Reliability Society

N E W S L E T T E R

January 1995

Table of Contents

Newsletter Inputs

All *IEEE Reliabilty Society Newsletter* inputs should be sent to the editor at:

Bruce Bream
NASA Lewis Research Center
M.S. 501-4
21000 Brookpark Road
Cleveland, OH 44135

Work: (216)433-6532
Fax: (216)433-5270

E-mail: bruce.bream@lerc.nasa.gov

Newsletter Input Due Dates

Newsletter	Due Date
January	November 19
April	February 26
July	May 28
October	August 27

Return to Jan-95 Table of Contents

President's Report

AdCom Election Results. The election results are in. You, the Reliability Society membership, have elected your Administrative Committee (AdCom) members. They will serve you from 1995 to 1997. This is the first AdCom class to be elected by vote of the entire membership.

- Loretta Arellano
- Richard A. Kowalski
- David A. Baglee
- Dev G. Raheja
- David L. Erhart
- Orlin D. Trapp

Twenty percent of the membership cast their ballots in the election. While this is a smaller percentage than we had hoped for, it is clearly large enough to support our action of enfranchising the membership. Reliability Society Audit The draft report of the IEEE Technical Activities Board (TAB) review of the Reliability Society has arrived (November 2). TAB reviews the 37 IEEE Societies in a fire year period and then begins again. The review was generally favorable and is summarized:

A. Mission

The review team found our mission and field of interest to be well

described and current. They also found our positioning in Division VI to be appropriate.

B. Governance

The review team found nothing unusual in this area. They liked our procedure of developing written job descriptions for our officers. Each officer updates the job description and passes it on to his successor. The review team recommended that other societies emulate this procedure. The review team did not like the geographic (no AdCom members in regions seven to nine and ten of the 18 elected AdCom members from region 2) or occupational (14 - industry, three - academia, and one government) of our AdCom. They liked the fact that we have no term limit for our treasurer. Our chapter program was not viewed as a problem however, the review team indicated that there is room for growth.

C. Technical Operations

The review team indicated that we have a very strong technical committee structure with exceptional visibility of the technical committees at the AdCom level.

D. Finances

The review team indicated that the Society's finances are in surprisingly good shape, but cautioned that this could reverse dramatically and quickly. They recommended that we establish long term financial management strategy.

E. Membership

The review team indicated that membership is declining and a potentially serious problem. They recommend that we solicit new members at conferences held by other IEEE societies. They noted that the Reliability Society has a higher number of IEEE Fellows than average and a declining student membership.

F. Meetings

The review team suggested that we consider additional workshops in addition to the major conferences and workshops we currently hold each year.

G. Publications

The review team indicated that our members receive an exceptional publication value for their dues. They particularly like the idea of including the Proceedings from a Society sponsored conference as part of the membership package and recommend that other societies consider doing it. They believe our publication delay is unacceptable - a disservice to authors and members alike. Conclusion "The picture of the Reliability Society that emerged from our review was of a society which is well managed, aware of their problems and (very considerable) opportunities and with a clear picture of what the future will be like in their technical field. However, the review committee feels that their is a serious lack of concrete planning to realize the vision and, in common with much of the IEEE, a lack of the kind of risk-taking dynamic leadership required to make the most of opportunities. With such leadership, reliability, as a discipline, could be positioned as a core capability across the entire spectrum of IEEE activities." Recommendations:

- Define and implement a five year strategic plan
- Formalize a process to achieve a broader geographic and institutional mix of AdCom members
- Become a matrix organization in support of other societies
- Conduct more topical workshops

The audit has been worthwhile. It forced us to take a close look at ourselves. We learned quite a bit from this self examination. We also obtained insight into the activities of other societies, and we

have the benefit of the TAB Review Committee comments which represent an outsider's look at our performance. All of this puts in an excellent position to make substantial improvement to an already excellent society next year. We will welcome the help of the entire membership in this effort.

W. Thomas Weir
President, IEEE Reliability Society

Return to Jan-95 Table of Contents

Editor's Column

The exact answer is not always the right answer. We spend innumerable hours calculating MTBFs, reliabilities and probabilities of failure. We use Mil-Hdbks, databases, computer codes, math coprocessors and sometimes even calculators. We use an array of models and mathematical function to hone in on the exact answer. But what do we really know about the answer? What assumptions were made along the way? What errors outside our structured lists are part of the answer? It may be comforting to some, once the calculation is complete, that a single number pops out of the machine. What's really needed is how good is that exact answer. A decision maker should be asking for more than just one number yet many are satisfied with only meeting an arbitrary goal. A financial analyst would not overlook the notes at the end of an annual report, nor a nutritionist overlook the details of product labeling, nor a car buyer the fine print in a lease agreement. In all of these instances, the users of the information are extending their understanding of an "exact" number by including information about underlying sources of uncertainty. In our field there are many ways to present these potential sources of error and variance. It can range from a simple list of ground rules and assumptions to a probabilistic assessment of the range of the variables being estimated. Obviously, how "exact" must fit the need. But, without some fine print to back up a number, the user can be left out in the cold.

