Center for Officer Education at Maxwell Air Force Base. With 23 years of experience in information management, he decided to embark on a second career in information security and turned to AUM for training.

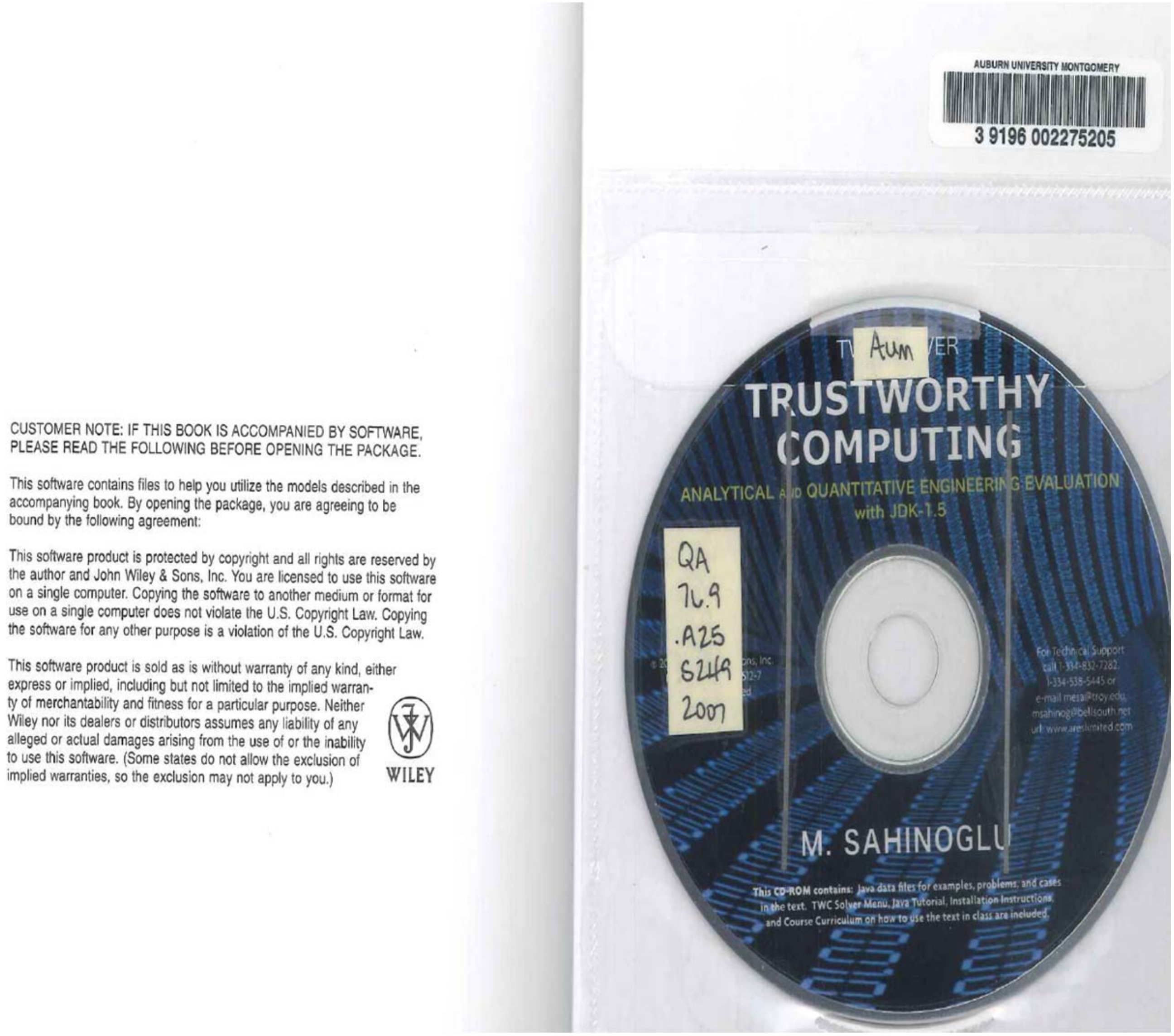
"When I was still in the Air Force, my job was the one that implemented information security policies," said Samelo. "The CSIS master's program at AUM taught us why policy makers want those policies implemented. This was a challenging program and I know that the knowledge I gained from it will help me in my next career. I woulddefinitely recommend it to others."

Established in 2010, AUM's cybersystems and information security program is the first program of its kind in Alabama. It prepares students to become leaders in the field of information and network security, offering instruction and research opportunities thatprovide graduates with the necessary knowledge and skills to effectively assess, develop, and manage secure information networks and respond to newly developed threats

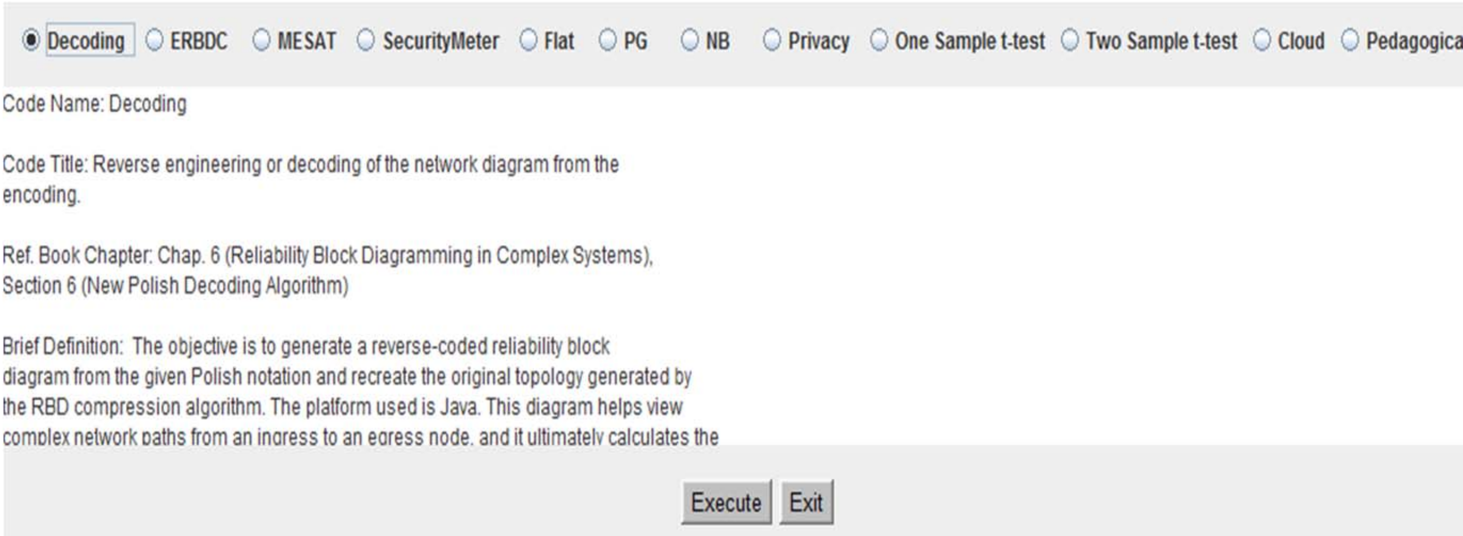
Students are prepared for careers in homeland security, government and state agencies, private businesses, and armed forces. The program is certified by the Committee on National Security Systems, approved by the Alabama Commission on Higher Education, and accredited by the Southern Association of Colleges and Schools.

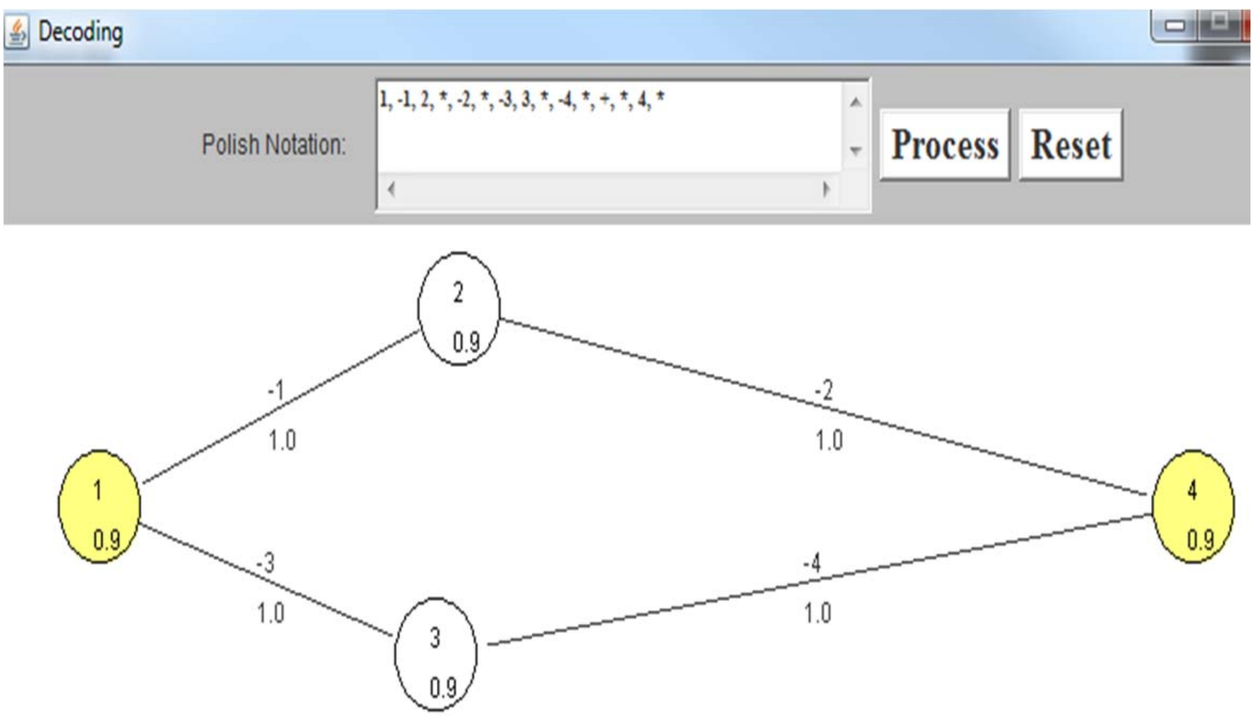
Learn more about the program at www.aum.edu/csis or by contacting program director Mehmet Sahinoglu at 334-244-3769 or msahinog@aum.edu.

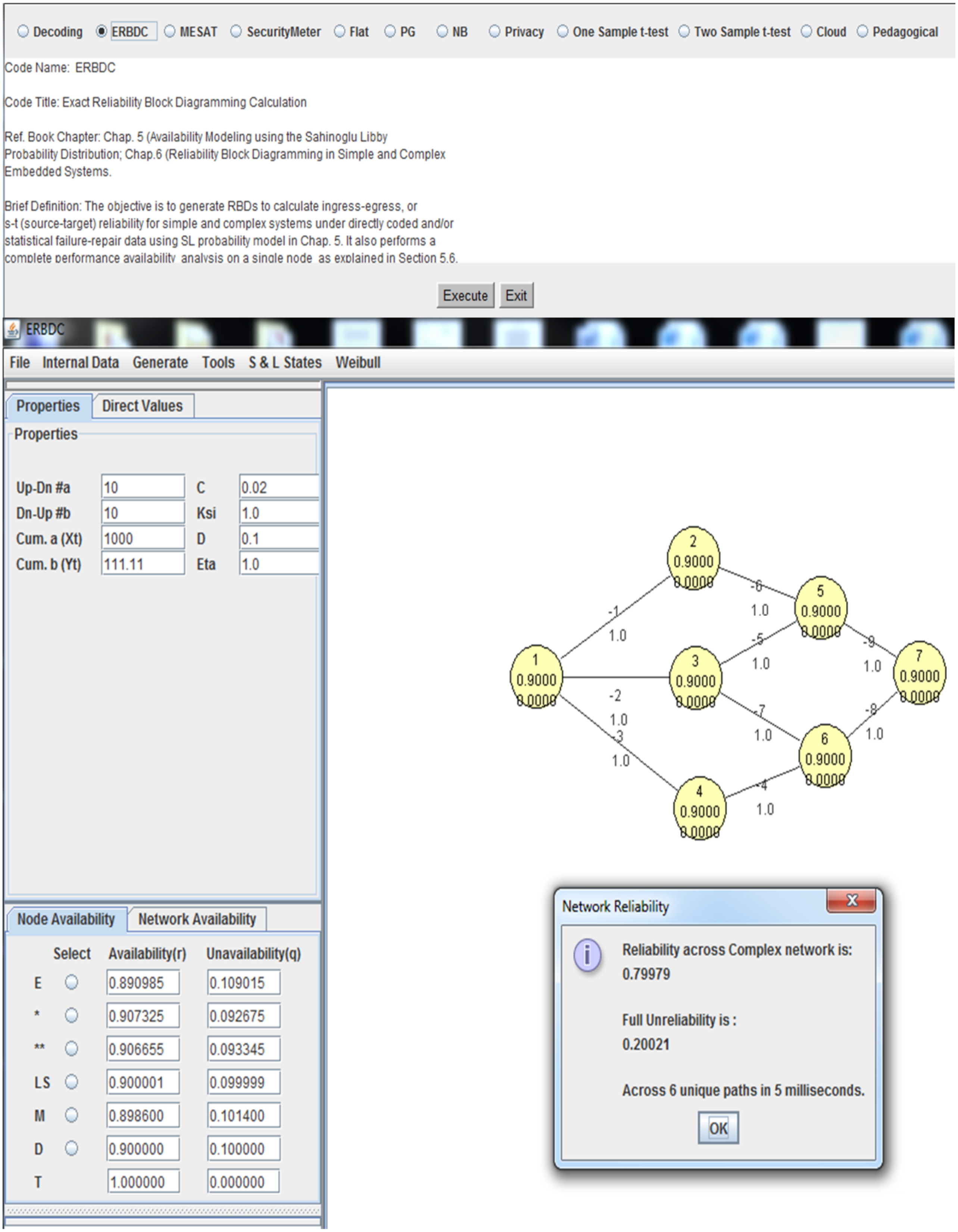
Samelo graduated during AUM's afternoon commencement ceremony at 2 p.m. on Saturday, along with graduates from the Schools of Sciences, Nursing, and Liberal Arts. At 10 a.m., students from the School of Education and College of Business received degrees. Benedict Okeke, AUM microbiology professor, served as keynote speaker.

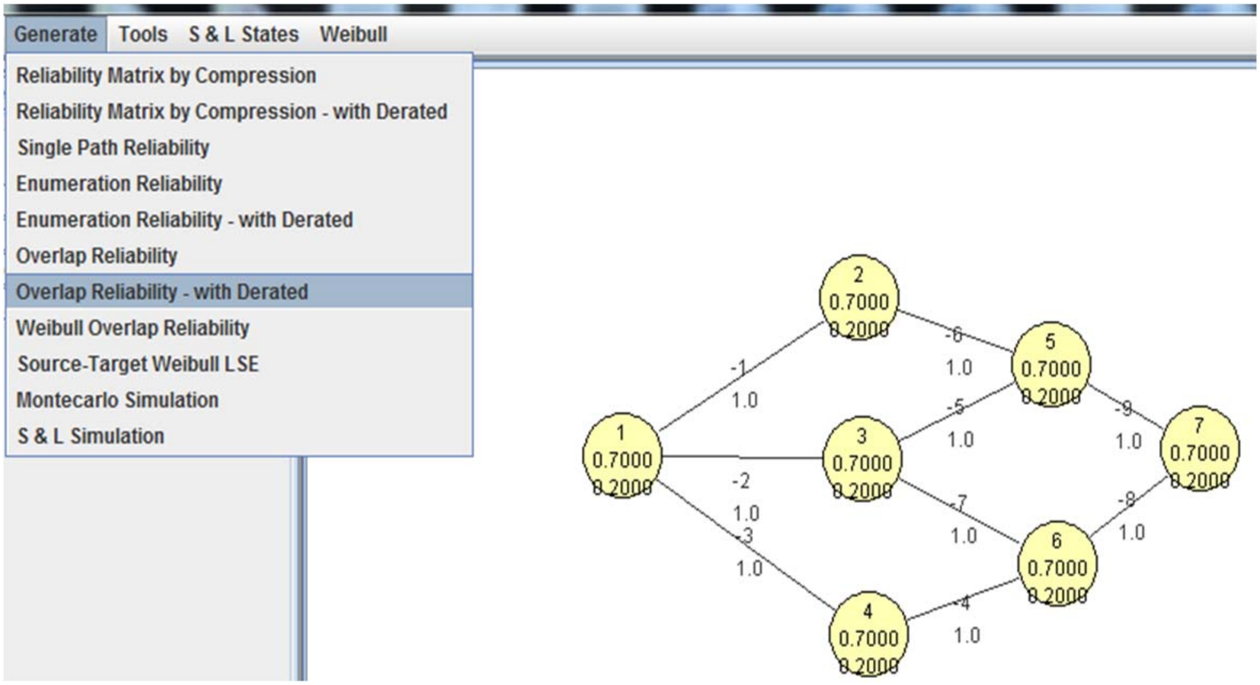

AUBURN UNIVERSITY MONTGOMERY
3 9196 002275205
CUSTOMER NOTE: IF THIS BOOK IS ACCOMPANIED BY SOFTWARE, PLEASE READ THE FOLLOWING BEFORE OPENING THE PACKAGE.
This software contains files to help you utilize the models described in the accompanying book. By opening the package, you are agreeing to be bound by the following agreement:
This software product is protected by copyright and all rights are reserved by the author and John Wiley & Sons, Inc. You are licensed to use this software on a single computer. Copying the software to another medium or format for use on a single computer does not violate the U.S. Copyright Law. Copying the software for any other purpose is a violation of the U.S. Copyright Law.
This software product is sold as is without warranty of any kind, either express or implied, including but not limited to the implied warranty of merchantability and fitness for a particular purpose. Neither Wiley nor its dealers or distributors assumes any liability of any alleged or actual damages arising from the use of or the inability to use this software. (Some states do not allow the exclusion of implied warranties, so the exclusion may not apply to you.)
WILEY
TRUSTWORTHY
COMPUTING
with JDK-1.5
QA 76.9 .A25 S249 2007
M. SAHINOGLU

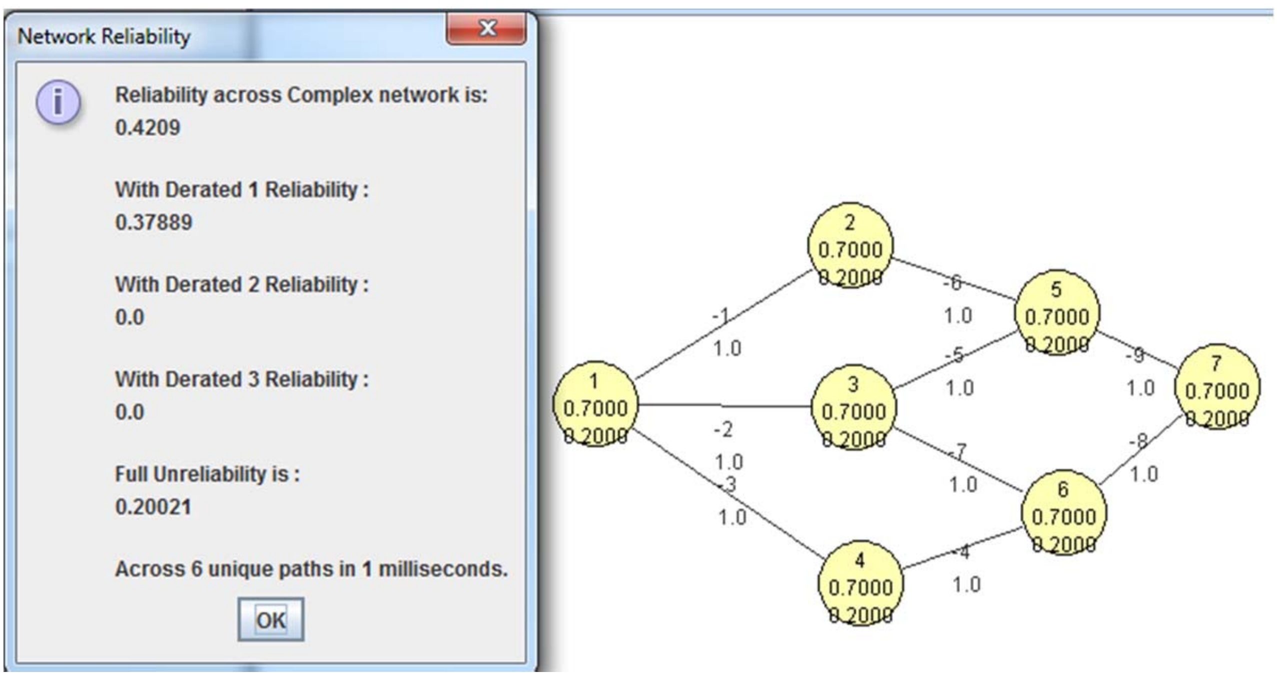

Decoding
ERBDC
MESAT
SecurityMeter
Flat
PG
NB
Privacy
One Sample t-test
Two Sample t-test
Cloud
Pedagogica
Choose a software program to run.
Execute
Exit

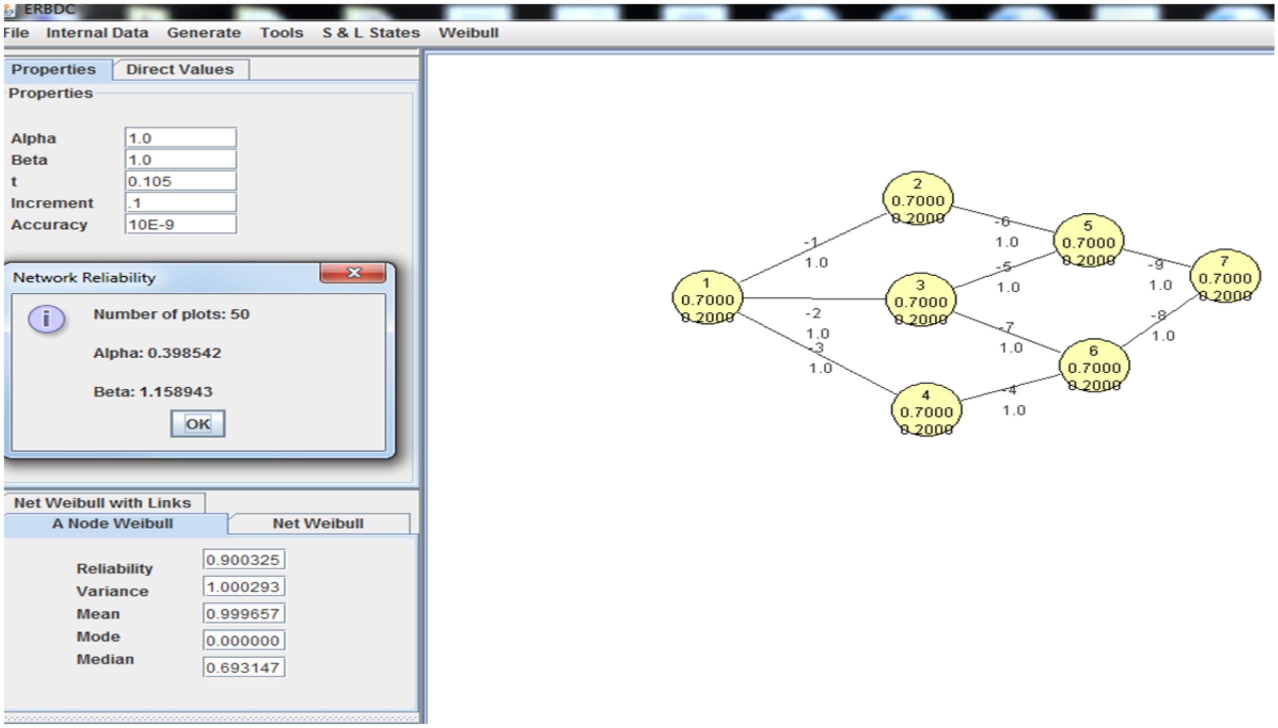

Decoding ERBDC MESAT SecurityMeter Flat PG NB Privacy One Sample t-test Two Sample t-test Cloud Pedagogica
Code Name: Decoding
Code Title: Reverse engineering or decoding of the network diagram from the encoding.
Ref. Book Chapter: Chap. 6 (Reliability Block Diagramming in Complex Systems), Section 6 (New Polish Decoding Algorithm)
Brief Definition: The objective is to generate a reverse-coded reliability block diagram from the given Polish notation and recreate the original topology generated by the RBD compression algorithm. The platform used is Java. This diagram helps view complex network paths from an ingress to an egress node, and it ultimately calculates the
Execute
Exit

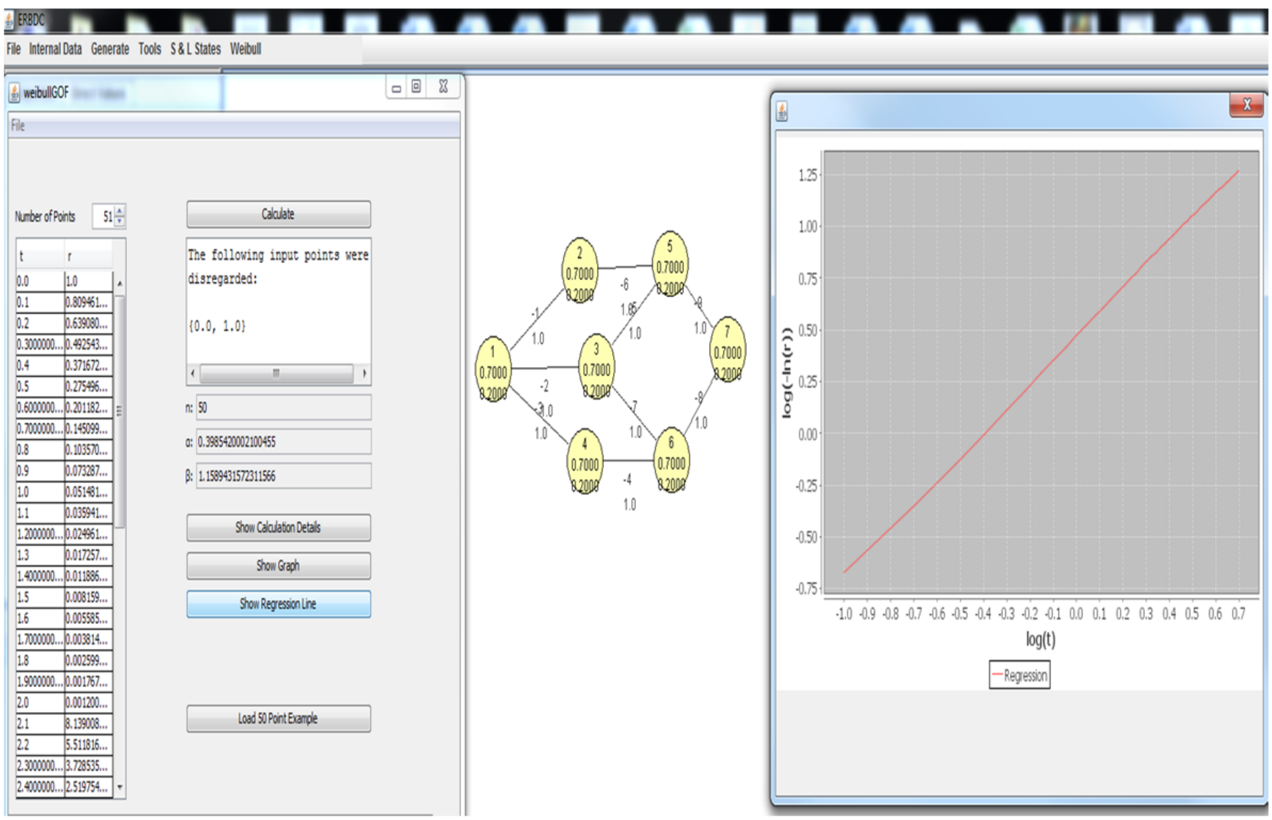

Decoding
Polish Notation:
1, -1, 2, *, -2, *, -3, 3, *, -4, *, +, *, 4, *
Process
Reset
2
0.9
-1
1.0
-2
1.0
1
0.9
4
0.9
-3
1.0
-4
1.0
3
0.9

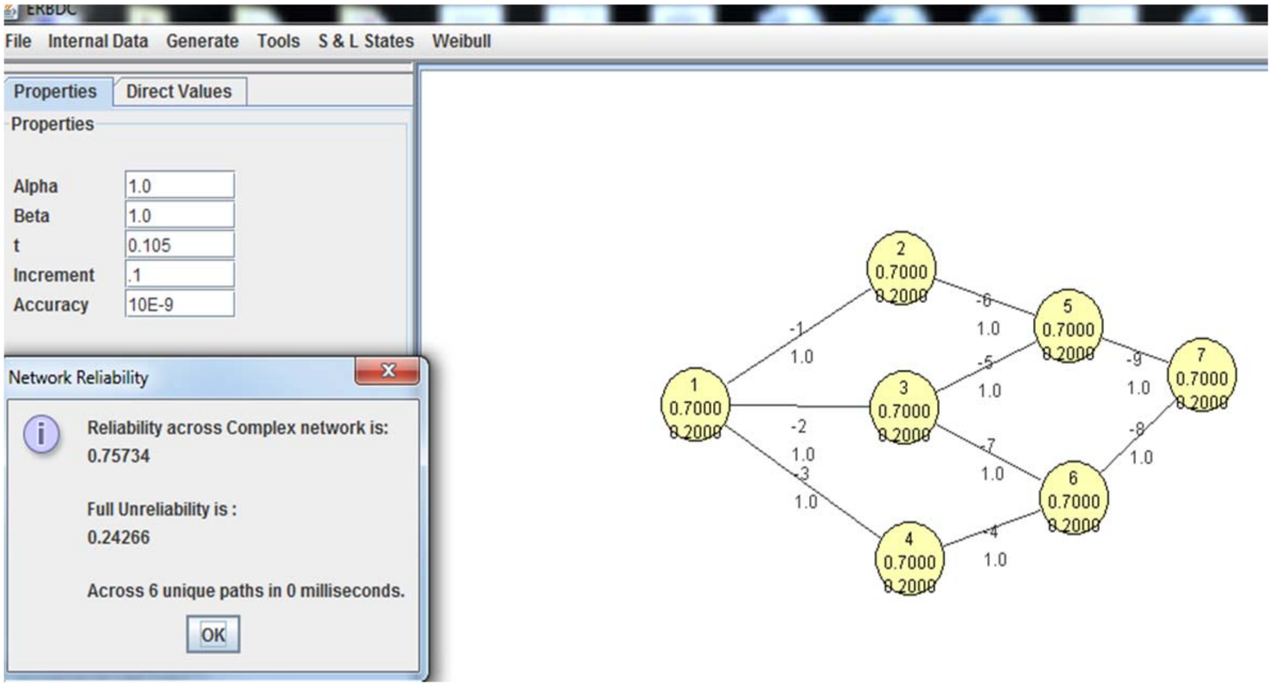

Decoding
ERBDC
MESAT
SecurityMeter
Flat
PG
NB
Privacy
One Sample t-test
Two Sample t-test
Cloud
Pedagogical
Code Name: ERBDC
Code Title: Exact Reliability Block Diagramming Calculation
Ref. Book Chapter: Chap. 5 (Availability Modeling using the Sahinoglu Libby Probability Distribution; Chap.6 (Reliability Block Diagramming in Simple and Complex Embedded Systems.
Brief Definition: The objective is to generate RBDs to calculate ingress-egress, or s-t (source-target) reliability for simple and complex systems under directly coded and/or statistical failure-repair data using SL probability model in Chap. 5. It also performs a complete performance availability analysis on a single node as explained in Section 5.6.
Execute
Exit
ERBDC
File
Internal Data
Generate
Tools
S & L States
Weibull
Properties
Direct Values
Properties
Up-Dn #a 10
C 0.02
Dn-Up #b 10
Ksi 1.0
Cum. a (Xt) 1000
D 0.1
Cum. b (Yt) 111.11
Eta 1.0
Node Availability
Network Availability
Select
Availability(r)
Unavailability(q)
E 0.890985 0.109015
* 0.907325 0.092675
** 0.906655 0.093345
LS 0.900001 0.099999
M 0.898600 0.101400
D 0.900000 0.100000
T 1.000000 0.000000
1 0.9000
2 0.9000
3 0.9000
4 0.9000
5 0.9000
6 0.9000
7 0.9000
-1 1.0
-2 1.0
-3 1.0
-4 1.0
-5 1.0
-6 1.0
-7 1.0
-8 1.0
-9 1.0
Network Reliability
Reliability across Complex network is:
0.79979
Full Unreliability is :
0.20021
Across 6 unique paths in 5 milliseconds.
OK

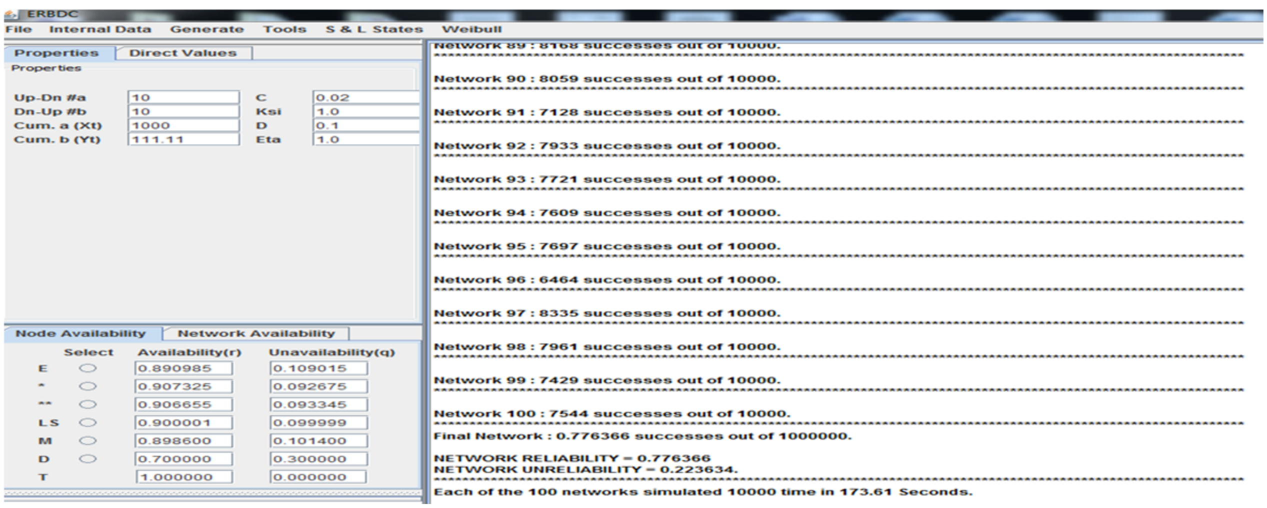

Generate
Tools
S & L States
Weibull
Reliability Matrix by Compression
Reliability Matrix by Compression - with Derated
Single Path Reliability
Enumeration Reliability
Enumeration Reliability - with Derated
Overlap Reliability
Overlap Reliability - with Derated
Weibull Overlap Reliability
Source-Target Weibull LSE
Montecarlo Simulation
S & L Simulation