Bruce Bream
Editor, Reliability Society Newsletter

Return to Jan-95 Table of Contents

Chapter Activities

Chicago Chapter

There were two joint meetings held by the Chicago chapter and other IEEE society chapters:

- November 1994 - Reliability of Personal Communications Services (PCS) - Speaker: Mr. David Hume of Motorola - Using the next generation of cellular technology is expected to be less costly and to provide higher quality of service with lighter handsets than current cellular systems.
- July 94 - Reliability of Repairable Mechanical Systems - Mr. Hubert Esser of Deere and Co. - Development of highly reliable systems under time pressure.

Hugh Edfors
Chicago Chapter

Cleveland Chapter

The Cleveland Chapter has had 2 meetings during this reporting period. Our October meeting was the 30th Annual High Technology Symposium. We tried to capture the hot topics for this year in our four technical sessions. The poster session was done by the local colleges. The exhibit area had an excellent display of

hardware, software, tools, literature and services. The symposium had a full house. Some will be sent a copy of the proceedings.

Our November meeting was a "Current Events at NASA". Donald Campbell, NASA Lewis Research Center (LeRC) Director, took some time out of his busy schedule to bring us up to date on current events at LeRC and to interact with the community. LeRC's number one priority is to develop an engine for the supersonic transport that will be acceptable to the people. Total quality efforts are being implemented. Many other changes are being made. Progress is being made on our Journey to Excellence. A timely, well received topic that was well supported.

We have put together a Local Publicity Committee for RAMS '95. Three tasks are being worked: 1) get the RAMS '95 invitations distributed, 2) invite the local colleges to participate, 3) get the sponsoring societies to present their awards at RAMS. We can use more people on this committee. If you are interested in helping with these tasks, contact Vince Lalli at (216)433-2354.

Several other meetings are being discussed: IEEE Video Conference, Winter Tour and Social. All in all here in Cleveland we are having fun staying active and trying to serve our membership.

Vincent Lalli
Cleveland Chapter Chair

Dallas Chapter

The Dallas IEEE Reliability Society has had two outstanding reliability presentations this year at its monthly meetings in September and October. The first presentation was entitled "Focused Ion Beam Milling" and was given by Scott Wills of Beam It Inc. The second presentation was entitled "From Concept to Customer" and was given by Norm Frigon of Quality Associates. The program for the remainder of this year and next year includes topics on 1) Cycles of Learning Key to Reliability Growth, 2) Software Reliability, 3) Atomic Force Microscopy, 4) Total Quality Management, and 5) Reliability Considerations in Sub-Micron Process Development. The wide variety of topics has continued to generate a lot of interest on the part of the attendees and has allowed the society to grow.

Bill Grimes
Chairman, Dallas IEEE Reliability Society

Swiss Chapter

During 1994 the Swiss Reliability Chapter organized, in cooperation with the Reliability Laboratory (RL) of the Swiss Federal Institute of Technology (ETH) Zurich, nine Meetings, one International Seminar, and three Courses. The total number of attendees was more than 300. More than half of the speakers came from abroad (three from the US). A highlight was the Int'l. Seminar on Surface Mount Technology (SMT) with Pitch Down to 0.5 mm. Also because of the investigations at the RL in close cooperation with industry since the early 90's, fully developed design and manufacturing rules for producing high quality SMT with pitch 0.5 were presented. As a second focal point, new approaches based on damage cumulation for investigating crack propagation in SMT solder joints were discussed by Werner Engelmaier (USA), Thomas Ahrens (CEM, Germany), and Ludger Weber (RL). Investigations are continuing for pitch 0.3 mm with the aim of finding out suitable models. Some of the topics discussed in this seminar can be found in the book by A. Birolini "Quality and Reliability of Technical Systems", published by Springer-Verlag 1994.

For 1995, seven Meetings, three Courses, and one Int'l. Seminar (Quality and Reliability Optimization in Fine Pitch SMT) are planned. In the first meeting on January 23, Professor W. Schneeweiss (Fern-Universitat Hagen, Germany) will speak on Fault Trees and their application in reliability. On February 20, Dr.

B. Stamenkovic (Ascom, Berne) will speak on the reliability and availability of complex repairable systems. A detailed program of further activities will be given in the April issue of this Newsletter. The meetings take place at 5:15 pm at the ETH Zurich, room ETF C1. For further information please call Ms. Sybill Steffen at +41 1 632-2743, fax: +41 1 632-1258, e-mail birolini@zuv.ee.ethz.ch.