Network Reliability
Reliability across Complex network is:
0.4209
With Derated 1 Reliability :
0.37889
With Derated 2 Reliability :
0.0
With Derated 3 Reliability :
0.0
Full Unreliability is :
0.20021
Across 6 unique paths in 1 milliseconds.
OK


ERBDC
File
Internal Data
Generate
Tools
S & L States
Weibull
Properties
Direct Values
Properties
Alpha 1.0
Beta 1.0
t 0.105
Increment .1
Accuracy 10E-9
Network Reliability
Number of plots: 50
Alpha: 0.398542
Beta: 1.158943
OK
Net Weibull with Links
A Node Weibull
Net Weibull
Reliability 0.900325
Variance 1.000293
Mean 0.999657
Mode 0.000000
Median 0.693147


ERBDC
File
Internal Data
Generate
Tools
S & L States
Weibull
weibullGOF
Number of Points 51
Calculate
The following input points were disregarded:
{0.0, 1.0}
n: 50
α: 0.3985420002100455
β: 1.1589431572311566
Show Calculation Details
Show Graph
Show Regression Line
Load 50 Point Example
log(-ln(r))
log(t)
Regression

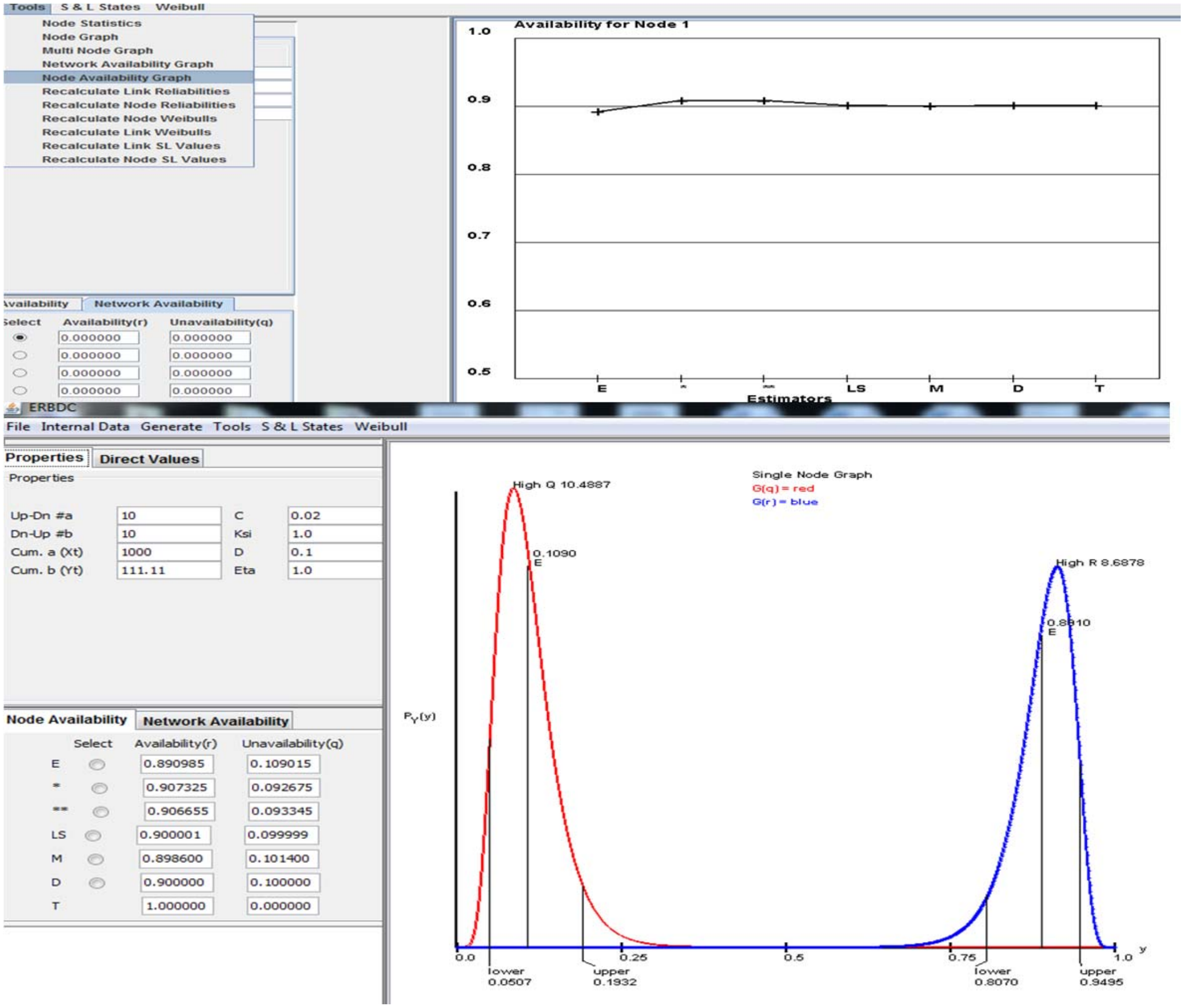




Monte Carlo Simulation Description

Ingress Node : 1 Egress Node : 7 Final Result: 7989 successes out of 10000.

NETWORK RELIABILITY = 0.7989 NETWORK UNRELIABILITY = 0.2011. Total Runs : 10000 in 0.012 Seconds.



Overview wires.wiley.com/compstats

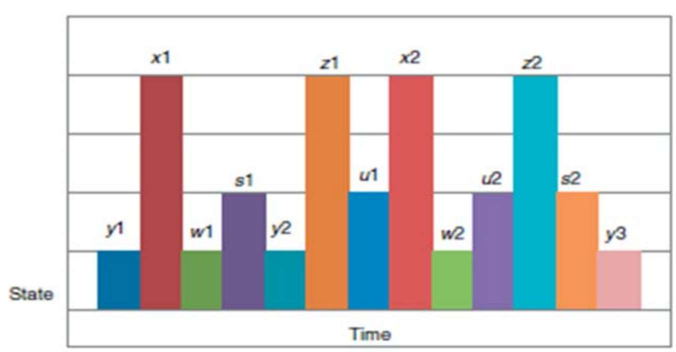
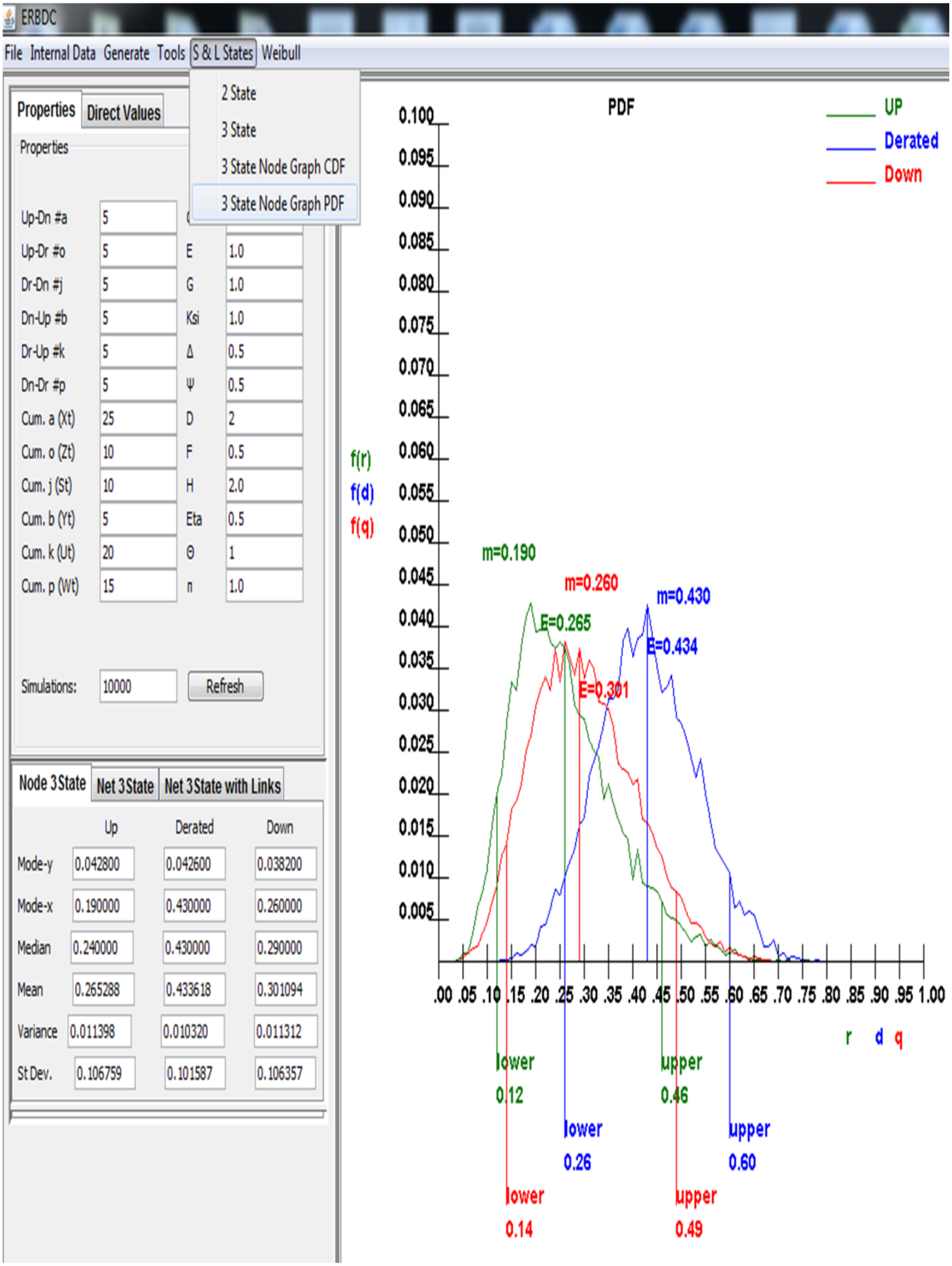
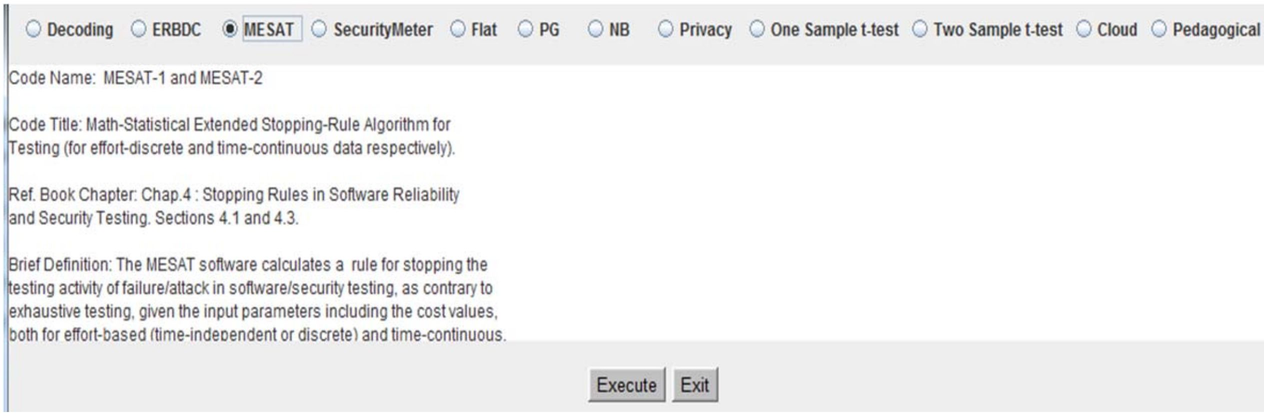
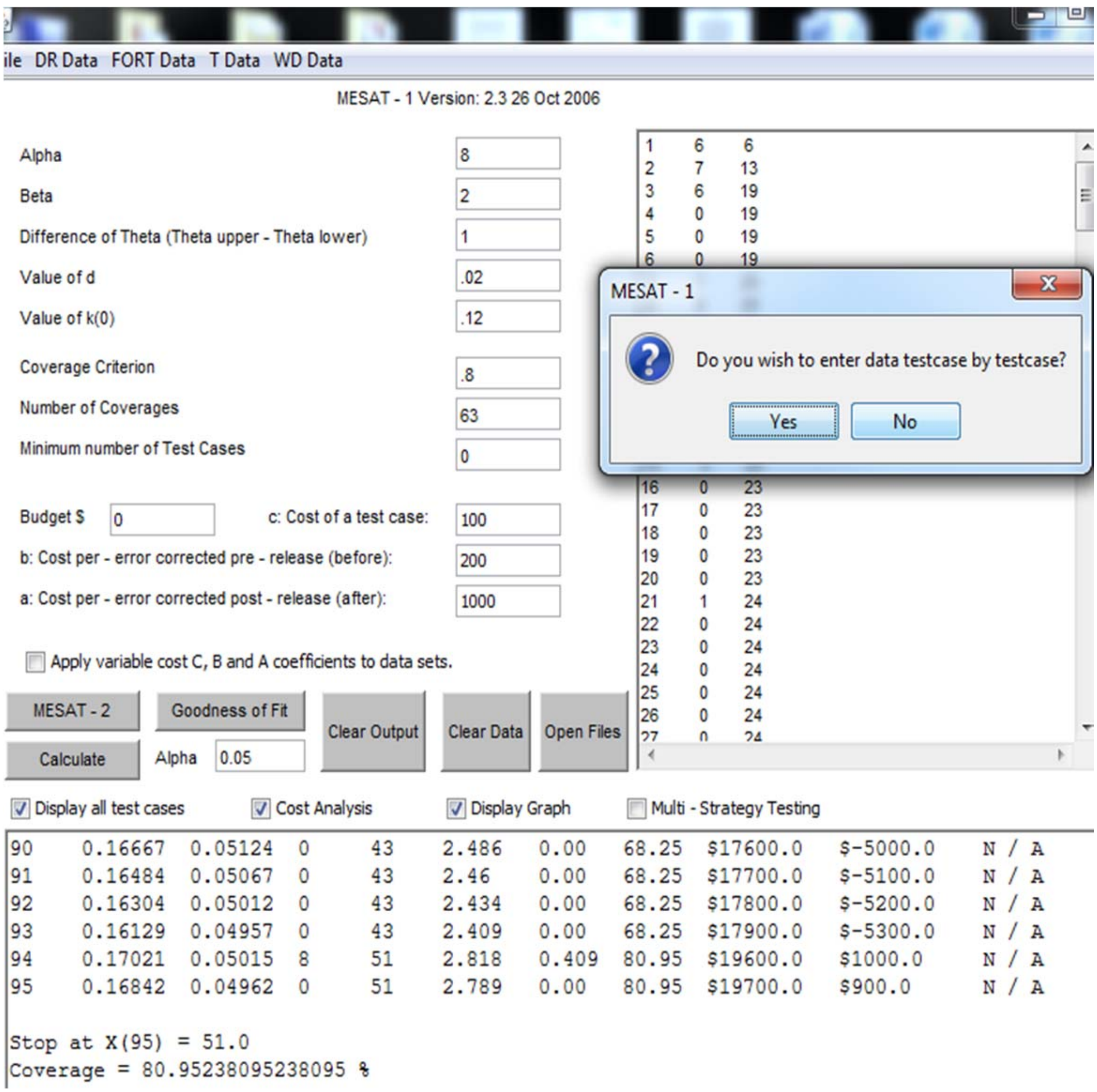
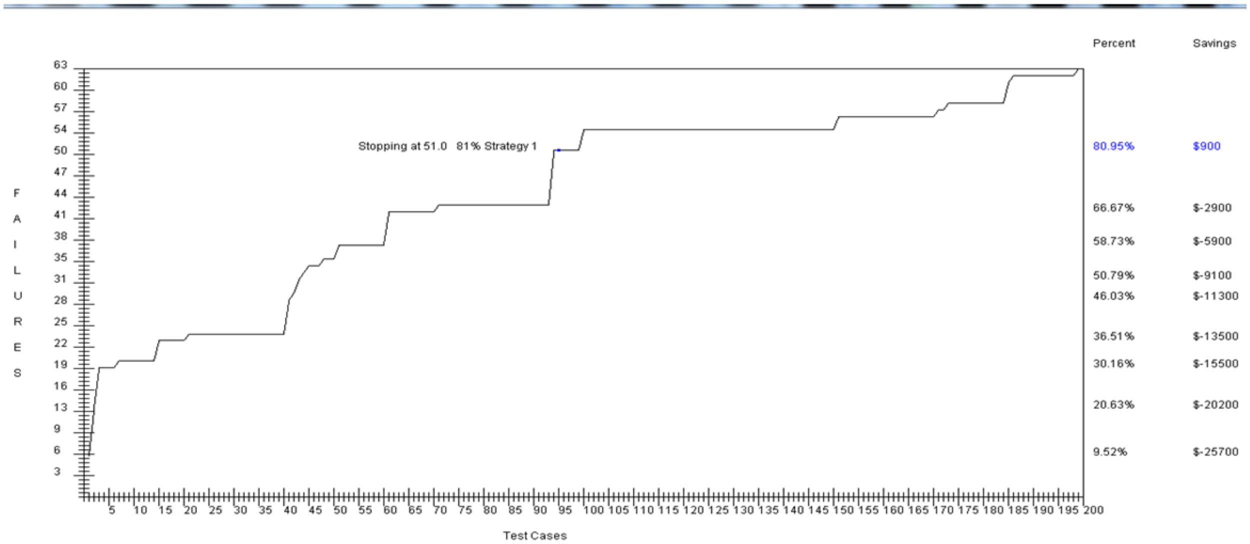


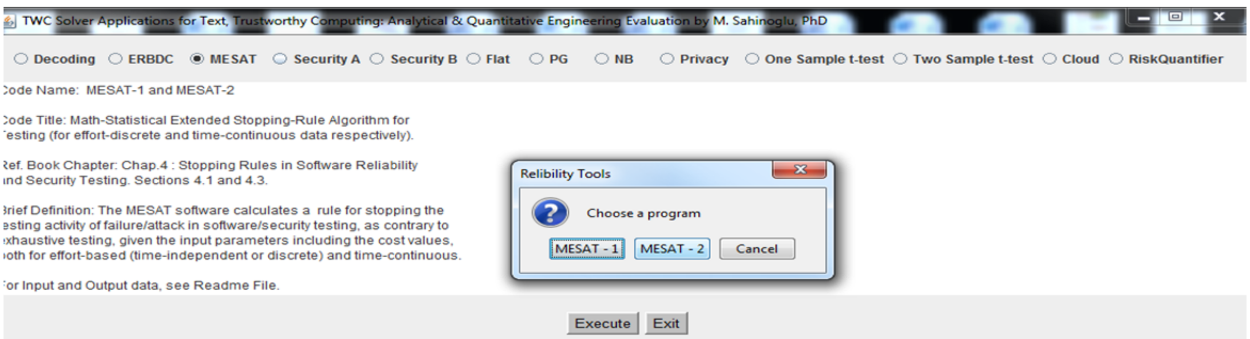
FIGURE 4 | A sample illustration of feasible transitions from Figure 3 implemented to subsections of *Three-State Sahinoglu Probability Model of Production Units* (Monte Carlo Simulation).

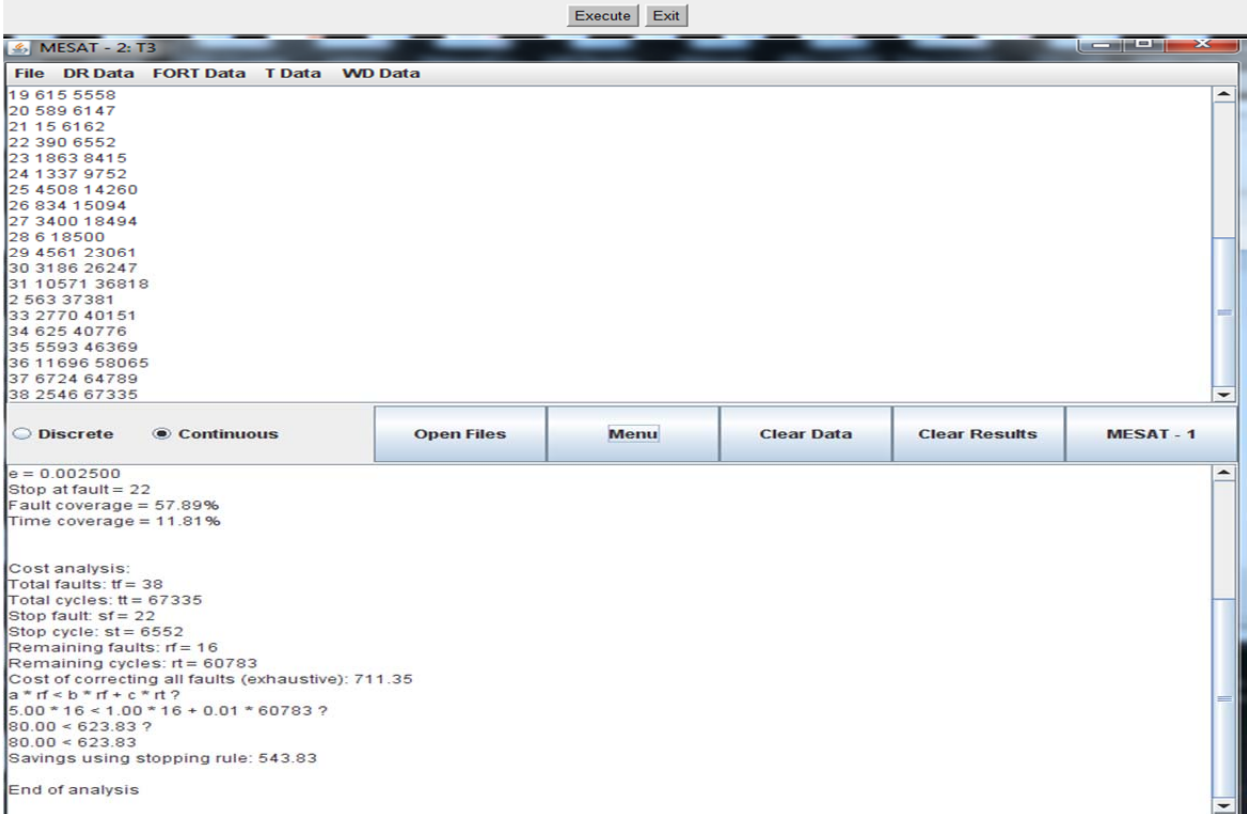

ERBDC
File Internal Data Generate Tools S & L States Weibull
2 State
3 State
3 State Node Graph CDF
3 State Node Graph PDF
Properties Direct Values
Properties
Up-Dn #a 5
Up-Dr #o 5 E 1.0
Dr-Dn #j 5 G 1.0
Dn-Up #b 5 Ksi 1.0
Dr-Up #k 5 Δ 0.5
Dn-Dr #p 5 Ψ 0.5
Cum. a (Xt) 25 D 2
Cum. o (Zt) 10 F 0.5
Cum. j (St) 10 H 2.0
Cum. b (Yt) 5 Eta 0.5
Cum. k (Ut) 20 Θ 1
Cum. p (Wt) 15 n 1.0
Simulations: 10000 Refresh
Node 3State Net 3State Net 3State with Links
Up Derated Down
Mode-y 0.042800 0.042600 0.038200
Mode-x 0.190000 0.430000 0.260000
Median 0.240000 0.430000 0.290000
Mean 0.265288 0.433618 0.301094
Variance 0.011398 0.010320 0.011312
St Dev. 0.106759 0.101587 0.106357
PDF
UP
Derated
Down
f(r)
f(d)
f(q)
m=0.190
m=0.260
m=0.430
E=0.265
E=0.434
E=0.301
r d q
lower 0.12
upper 0.46
lower 0.26
upper 0.60
lower 0.14
upper 0.49

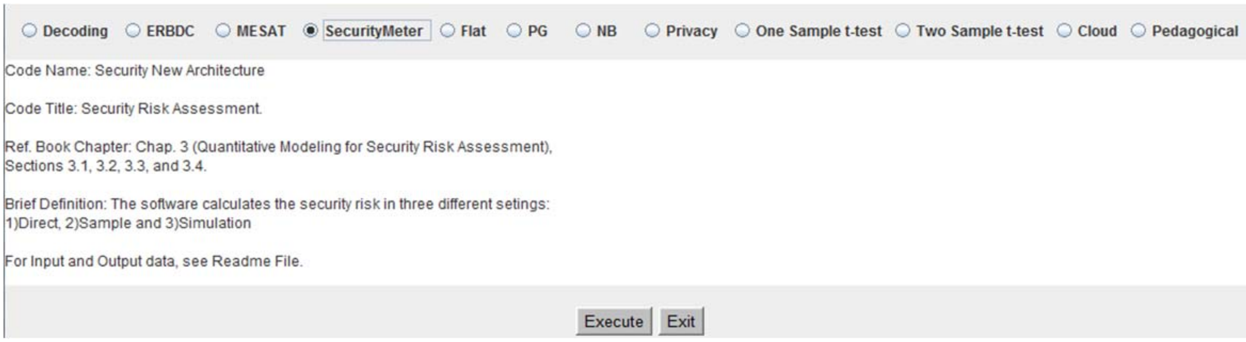

Decoding ERBDC MESAT SecurityMeter Flat PG NB Privacy One Sample t-test Two Sample t-test Cloud Pedagogical
Code Name: MESAT-1 and MESAT-2
Code Title: Math-Statistical Extended Stopping-Rule Algorithm for Testing (for effort-discrete and time-continuous data respectively).
Ref. Book Chapter: Chap.4 : Stopping Rules in Software Reliability and Security Testing. Sections 4.1 and 4.3.
Brief Definition: The MESAT software calculates a rule for stopping the testing activity of failure/attack in software/security testing, as contrary to exhaustive testing, given the input parameters including the cost values, both for effort-based (time-independent or discrete) and time-continuous.
Execute
Exit

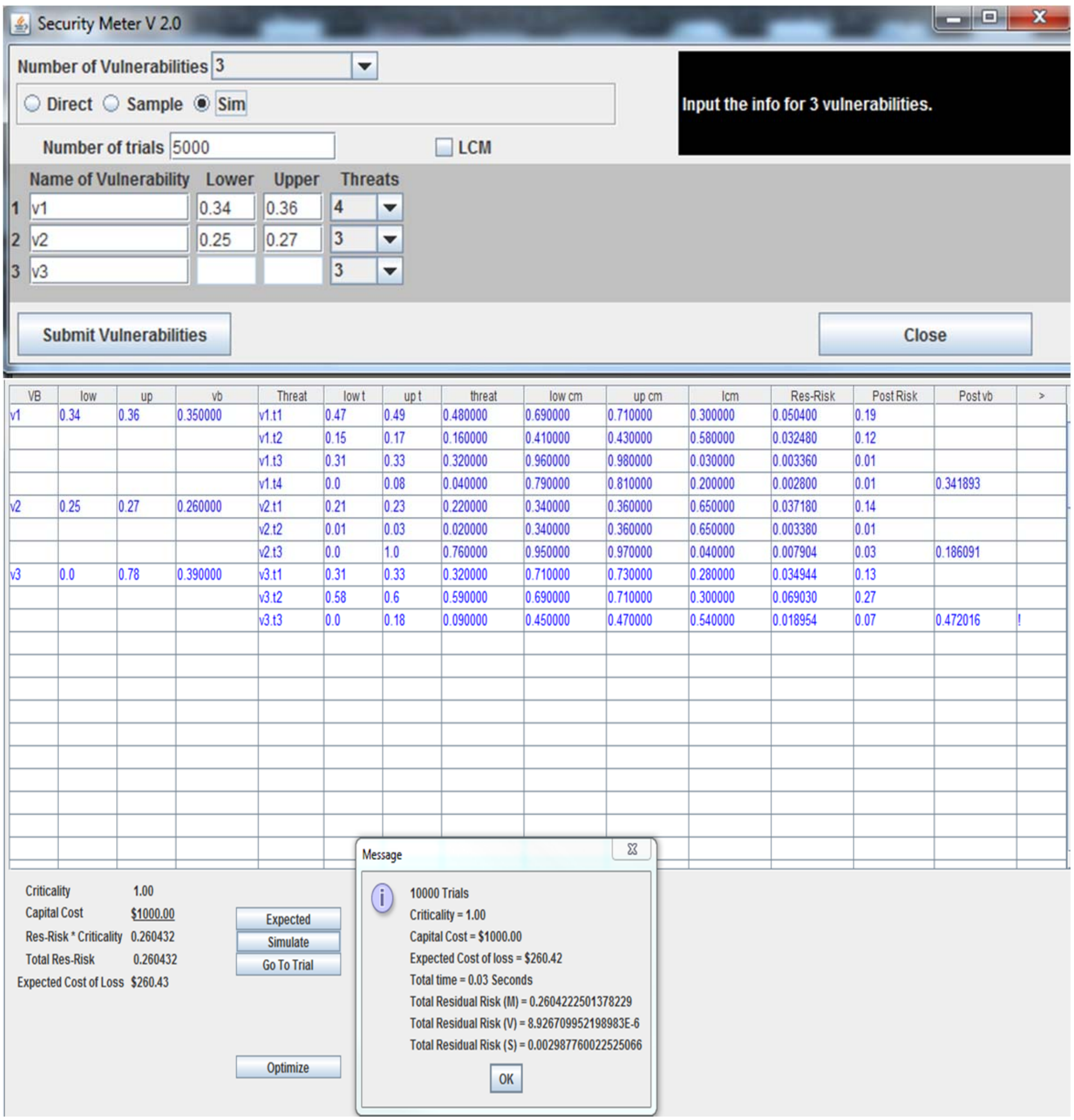

ile DR Data FORT Data T Data WD Data
MESAT - 1 Version: 2.3 26 Oct 2006
Alpha 8
Beta 2
Difference of Theta (Theta upper - Theta lower) 1
Value of d .02
Value of k(0) .12
Coverage Criterion .8
Number of Coverages 63
Minimum number of Test Cases 0
Budget $ 0
c: Cost of a test case: 100
b: Cost per - error corrected pre - release (before): 200
a: Cost per - error corrected post - release (after): 1000
Apply variable cost C, B and A coefficients to data sets.
MESAT - 2
Goodness of Fit
Clear Output
Clear Data
Open Files
Calculate
Alpha 0.05
MESAT - 1
Do you wish to enter data testcase by testcase?
Yes
No
Display all test cases
Cost Analysis
Display Graph
Multi - Strategy Testing
90 0.16667 0.05124 0 43 2.486 0.00 68.25 $17600.0 $-5000.0 N / A
91 0.16484 0.05067 0 43 2.46 0.00 68.25 $17700.0 $-5100.0 N / A
92 0.16304 0.05012 0 43 2.434 0.00 68.25 $17800.0 $-5200.0 N / A
93 0.16129 0.04957 0 43 2.409 0.00 68.25 $17900.0 $-5300.0 N / A
94 0.17021 0.05015 8 51 2.818 0.409 80.95 $19600.0 $1000.0 N / A
95 0.16842 0.04962 0 51 2.789 0.00 80.95 $19700.0 $900.0 N / A
Stop at X(95) = 51.0
Coverage = 80.95238095238095 %


Percent
Savings
Stopping at 51.0 81% Strategy 1
80.95% $900
66.67% $-2900
58.73% $-5900
50.79% $-9100
46.03% $-11300
36.51% $-13500
30.16% $-15500
20.63% $-20200
9.52% $-25700
FAILURES
Test Cases

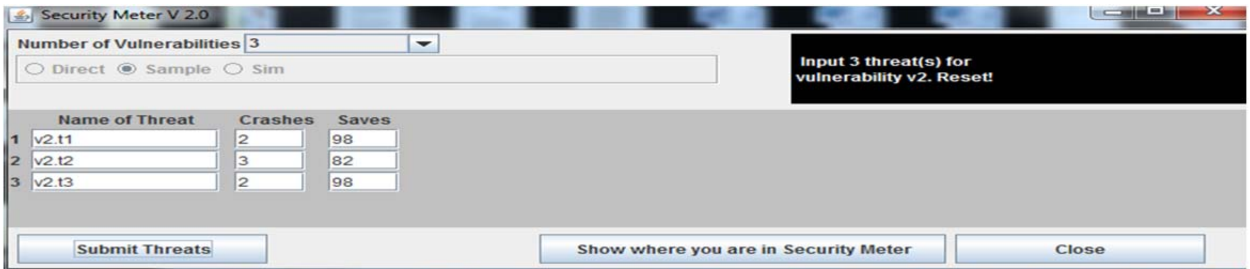

TWC Solver Applications for Text, Trustworthy Computing: Analytical & Quantitative Engineering Evaluation by M. Sahinoglu, PhD
Decoding ERBDC MESAT Security A Security B Flat PG NB Privacy One Sample t-test Two Sample t-test Cloud RiskQuantifier
Code Name: MESAT-1 and MESAT-2
Code Title: Math-Statistical Extended Stopping-Rule Algorithm for Testing (for effort-discrete and time-continuous data respectively).
Ref. Book Chapter: Chap.4 : Stopping Rules in Software Reliability and Security Testing. Sections 4.1 and 4.3.
Brief Definition: The MESAT software calculates a rule for stopping the testing activity of failure/attack in software/security testing, as contrary to exhaustive testing, given the input parameters including the cost values, both for effort-based (time-independent or discrete) and time-continuous.
For Input and Output data, see Readme File.
Relibility Tools
Choose a program
MESAT - 1 MESAT - 2 Cancel
Execute Exit

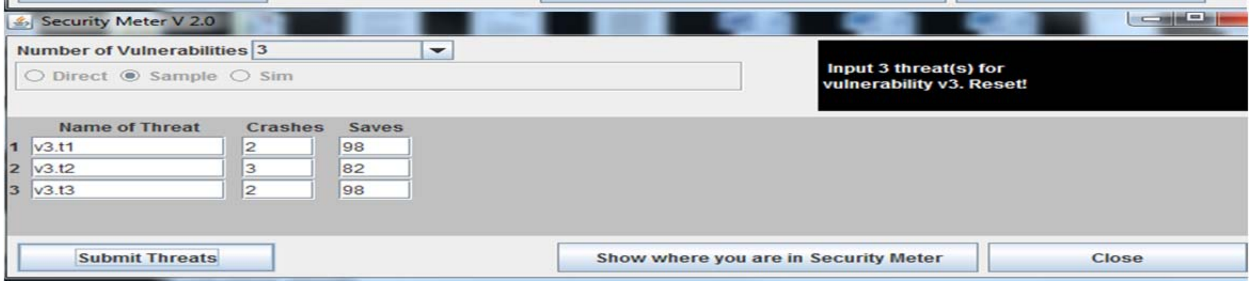

MESAT - 2: T3
File DR Data FORT Data T Data WD Data
19 615 5558
20 589 6147
21 15 6162
22 390 6552
23 1863 8415
24 1337 9752
25 4508 14260
26 834 15094
27 3400 18494
28 6 18500
29 4561 23061
30 3186 26247
31 10571 36818
2 563 37381
33 2770 40151
34 625 40776
35 5593 46369
36 11696 58065
37 6724 64789
38 2546 67335
Discrete Continuous Open Files Menu Clear Data Clear Results MESAT - 1
e = 0.002500
Stop at fault = 22
Fault coverage = 57.89%
Time coverage = 11.81%
Cost analysis:
Total faults: tf = 38
Total cycles: tt = 67335
Stop fault: sf = 22
Stop cycle: st = 6552
Remaining faults: rf = 16
Remaining cycles: rt = 60783
Cost of correcting all faults (exhaustive): 711.35
a * rf < b * rf + c * rt ?
5.00 * 16 < 1.00 * 16 + 0.01 * 60783 ?
80.00 < 623.83 ?
80.00 < 623.83
Savings using stopping rule: 543.83
End of analysis