Professor Alessandro Birolini
Chairman

Return to Jan-95 Table of Contents

FMEA/FMECA Project

The Society of Automotive Engineers G-11 subcommittee on RMS Standards has recently formed a project to develop a new standard for Failure Mode and Effects Analysis (FMEA) and Failure Mode Effects and Criticality Analysis (FMECA). The new standard will replace Mil-Std-1629A and update commercial standards and practices. This is a pilot project of the Partnership in Standards, a joint professional society initiative to replace current military standards (which are no longer being supported) with commercial standards reflecting current "best practices" and management know-how. Anyone interested in participating in this effort or desiring further information should contact:

John Bowles
Electrical and Computer Engineering
University of South Carolina
Columbia, SC 29208 USA
Tel: (803)777-2689
E-mail: bowles@ece.scarolina.edu

Revision to IEEE Reliability Society Constitution

Changes were made to the Reliability Society Constitution in Article III, Section 1 & 2, which incorporate an updating and clarification of our "field of interest". Most IEEE societies have made similar changes this year. These changes have already been approved by TAB and are being published in the newsletter for review by the membership. These changes take effect after publication unless there is objection by at least 10% of the membership (see Article IX, Section 1).

IEEE Reliability Society Constitution
Return to Jan-95 Table of Contents

Free Proceedings

The Reliability Society has surplus copies of the 1992 and 1994 IRPS Proceedings and of the 1993 and 1994 RAMS Proceedings. Free copies will be sent on request, so long as supplies last, to:

- Reliability Society members
- Instructors in reliability (The society will be happy to supply a copy for every member of a class on reliability.)
- Technical Libraries

Those interested should indicate how many copies are desired and which proceedings are wanted. We have only those listed above.

Send requests to Anthony Coppola, IITRI, 201 Mill St., Rome NY 13340. Tel: (315) 339-7075 (prefer fax or e-mail). Fax: (315) 337-9932. E-mail: acoppola@mail.iitri.com

---

IEEE Reliability Society Newsletter
Editor: Bruce Bream

Associate Editor: Dave Franklin

IEEE Reliability Society National Technical Organization Representatives

Welcome! Any Reliability Society member wishing to find out more about any of these joint activities or desiring to participate is encouraged to contact either myself or one of the Organization representatives. If you are already active in one of these organizations, you would be a major asset to our representative. If interested, perhaps you could even become a co-representative.

We try to keep active with these groups and to share the knowledge that is available. In an attempt to build on this sharing, we invite you to contact these representatives and ask for information to be mailed to you. This information typically would be recent meeting minutes and special white papers. In the future we intend to have a column for articles about each of the joint activities.

As you might know, our members are very active with ADCOM Activities in addition to their support as being representatives to the National Organizations and Technical Societies. They could use your support. If you have any questions or need further information, please do not hesitate to call, e-mail or write to me.

Sincerely Yours,
Bill Tonti VP of Tech. Operations

Appointees to National Organizations and Technical Societies

Tony Coppola	American Institute of Aeronautics and Astronautics
Dick Doyle	American Society of Mechanical Engineers
Vacant	American Society for Quality Control
Joe Gruessing	American Society for Testing and Materials
Tom Fagan	Annual Reliability and Maintainability Symposium
Tom Weir	Electrical Power Research Institute
Joseph Caroli	Electronic Industries Association
Vince Lalli	Institute for Environmental Sciences
Puran Luthra	Institute of Industrial Engineers
Fulvio Oliveto	Inter-RAMQ
Harry Schafft	International Integrated Reliability Workshop
O.D. "Bud" Trapp	International Reliability Physics Symposium
Sam Keene	International Software Reliability Engineering Symposium
Randy Freeman	North American Electric Reliability Council
Ray Koehler	Society of Automotive Engineers

Ken Lasala	Society of Logistics Engineers
Sam Keene	Society of Reliability Engineers
Bill Wallace	System Safety Society

Reliability Society
NEWSLETTER
January 1995

Book Review

REVIEWERS
Kenneth P. LaSala, Ph.D., member IEEE
Erik Hollnagel, Ph.D., member IEEE

BOOK REVIEW TITLE
Human Reliability and Safety Analysis Data Handbook

AUTHORS
David I. Gertman / Harold S. Blackman

PUBLISHER
John Wiley & Sons, Inc., 1994, 448 pages.
ISBN: 0-471-59110-6

Human reliability is considered a "black art" by many reliability professionals for a variety of reasons. One reason is the dearth of well-written, instructive information on the subject. Every so often, a text appears that sheds a little more light on the subject. In recent years, texts by Dougherty and Fragola, Park, and Booher have served that role. Gertman and Blackman have continued the enlightenment process with the "Human Reliability and Safety Data Handbook."