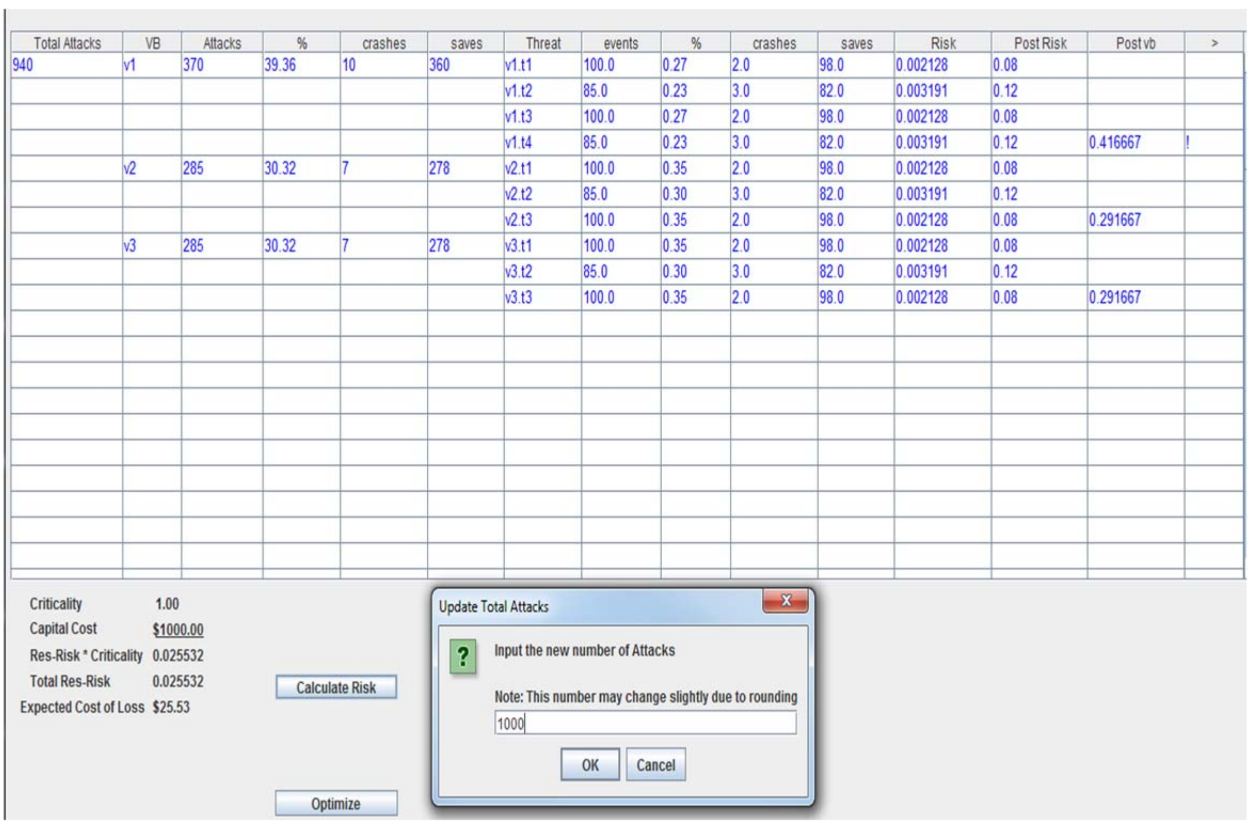




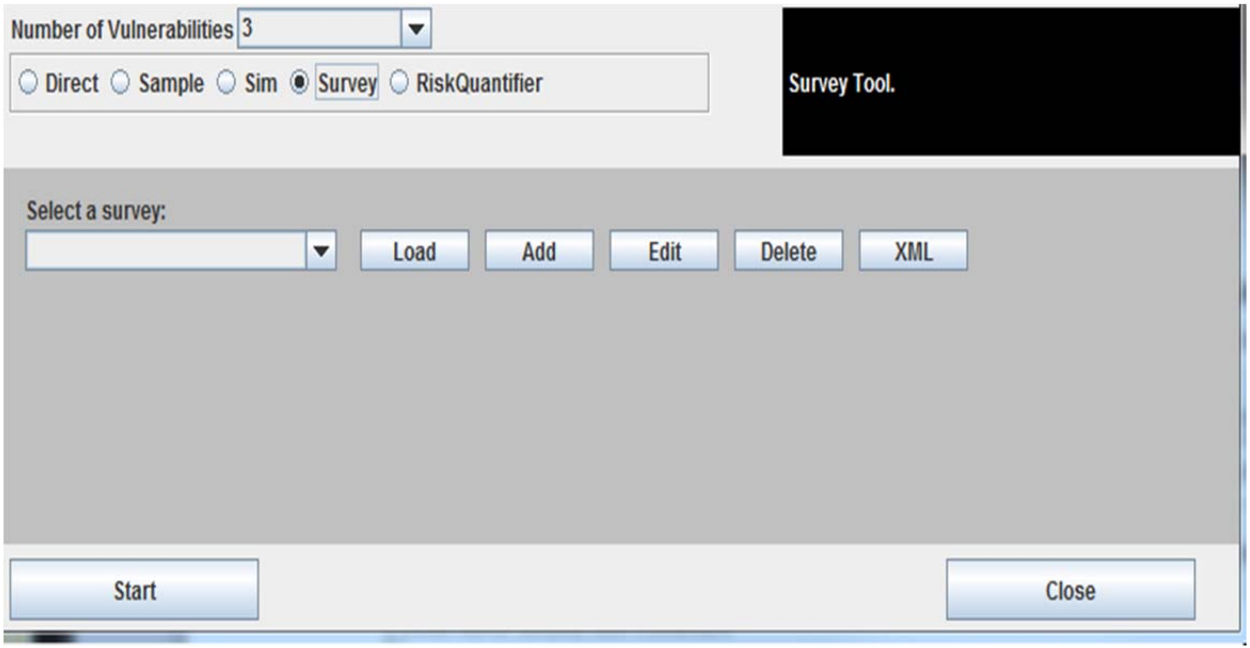
VB	low	up	vb	Threat	low t	up t	threat	low cm	up cm	lcm	Res-Risk	Post Risk	Post vb	>
v1	0.34	0.36	0.350000	v1.t1	0.47	0.49	0.480000	0.690000	0.710000	0.300000	0.050400	0.19		
				v1.t2	0.15	0.17	0.160000	0.410000	0.430000	0.580000	0.032480	0.12		
				v1.t3	0.31	0.33	0.320000	0.960000	0.980000	0.030000	0.003360	0.01		
				v1.t4	0.0	0.08	0.040000	0.790000	0.810000	0.200000	0.002800	0.01	0.341893	
v2	0.25	0.27	0.260000	v2.t1	0.21	0.23	0.220000	0.340000	0.360000	0.650000	0.037180	0.14		
				v2.t2	0.01	0.03	0.020000	0.340000	0.360000	0.650000	0.003380	0.01		
				v2.t3	0.0	1.0	0.760000	0.950000	0.970000	0.040000	0.007904	0.03	0.186091	
v3	0.0	0.78	0.390000	v3.t1	0.31	0.33	0.320000	0.710000	0.730000	0.280000	0.034944	0.13		
				v3.t2	0.58	0.6	0.590000	0.690000	0.710000	0.300000	0.069030	0.27		
				v3.t3	0.0	0.18	0.090000	0.450000	0.470000	0.540000	0.018954	0.07	0.472016	!

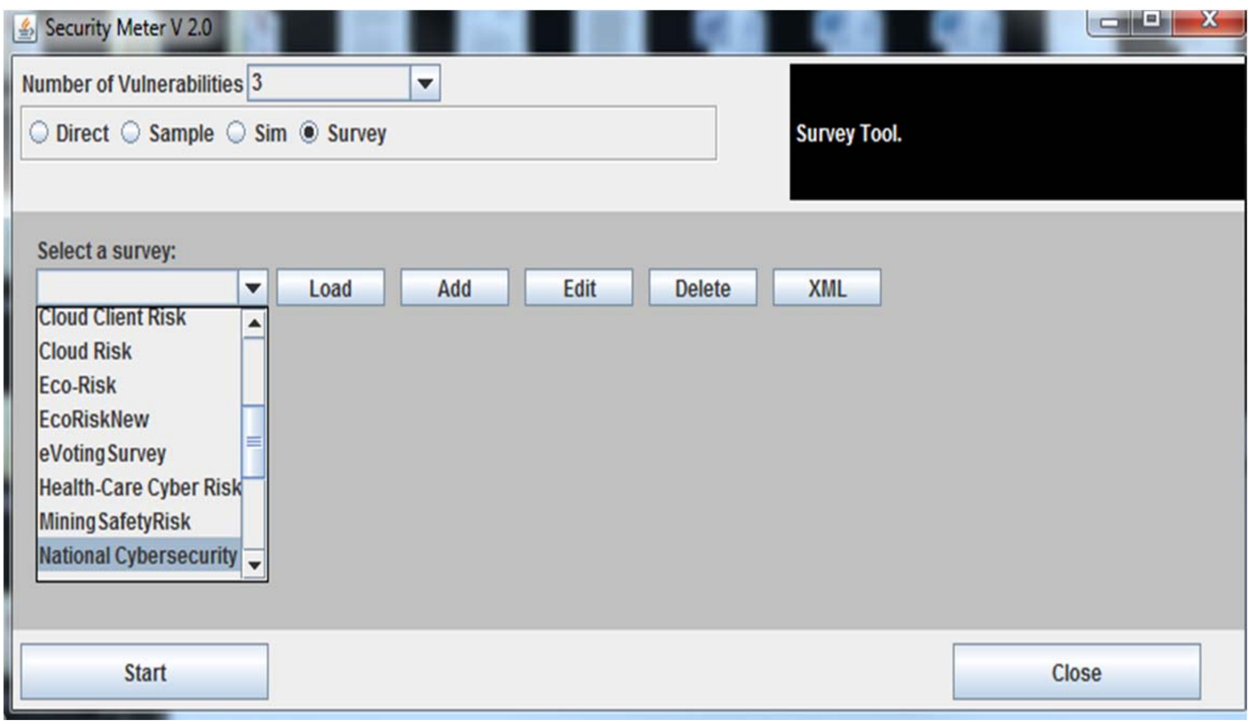


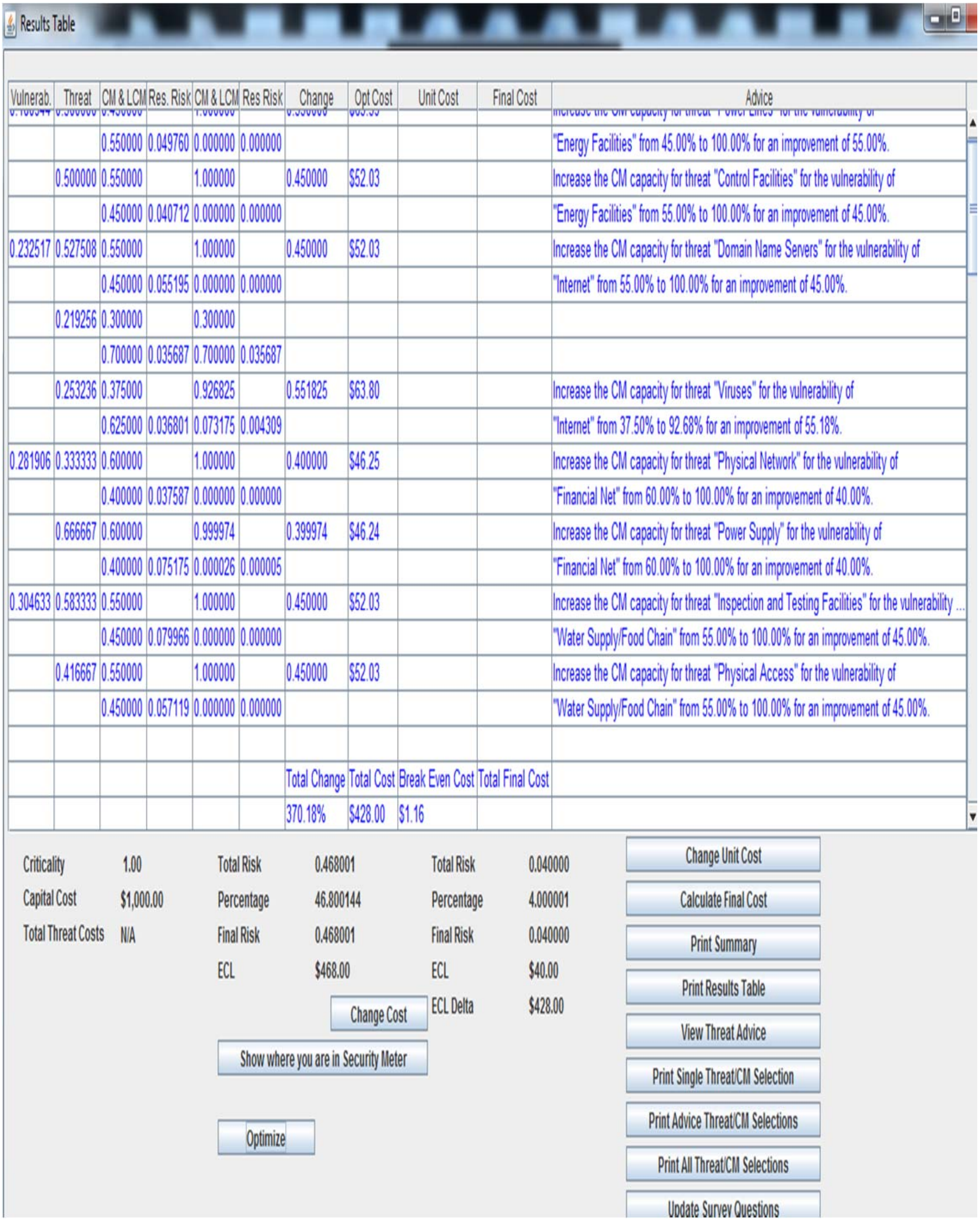


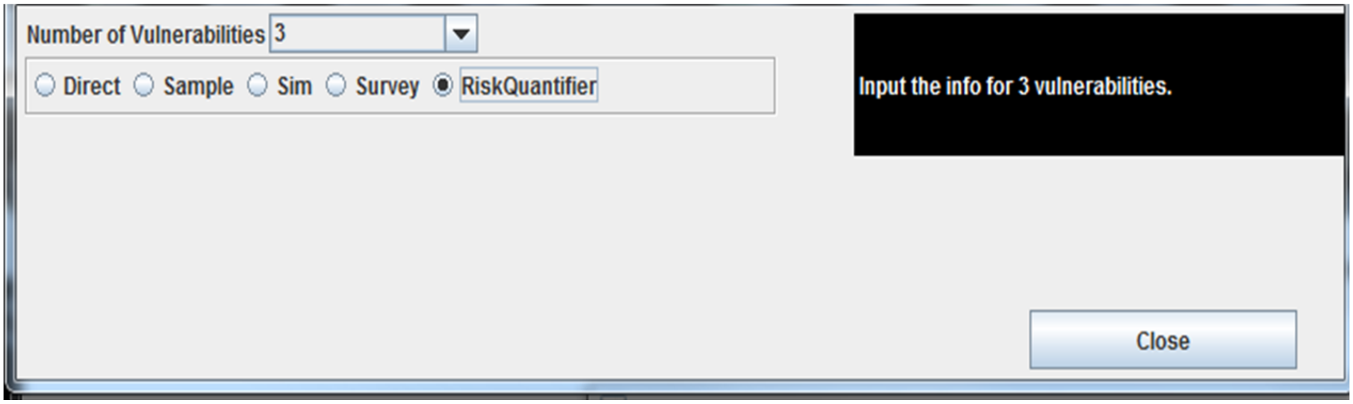


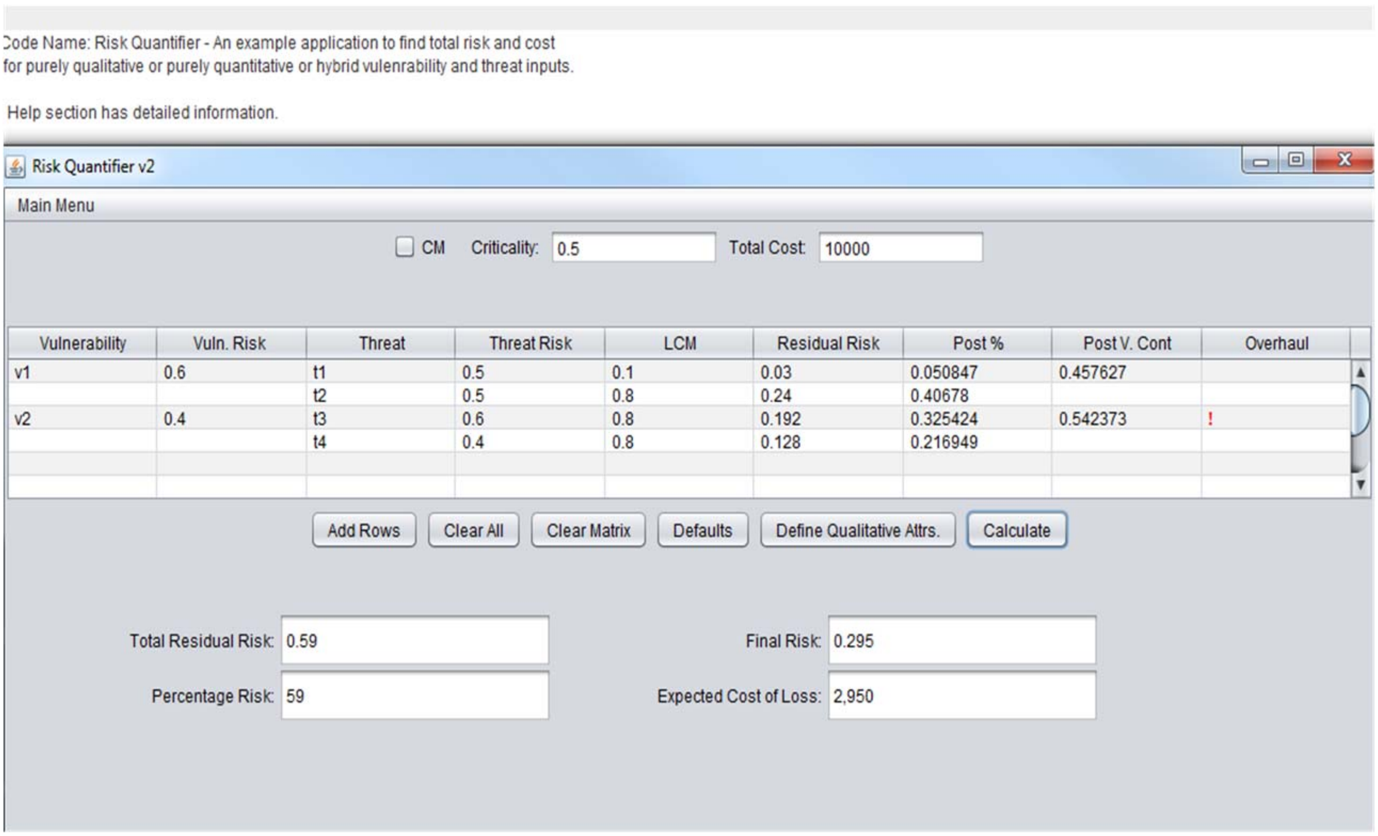
Total Attacks	VB	Attacks	%	crashes	saves	Threat	events	%	crashes	saves	Risk	Post Risk	Post vb	>
940	v1	370	39.36	10	360	v1.t1	100.0	0.27	2.0	98.0	0.002128	0.08		
						v1.t2	85.0	0.23	3.0	82.0	0.003191	0.12		
						v1.t3	100.0	0.27	2.0	98.0	0.002128	0.08		
						v1.t4	85.0	0.23	3.0	82.0	0.003191	0.12	0.416667	!
	v2	285	30.32	7	278	v2.t1	100.0	0.35	2.0	98.0	0.002128	0.08		
						v2.t2	85.0	0.30	3.0	82.0	0.003191	0.12		
						v2.t3	100.0	0.35	2.0	98.0	0.002128	0.08	0.291667	
	v3	285	30.32	7	278	v3.t1	100.0	0.35	2.0	98.0	0.002128	0.08		
						v3.t2	85.0	0.30	3.0	82.0	0.003191	0.12		
						v3.t3	100.0	0.35	2.0	98.0	0.002128	0.08	0.291667	


Number of Vulnerabilities 3
Direct Sample Sim Survey RiskQuantifier
Survey Tool.
Select a survey:
Load Add Edit Delete XML
Start
Close

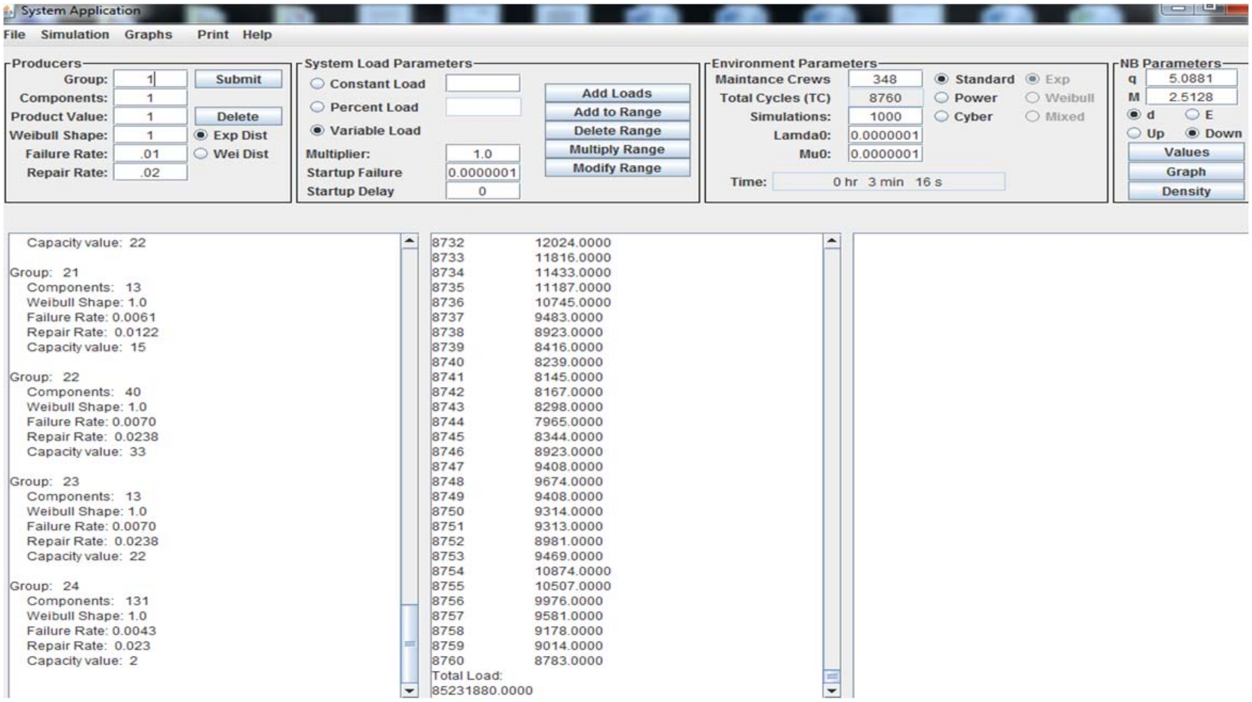

Security Meter V 2.0
Number of Vulnerabilities 3
Direct Sample Sim Survey
Survey Tool.
Select a survey:
Load Add Edit Delete XML
Cloud Client Risk
Cloud Risk
Eco-Risk
EcoRiskNew
eVoting Survey
Health-Care Cyber Risk
Mining SafetyRisk
National Cybersecurity
Start
Close

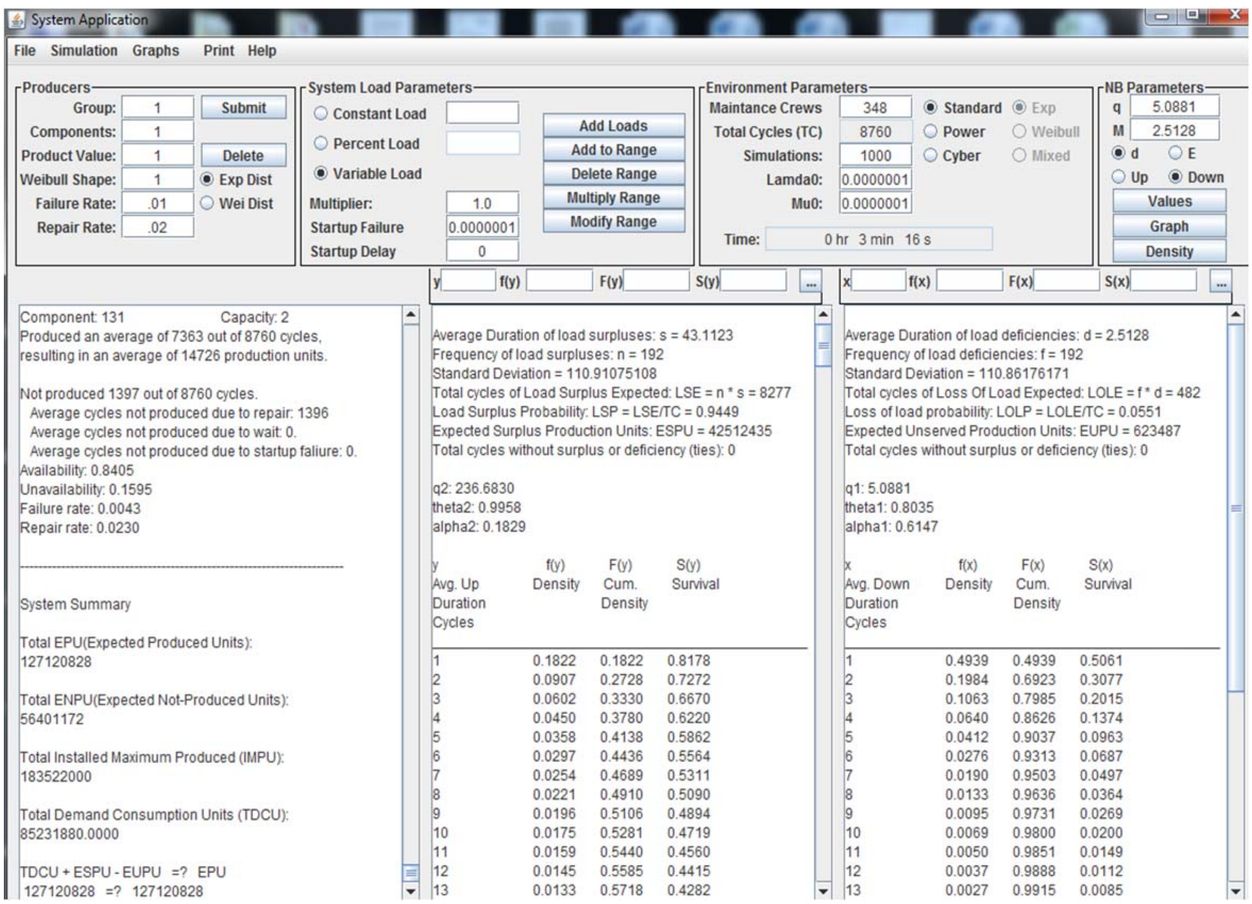

Results Table
Vulnerab. | Threat | CM & LCM | Res. Risk | CM & LCM | Res Risk | Change | Opt Cost | Unit Cost | Final Cost | Advice
0.550000 0.049760 0.000000 0.000000 "Energy Facilities" from 45.00% to 100.00% for an improvement of 55.00%.
0.500000 0.550000 1.000000 0.450000 $52.03 Increase the CM capacity for threat "Control Facilities" for the vulnerability of
0.450000 0.040712 0.000000 0.000000 "Energy Facilities" from 55.00% to 100.00% for an improvement of 45.00%.
0.232517 0.527508 0.550000 1.000000 0.450000 $52.03 Increase the CM capacity for threat "Domain Name Servers" for the vulnerability of
0.450000 0.055195 0.000000 0.000000 "Internet" from 55.00% to 100.00% for an improvement of 45.00%.
0.219256 0.300000 0.300000
0.700000 0.035687 0.700000 0.035687
0.253236 0.375000 0.926825 0.551825 $63.80 Increase the CM capacity for threat "Viruses" for the vulnerability of
0.625000 0.036801 0.073175 0.004309 "Internet" from 37.50% to 92.68% for an improvement of 55.18%.
0.281906 0.333333 0.600000 1.000000 0.400000 $46.25 Increase the CM capacity for threat "Physical Network" for the vulnerability of
0.400000 0.037587 0.000000 0.000000 "Financial Net" from 60.00% to 100.00% for an improvement of 40.00%.
0.666667 0.600000 0.999974 0.399974 $46.24 Increase the CM capacity for threat "Power Supply" for the vulnerability of
0.400000 0.075175 0.000026 0.000005 "Financial Net" from 60.00% to 100.00% for an improvement of 40.00%.
0.304633 0.583333 0.550000 1.000000 0.450000 $52.03 Increase the CM capacity for threat "Inspection and Testing Facilities" for the vulnerability ...
0.450000 0.079966 0.000000 0.000000 "Water Supply/Food Chain" from 55.00% to 100.00% for an improvement of 45.00%.
0.416667 0.550000 1.000000 0.450000 $52.03 Increase the CM capacity for threat "Physical Access" for the vulnerability of
0.450000 0.057119 0.000000 0.000000 "Water Supply/Food Chain" from 55.00% to 100.00% for an improvement of 45.00%.
Total Change | Total Cost | Break Even Cost | Total Final Cost
370.18% | $428.00 | $1.16
Criticality 1.00
Capital Cost $1,000.00
Total Threat Costs N/A
Total Risk 0.468001
Percentage 46.800144
Final Risk 0.468001
ECL $468.00
Total Risk 0.040000
Percentage 4.000001
Final Risk 0.040000
ECL $40.00
ECL Delta $428.00
Change Cost
Show where you are in Security Meter
Optimize
Change Unit Cost
Calculate Final Cost
Print Summary
Print Results Table
View Threat Advice
Print Single Threat/CM Selection
Print Advice Threat/CM Selections
Print All Threat/CM Selections
Update Survey Questions

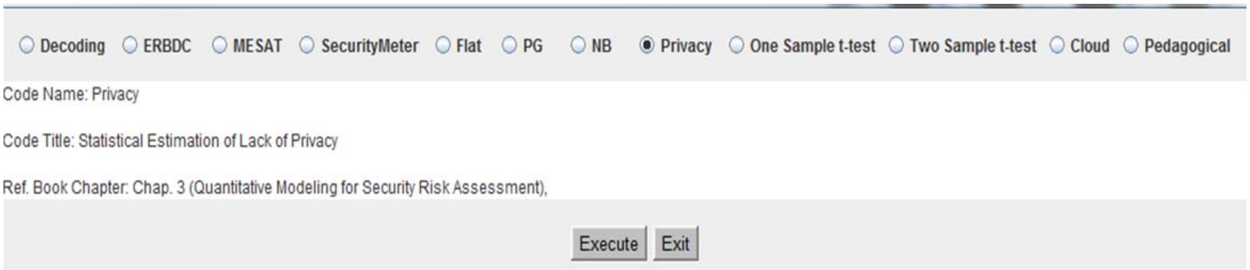

Number of Vulnerabilities 3
Direct
Sample
Sim
Survey
RiskQuantifier
Input the info for 3 vulnerabilities.
Close

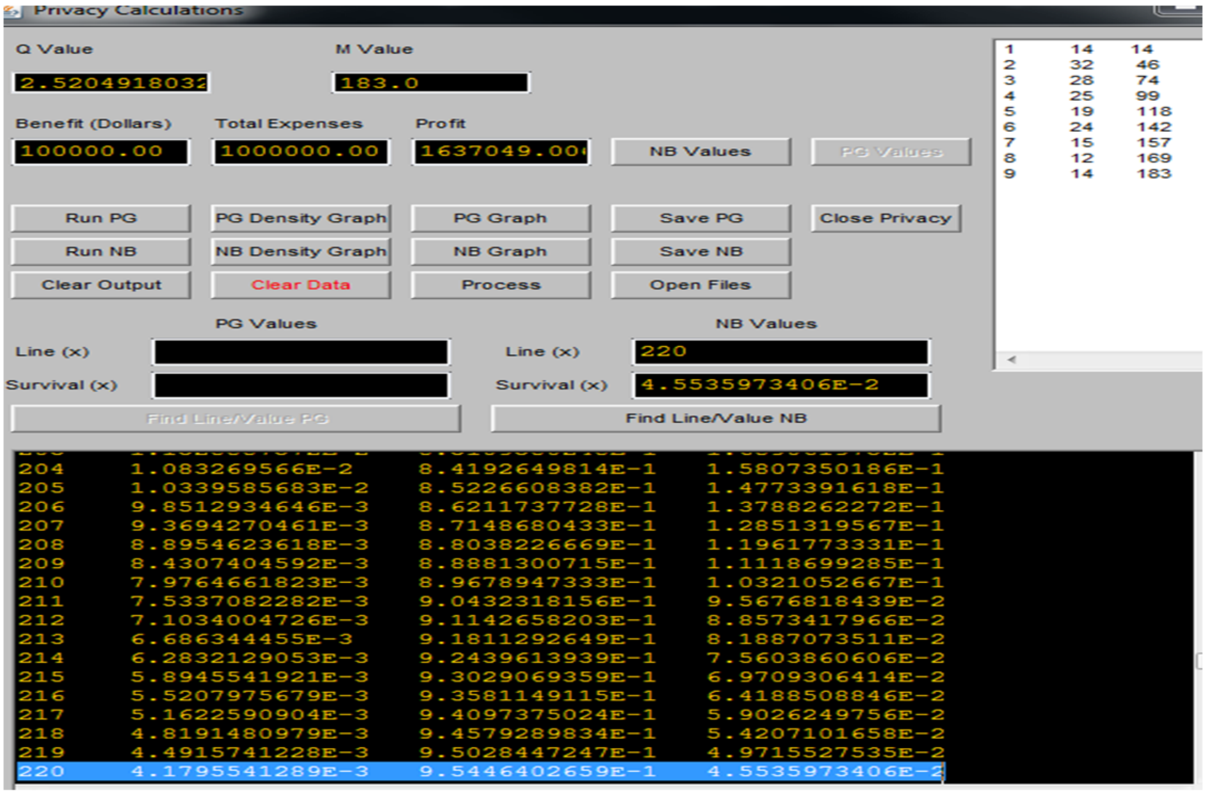

Code Name: Risk Quantifier - An example application to find total risk and cost
for purely qualitative or purely quantitative or hybrid vulenrability and threat inputs.
Help section has detailed information.
Risk Quantifier v2
Main Menu
CM
Criticality: 0.5
Total Cost: 10000
Vulnerability
Vuln. Risk
Threat
Threat Risk
LCM
Residual Risk
Post %
Post V. Cont
Overhaul
v1 0.6 t1 0.5 0.1 0.03 0.050847 0.457627
t2 0.5 0.8 0.24 0.40678
v2 0.4 t3 0.6 0.8 0.192 0.325424 0.542373 !
t4 0.4 0.8 0.128 0.216949
Add Rows
Clear All
Clear Matrix
Defaults
Define Qualitative Attrs.
Calculate
Total Residual Risk: 0.59
Final Risk: 0.295
Percentage Risk: 59
Expected Cost of Loss: 2,950

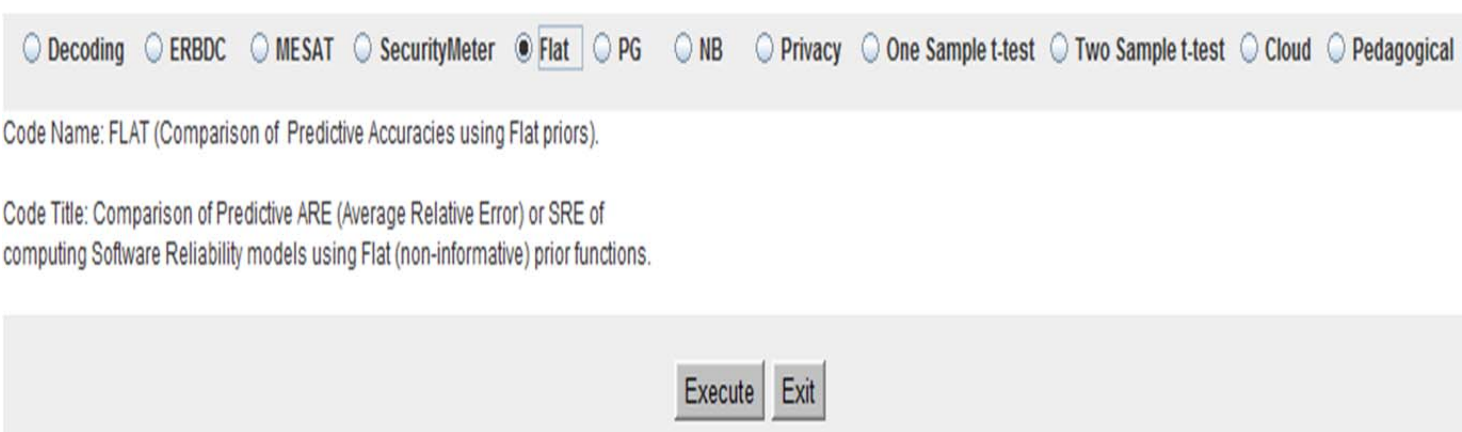

Decoding
ERBDC
MESAT
SecurityMeter
Flat
PG
NB
Privacy
One Sample t-test
Two Sample t-test
Cloud
Pedagogical
Code Name: Cloud System
See Readme File.
Execute
Exit

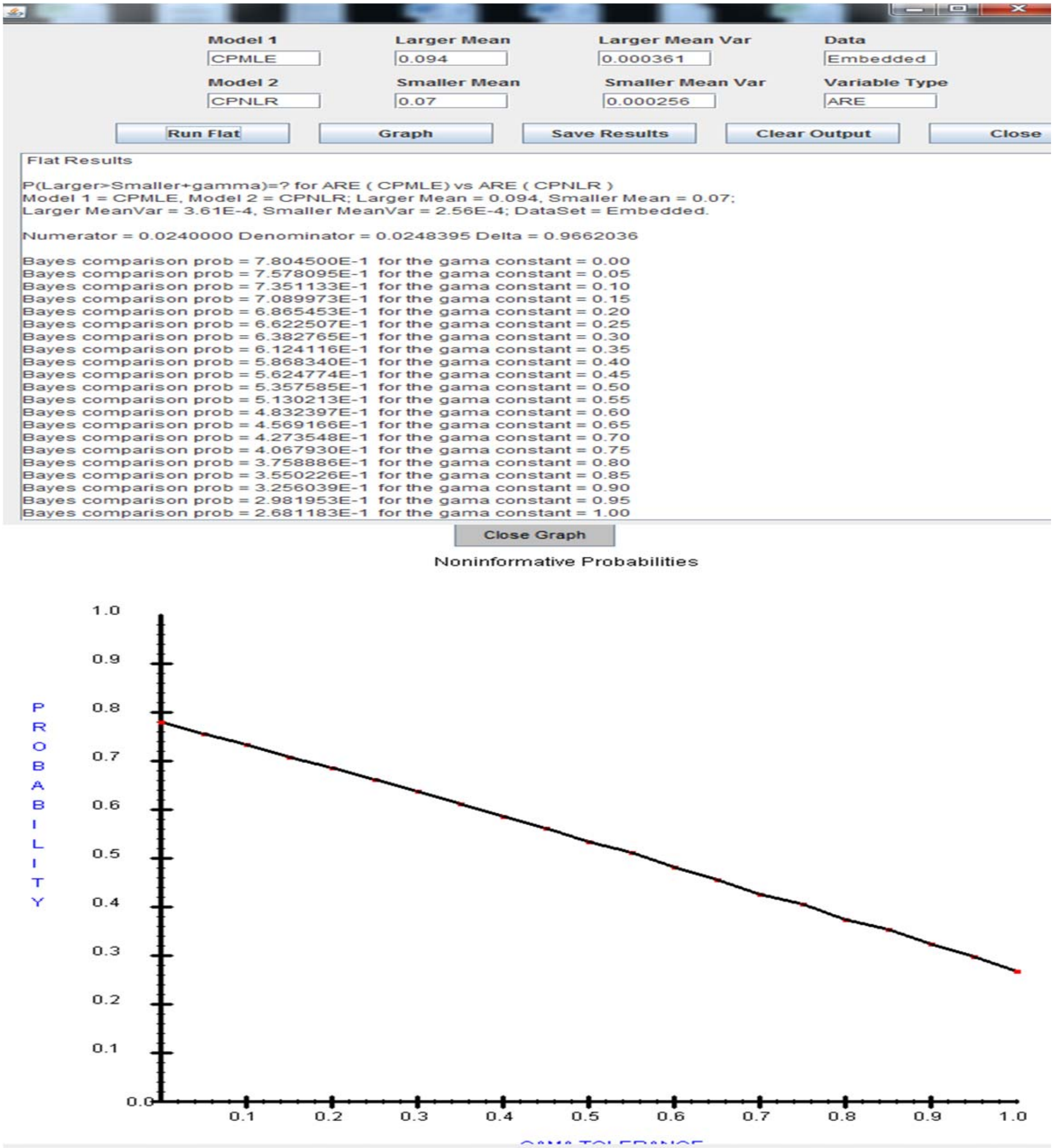

System Application
File Simulation Graphs Print Help
Producers
Group: 1 Submit
Components: 1
Product Value: 1 Delete
Weibull Shape: 1 Exp Dist
Failure Rate: .01 Wei Dist
Repair Rate: .02
System Load Parameters
Constant Load
Percent Load
Variable Load
Multiplier: 1.0
Startup Failure 0.0000001
Startup Delay 0
Add Loads
Add to Range
Delete Range
Multiply Range
Modify Range
Environment Parameters
Maintance Crews 348
Total Cycles (TC) 8760
Simulations: 1000
Lamda0: 0.0000001
Mu0: 0.0000001
Standard Exp
Power Weibull
Cyber Mixed
Time: 0 hr 3 min 16 s
NB Parameters
q 5.0881
M 2.5128
d E
Up Down
Values
Graph
Density
Capacity value: 22
Group: 21
Components: 13
Weibull Shape: 1.0
Failure Rate: 0.0061
Repair Rate: 0.0122
Capacity value: 15
Group: 22
Components: 40
Weibull Shape: 1.0
Failure Rate: 0.0070
Repair Rate: 0.0238
Capacity value: 33
Group: 23
Components: 13
Weibull Shape: 1.0
Failure Rate: 0.0070
Repair Rate: 0.0238
Capacity value: 22
Group: 24
Components: 131
Weibull Shape: 1.0
Failure Rate: 0.0043
Repair Rate: 0.023
Capacity value: 2
8732 12024.0000
8733 11816.0000
8734 11433.0000
8735 11187.0000
8736 10745.0000
8737 9483.0000
8738 8923.0000
8739 8416.0000
8740 8239.0000
8741 8145.0000
8742 8167.0000
8743 8298.0000
8744 7965.0000
8745 8344.0000
8746 8923.0000
8747 9408.0000
8748 9674.0000
8749 9408.0000
8750 9314.0000
8751 9313.0000
8752 8981.0000
8753 9469.0000
8754 10874.0000
8755 10507.0000
8756 9976.0000
8757 9581.0000
8758 9178.0000
8759 9014.0000
8760 8783.0000
Total Load:
85231880.0000

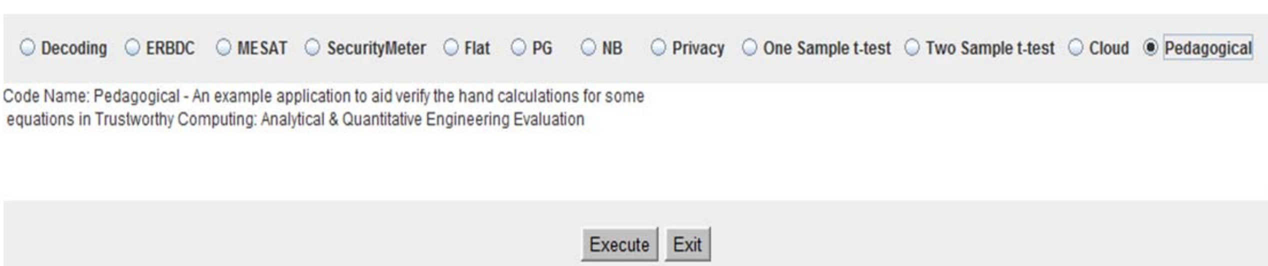

System Application
File Simulation Graphs Print Help
Producers
Group: 1 Submit
Components: 1
Product Value: 1 Delete
Weibull Shape: 1 Exp Dist
Failure Rate: .01 Wei Dist
Repair Rate: .02
System Load Parameters
Constant Load
Percent Load
Variable Load
Multiplier: 1.0
Startup Failure 0.0000001
Startup Delay 0
Add Loads
Add to Range
Delete Range
Multiply Range
Modify Range
Environment Parameters
Maintance Crews 348
Total Cycles (TC) 8760
Simulations: 1000
Lamda0: 0.0000001
Mu0: 0.0000001
Standard Exp
Power Weibull
Cyber Mixed
Time: 0 hr 3 min 16 s
NB Parameters
q 5.0881
M 2.5128
d E
Up Down
Values
Graph
Density
y f(y) F(y) S(y)
x f(x) F(x) S(x)
Component: 131 Capacity: 2
Produced an average of 7363 out of 8760 cycles, resulting in an average of 14726 production units.
Not produced 1397 out of 8760 cycles.
Average cycles not produced due to repair: 1396
Average cycles not produced due to wait: 0.
Average cycles not produced due to startup failure: 0.
Availability: 0.8405
Unavailability: 0.1595
Failure rate: 0.0043
Repair rate: 0.0230
System Summary
Total EPU(Expected Produced Units):
127120828
Total ENPU(Expected Not-Produced Units):
56401172
Total Installed Maximum Produced (IMPU):
183522000
Total Demand Consumption Units (TDCU):
85231880.0000
TDCU + ESPU - EUPU =? EPU
127120828 =? 127120828
Average Duration of load surpluses: s = 43.1123
Frequency of load surpluses: n = 192
Standard Deviation = 110.91075108
Total cycles of Load Surplus Expected: LSE = n * s = 8277
Load Surplus Probability: LSP = LSE/TC = 0.9449
Expected Surplus Production Units: ESPU = 42512435
Total cycles without surplus or deficiency (ties): 0
q2: 236.6830
theta2: 0.9958
alpha2: 0.1829
y Avg. Up Duration Cycles | f(y) Density | F(y) Cum. Density | S(y) Survival
1 0.1822 0.1822 0.8178
2 0.0907 0.2728 0.7272
3 0.0602 0.3330 0.6670
4 0.0450 0.3780 0.6220
5 0.0358 0.4138 0.5862
6 0.0297 0.4436 0.5564
7 0.0254 0.4689 0.5311
8 0.0221 0.4910 0.5090
9 0.0196 0.5106 0.4894
10 0.0175 0.5281 0.4719
11 0.0159 0.5440 0.4560
12 0.0145 0.5585 0.4415
13 0.0133 0.5718 0.4282
Average Duration of load deficiencies: d = 2.5128
Frequency of load deficiencies: f = 192
Standard Deviation = 110.86176171
Total cycles of Loss Of Load Expected: LOLE = f * d = 482
Loss of load probability: LOLP = LOLE/TC = 0.0551
Expected Unserved Production Units: EUPU = 623487
Total cycles without surplus or deficiency (ties): 0
q1: 5.0881
theta1: 0.8035
alpha1: 0.6147
x Avg. Down Duration Cycles | f(x) Density | F(x) Cum. Density | S(x) Survival
1 0.4939 0.4939 0.5061
2 0.1984 0.6923 0.3077
3 0.1063 0.7985 0.2015
4 0.0640 0.8626 0.1374
5 0.0412 0.9037 0.0963
6 0.0276 0.9313 0.0687
7 0.0190 0.9503 0.0497
8 0.0133 0.9636 0.0364
9 0.0095 0.9731 0.0269
10 0.0069 0.9800 0.0200
11 0.0050 0.9851 0.0149
12 0.0037 0.9888 0.0112
13 0.0027 0.9915 0.0085

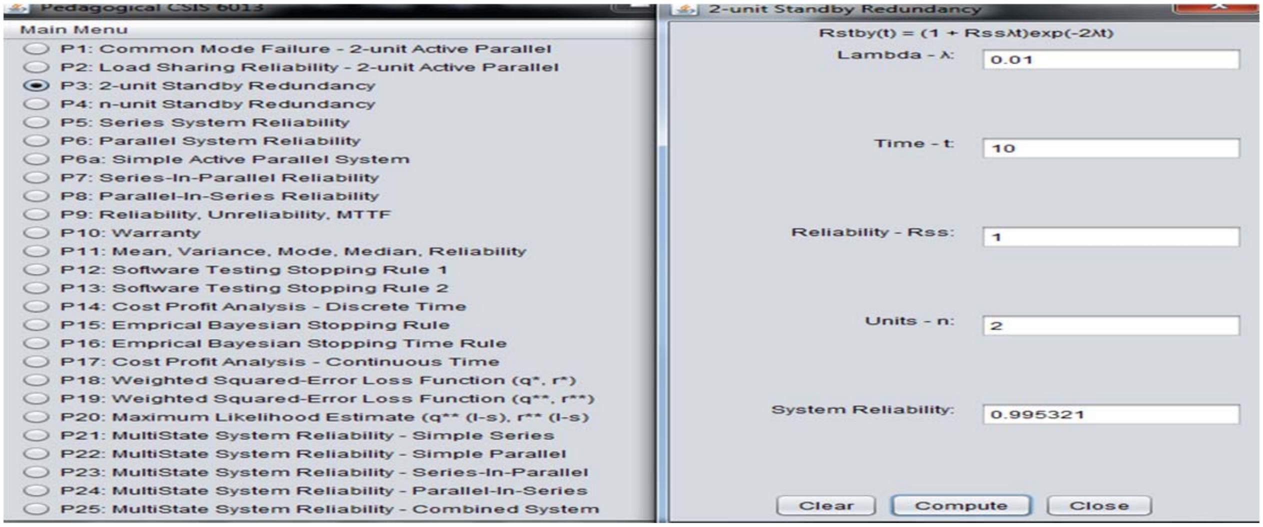

Decoding
ERBDC
MESAT
SecurityMeter
Flat
PG
NB
Privacy
One Sample t-test
Two Sample t-test
Cloud
Pedagogical
Code Name: Privacy
Code Title: Statistical Estimation of Lack of Privacy
Ref. Book Chapter: Chap. 3 (Quantitative Modeling for Security Risk Assessment),
Execute
Exit


Privacy Calculations
Q Value
2.5204918032
M Value
183.0
Benefit (Dollars)
100000.00
Total Expenses
1000000.00
Profit
1637049.00
NB Values
PG Values
Run PG
PG Density Graph
PG Graph
Save PG
Close Privacy
Run NB
NB Density Graph
NB Graph
Save NB
Clear Output
Clear Data
Process
Open Files
1 14 14
2 32 46
3 28 74
4 25 99
5 19 118
6 24 142
7 15 157
8 12 169
9 14 183
PG Values
Line (x)
Survival (x)
Find Line/Value PG
NB Values
Line (x)
220
Survival (x)
4.5535973406E-2
Find Line/Value NB
204 1.083269566E-2 8.4192649814E-1 1.5807350186E-1
205 1.0339585683E-2 8.5226608382E-1 1.4773391618E-1
206 9.8512934646E-3 8.6211737728E-1 1.3788262272E-1
207 9.3694270461E-3 8.7148680433E-1 1.2851319567E-1
208 8.8954623618E-3 8.8038226669E-1 1.1961773331E-1
209 8.4307404592E-3 8.8881300715E-1 1.1118699285E-1
210 7.9764661823E-3 8.9678947333E-1 1.0321052667E-1
211 7.5337082282E-3 9.0432318156E-1 9.5676818439E-2
212 7.1034004726E-3 9.1142658203E-1 8.8573417966E-2
213 6.686344455E-3 9.1811292649E-1 8.1887073511E-2
214 6.2832129053E-3 9.2439613939E-1 7.5603860606E-2
215 5.8945541921E-3 9.3029069359E-1 6.9709306414E-2
216 5.5207975679E-3 9.3581149115E-1 6.4188508846E-2
217 5.1622590904E-3 9.4097375024E-1 5.9026249756E-2
218 4.8191480979E-3 9.4579289834E-1 5.4207101658E-2
219 4.4915741228E-3 9.5028447247E-1 4.9715527535E-2
220 4.1795541289E-3 9.5446402659E-1 4.5535973406E-2

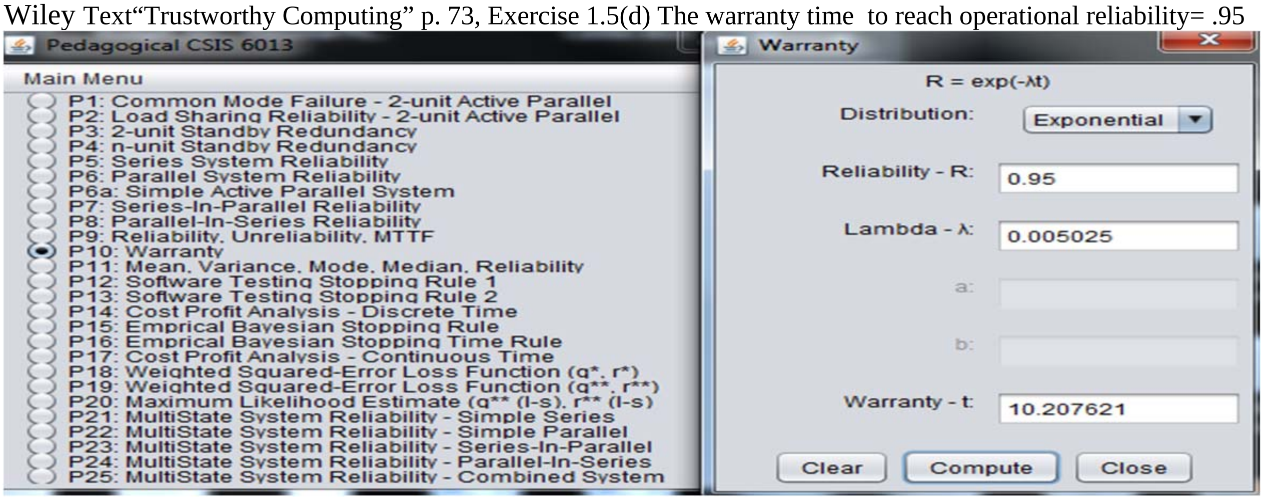

Decoding
ERBDC
MESAT
SecurityMeter
Flat
PG
NB
Privacy
One Sample t-test
Two Sample t-test
Cloud
Pedagogical
Code Name: FLAT (Comparison of Predictive Accuracies using Flat priors).
Code Title: Comparison of Predictive ARE (Average Relative Error) or SRE of
computing Software Reliability models using Flat (non-informative) prior functions.
Execute
Exit


Model 1
CPMLE
Larger Mean
0.094
Larger Mean Var
0.000361
Data
Embedded
Model 2
CPNLR
Smaller Mean
0.07
Smaller Mean Var
0.000256
Variable Type
ARE
Run Flat
Graph
Save Results
Clear Output
Close
Flat Results
P(Larger>Smaller+gamma)=? for ARE (CPMLE) vs ARE (CPNLR)
Model 1 = CPMLE, Model 2 = CPNLR; Larger Mean = 0.094, Smaller Mean = 0.07;
Larger MeanVar = 3.61E-4, Smaller MeanVar = 2.56E-4; DataSet = Embedded.
Numerator = 0.0240000 Denominator = 0.0248395 Delta = 0.9662036
Bayes comparison prob = 7.804500E-1 for the gama constant = 0.00
Bayes comparison prob = 7.578095E-1 for the gama constant = 0.05
Bayes comparison prob = 7.351133E-1 for the gama constant = 0.10
Bayes comparison prob = 7.089973E-1 for the gama constant = 0.15
Bayes comparison prob = 6.865453E-1 for the gama constant = 0.20
Bayes comparison prob = 6.622507E-1 for the gama constant = 0.25
Bayes comparison prob = 6.382765E-1 for the gama constant = 0.30
Bayes comparison prob = 6.124116E-1 for the gama constant = 0.35
Bayes comparison prob = 5.868340E-1 for the gama constant = 0.40
Bayes comparison prob = 5.624774E-1 for the gama constant = 0.45
Bayes comparison prob = 5.357585E-1 for the gama constant = 0.50
Bayes comparison prob = 5.130213E-1 for the gama constant = 0.55
Bayes comparison prob = 4.832397E-1 for the gama constant = 0.60
Bayes comparison prob = 4.569166E-1 for the gama constant = 0.65
Bayes comparison prob = 4.273548E-1 for the gama constant = 0.70
Bayes comparison prob = 4.067930E-1 for the gama constant = 0.75
Bayes comparison prob = 3.758886E-1 for the gama constant = 0.80
Bayes comparison prob = 3.550226E-1 for the gama constant = 0.85
Bayes comparison prob = 3.256039E-1 for the gama constant = 0.90
Bayes comparison prob = 2.981953E-1 for the gama constant = 0.95
Bayes comparison prob = 2.681183E-1 for the gama constant = 1.00
Close Graph
Noninformative Probabilities
PROBABILITY
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1.0

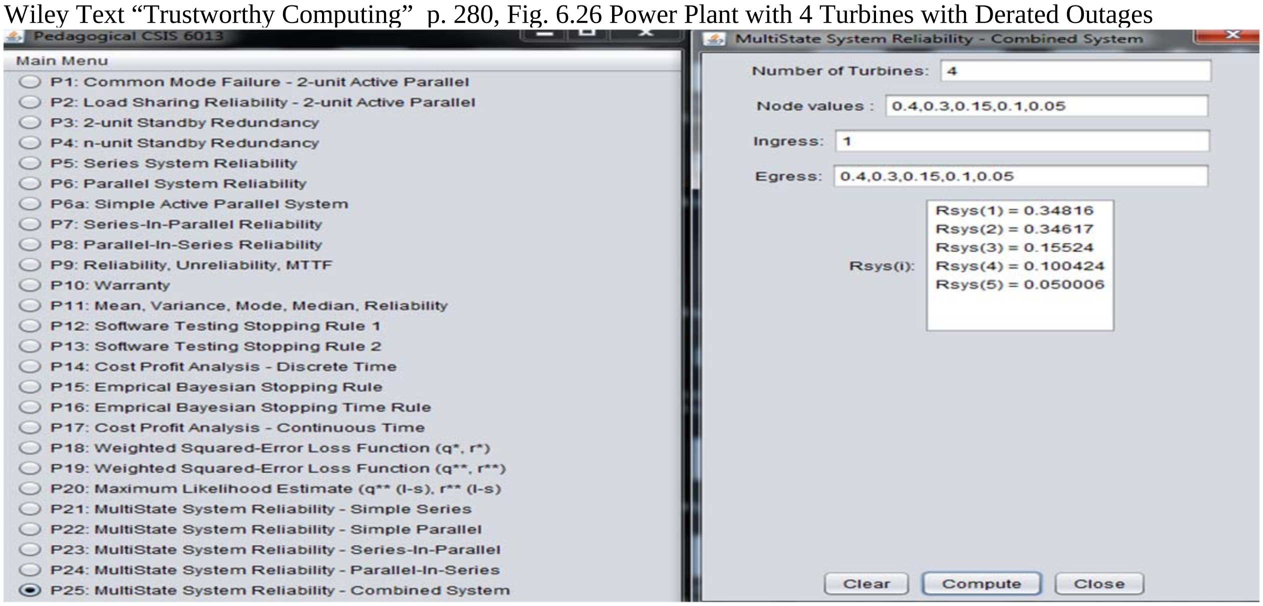

Decoding
ERBDC
MESAT
SecurityMeter
Flat
PG
NB
Privacy
One Sample t-test
Two Sample t-test
Cloud
Pedagogical
Code Name: Pedagogical - An example application to aid verify the hand calculations for some
equations in Trustworthy Computing: Analytical & Quantitative Engineering Evaluation
Execute
Exit



Wiley Text"Trustworthy Computing" p. 73, Exercise 1.5(d) The warranty time to reach operational reliability= .95



Wiley Text "Trustworthy Computing" p. 280, Fig. 6.26 Power Plant with 4 Turbines with Derated Outages



Orchard Park Central School

This Certifies That

Mehmet Sahinoglu

has completed a Course of Study prescribed by the Board of Education and approved by the University of the State of New York for the Orchard Park Central School and is therefore awarded this

Diploma

Given at Orchard Park, in the State of New York, this

June 22, 1969.

Winford A. Swanson — Principal

Paul G. Rohrdanz — President, Board of Education

Official Transcript

GRADES 9 - 12

ORCHARD PARK CENTRAL SCHOOL
Orchard Park, New York 14127
Telephone 716 - 662 9311

ACCREDITED BY
Middle States Ass'n.
N.Y.S. Education Dept.

Name Sahinoglu, Mehmet (AFS) Address 33 Chauncey La., Orchard Park, N.Y. Birth Date 6/23/51 Sex M

Parent or Guardian Mr. & Mrs. Paul Rohrdanz Entered OPCS 9/68 Grade 12 Was / Will be graduated 6/69

Previous School Attended

	R	Final Grades	Unit
ENGLISH			
9			
10			
11			
12			
Adv. Lit. & Comp.		89	1
SOCIAL STUDIES			
Social Studies 9			
World History			
American History (½ year)		91	½
Economics			
Sociology		92	½
SCIENCE			
General Science			
Biology			
Chemistry			
Physics			
Advanced Biology			
Advanced Chemistry		91	1

	R	Final Grades	Unit
MATHEMATICS			
General Math			
Elementary Algebra			
Plane Geometry			
Inter. Algebra			
Math 11			
Advanced Math I			
Advanced Math II		95	1
LANGUAGE			
Spanish I & II			
Spanish III & IV			
French I & II			
French III & IV			
Latin I & II			
Latin III & IV			
German I & II			
German III & IV			

	R	Final Grades	Unit
BUSINESS			
Typing			
Shorthand I			
Shtnd. II & Trans.			
Bookkeeping I			
Bookkeeping II			
Gen. Business			
Business Law			
Business Arith.			
Office Practice			
Sec. Practice			
INDUSTRIAL ARTS			
Technical Drawing		88	1
Electronics (½ year)		88	1/2
Other			
Orchestra		S	1

Class periods are 40 minutes, 5 times a week, 38 weeks a year. School requires 16 units for graduation.

Applicant ranks ______ in a class of ______ students with a 90.36 average. No rank available
Rank computed using numerically graded subjects from grade 9 through ______ semester of grade ______. Average for Honors students determined by [illegible]

SYMBOLS
S=Satisfactory
R=Regents
H=Honors
L-Lab Course
SS=Summer School
RM=Repeat to Raise Mark

GRADE KEY
90 - 100=A
80 - 89 =B
70 - 79 =C
65 - 69 =D
Below 65=U or Failing

TÜRKİYE CUMHURİYETİ

)RTA DOĞU TEKNİK ÜNİVERSİTESİ

ANKARA

Mehmet Şahinoğlu

MÜHENDİSLİK

FAKÜLTESİ

ELEKTRİK

)MÜNDE GEREKLİ ÇALIŞMALARI BAŞARI İLE TAMAMLAYARAK

29 HAZİRAN 1973 TARİHİNDE

ELEKTRİK MÜHENDİSİ

DERECESİNİ

TANINAN BÜTÜN YETKİLERİYLE BİRLİKTE

ALMAYA HAK KAZANMIŞTIR

İ HEYETİ BAŞKANI — REKTÖR — F] ÜLTE DEKANI

REPUBLIC OF TURKEY

MIDDLE EAST TECHNICAL UNIVERSITY

ANKARA

Mehmet Şahinoğlu

HAVING SATISFACTORILY COMPLETED ALL REQUIREMENTS OF

THE DEPARTMENT OF

ELECTRICAL ENGINEERING

IN THE FACULTY OF

ENGINEERING

ON JUNE 29th, 1973

HAS BEEN AWARDED THE DEGREE OF

BACHELOR OF SCIENCE IN ELECTRICAL ENGINEERING

WITH ALL THE PRIVILEGES CONNECTED THEREUNTO

CHAIRMAN, BOARD OF TRUSTEES — PRESIDENT — DEAN OF THE FACULTY

THE VICTORIA

UNIVERSITY OF MANCHESTER

Degree of

Master of Science

in the Faculty of Technology

It is hereby certified that

Mehmet Sahinoglu

been duly admitted as a MASTER OF SCIENCE in the Faculty of
chnology of this University.

H Lipson Dean of the Faculty.

Registrar.

Master is requested to sign here.)

THE UNIVERSITY OF MANCHESTER

EXAMINATION RESULTS

The following result is published subject to confirmation by Senate:

DEGREE OF M.Sc.

(FACULTY OF TECHNOLOGY)

The following have satisfied the Examiners:

By Examination and Dissertation

Abang Abdullah, B.A.A.
Adams, O.M.J.
Adrangi, Bahman
Alexandratos, Anastasios
Al-Saffar, A.H.
Alvi, M.A.
Amin, N.R.
Appleby, T.H.
Arfaei-Malekzadeh, Fazlolah
Aronov, Niki
Awe, A.A.
Awouda, M.E.H.
Bailey, Ruth (nee Mansfield)
Balaram, C.M.
Belazi, Maria C.D.
Bermudez, J.F.
Bevilacqua, G.L.
Birk, G.S.
Bridges, C.E.
Butler, H.J.
Cannas, Ioannis
Cantu, G.M.
Caykoylu, E.S.
Child, P.A.
Chin, Yit Meng
Clarke, Margaret E. (Mrs.)
Coates, B.J.
Colles, J.M.
Coombs, T.J.
Correa, Lorman
Das, U.K.
Depledge, P.G.
Dever, Madeline R.
Din, Sunan
Dines, Steven
Edwards, M.J.
Elamin, I.M.
Eldem, Suleyman
Ercil, M.Y.
Farrell, M.D.
Fatheldin, M.T.
Fazlollahi, Khalil
Fiorotto, Valerio
Fox, W.F.
Fu, Shu-Leung
Gad, Fatma K. (Mrs.)
Garcia Guirola, O.A.
Gates, P.L.
Georgakakis, J.G.
Ghaemi, Amir-Hossien
Hamilton, D.J.
Harper, J.N.
Hawcroft, L.J.
Hill, Linda M.
Hladky, Karel
Ioannou, Dimitrios
Jackson, P.M.
Johnston, Ali
Kamara, D.L.B.
Khachik, Fredrick
Kirkbright, J.D.
Koussiouris, Trifon
Ladeinde, O.O.
Ladopoulos, Eugenios
Lambert, P.W.
Leivers, M.F.
Lombardeas, Michael
Lopez, R.E.
Lyth, Kevin
Meads, G.D.
Mehmetoglu, M.T.
Meijer, P.J.H.
Mohammadi-Yazdi, Reza
Nastas, A.J.
Noriega, Carlos
Oates, C.D.M.
Ogundipe, C.O.E.
Oyedara, A.T.
Paiva, E.D. de A.
Paki, Davood
Pal, A.K.
Palmer, Keith
Polenas, W.S.
Powell, Lynn
Pradhan, P.R.
Quieta, J.C.
Quintas, A.M.L. Da R.
Qureshi, Nadeem
Rabie, A.R.M.
Rajagopal, Krishnamurthy
Ramezani, Parvin
Rashid, H.U.
Reyes, J.A.
Roberts, Christopher
Ronen, Meir
Saebi, Mojtaba
Sahinoglu, Mehmet
Salih, S.E.A.
Scialom, Isaac
Senior, H.S.
Serro, C.A.J.
Sivalingam, Sinnathurai
Solomon, Isaac
Sreedhar, Rajiv
Stampella, R.S.
Stanistreet, K.C.P.
Streets, David
Taiwo, Oluwafemi
Takieddine, F.N.
Tallah, W.S.
Tam, Alex
Tariq, M.H.
Taylor, T.J.
Thompson, C.B.
Tomlinson, G.J.
Tsui, K.C.
Turner, W.H.D.
Underhill, C.J.
Underwood, T.C.
Urquhart, J.H.
Vaidya, A.W.
Valtis-Spanopoulos, Nicholas
Vovos, Nickolas
Vulijscher, S.O.
Wan-Abdullah, B.A.
Watson, A.R.
Weerapperuma, D.G.K.E.
Westall, F.A.
Whalley, John
Wilson, Ronald
Winterbottom, M.A.
Wong, Siu-Hin
Wong, W.H.P.
Yeo, K.T.
Yip, C.W.
Yung, K.M.

Texas A&M University

To all to whom these presents may come Greeting

Be it Known that

Mehmet Sahinoglu

having completed the studies and satisfied the requirements for the Degree of

Doctor of Philosophy

has accordingly been admitted to that Degree with all the honors, rights and privileges belonging thereto.

Given under the seal of the University at College Station, Texas, on the eleventh day of December, A.D. nineteen hundred eighty-one

President of the University

Edwin H. Cooper

Dean of Admissions and Records

TEXAS A&M UNIVERSITY

COLLEGE STATION, TEXAS

ZIP CODE 77843

Office of
DEAN OF THE GRADUATE COLLEGE
(713) 845-3631

December 11, 1981

Dr. Mehmet Sahinoglu
402-A Second Street
College Station, TX 77840

Dear Dr. Sahinoglu:

It is a pleasure to be one of the first to address you as "Doctor" in recognition of the degree conferred upon you on December 11, 1981, by Texas A&M University. Certainly no one knows better than you and your immediate family the personal sacrifices, the long hours of study, and the devotion to scholarly research that the earning of a doctorate requires. I congratulate you upon your achievement, for the doctorate still represents the highest earned degree conferred by the colleges and universities of our nation.

I am sure that in the years ahead you will be a successful and productive person, and like so many of our fine graduates will bring credit not only to yourself, but to Texas A&M University. If this office can be of any help to you in the future, please let me know. I wish for you the best of luck, and a happy and prosperous future.

Sincerely yours,

George W. Kunze
Dean

GWK/ep