The book is laid out as a broad survey of the methods and principles of Human Reliability Analysis (HRA) as it is currently practiced. The book provides a detailed and competent, although incomplete, picture of the current scene and thus complements existing works (e.g. by Dougherty and Fragola, Park, and Booher). Although the book title leads the prospective reader to believe that it is just a compendium of data, the book itself is far more than that. It covers subjects such as HRA, human fault and event trees, existing data sources and data banks, several case studies, the use of simulation, organizational factors, outstanding issues, behavioral mechanisms, and emerging technologies. It provides overviews of the formal methods for estimating human reliability such as THERP, HCR, MAPPS, SLIM and SLIM-MAUD. Similarly, the use of fault trees and event trees in HRA is covered in a comprehensive manner, complete with an example. The second half of the book (Chapters 8 to 14) provides a discussion of some of the important issues in doing HRA: the relation to system safety, the use of simulation, organizational factors, behavioral mechanisms and the representation of errors, and HRA in the light of developing hardware and software technologies.

Although the book is commended for is clarity, its current treatment of a broad range of topics, and the inclusion of examples and case studies, it has some significant shortcomings. The treatment of classical aspects of risk, exemplified by HAZOPs and FMECAs, is conspicuously absent. There is the lack of a summary or conclusion for each chapter or for the book as a whole and an uneven distribution of topics. HRA is almost exclusively treated in the context of nuclear power plants in the US nuclear domain. The possibility that HRA in itself may provide valuable insights into human behavior is not seriously considered. Likewise, there is no discussion of the concept of error modes or error phenomenology. Some of the many figures and tables easily could have been omitted. The index is very poor.

The target audience for this book appears to be the technically trained people in the nuclear power industry who are aware of the importance of HRA and Probabilistic Risk Analysis and who feel a need to learn more about it. However, while this focus on nuclear

power is good for the nuclear power industry and associated government regulatory agencies, it does little to broaden the analysis of human reliability in other applications, such as air traffic control or other "human-in-the-loop" situations. A text that addresses these other applications would be useful.

Return to Jan-95 Reliability Society Newsletter

IEEE Reliability Society Newsletter
Editor: Bruce Bream
Associate Editor: Dave Franklin

Reliability Society
NEWSLETTER
January 1995

CALL FOR WHITE PAPERS

NIST - Center for High Integrity Software Systems Assurance

A Center Established by the
National Institute of Standards and Technology (NIST)
Technology Administration
Department of Commerce

NIST is establishing the Center for High Integrity Software Systems Assurance (CHISSA) as a collaborative approach for government, industry, and academia to make available the technology which is necessary for assuring high integrity software in an ever growing number of applications.

Good dependability techniques developed in the laboratory have not made it into use by development organizations, Conversely, very real problems faced by development organizations are not being addressed by the research community. A major goal of CHISSA is to make it easier for researchers to collaborate with developers to:

1. see how research results perform in practice,
2. improve the dependability of the resulting applications, and
3. direct the researchers' efforts more towards helping the developers with their real problems.

Activities from all aspects of modem society require high integrity software (e.g., software which must and can be trusted to work dependably). High integrity software controls a wide range of essential activities including banking and commerce, manufacturing, education, transportation, health care, and entertainment. It is imperative that the tools and methodologies used to build and evolve these software systems be able to ensure very high quality, reliability, security, and safety.

The emergence of the National Information Infrastructure (NII) and the surge in applications for use on the NII and in other distributed environments (e.g., health care systems, manufacturing, finance, education, the Intelligent Vehicle Highway Systems (IVHS) will greatly magnify these issues since they will inevitably stimulate the use of automated systems involving critical hardware and software functions. CHISSA will be a focal point for addressing the need to significantly improve the robustness, safety, and security of these critical software systems.

CHISSA will pursue visionary solutions to industry-defined problems in the assurance of software-intensive systems. CHISSA will foster and coordinate activities relating to high integrity software system technology. It will help guide research and development, analysis, and testing techniques, conduct assessments on software system technology, and provide transfer of those technologies deemed useful to the industrial sector. CHISSA will cooperate with other Federal agencies, industry, and the research community to develop standards and guidelines for high integrity software. Issues concerning the linkage between software assurance and the systems in which that software is embedded wig be addressed as well. NIST will ensure that CHISSA partners have equitable access to CHISSA solutions.

The program will have three major components:

1. promotion of high integrity software systems research and development;
2. improvement of software system technology assessment;

and
3. acceleration of the transfer and use of high integrity software systems technology.

NIST, with industry, academia, and other Federal agencies' guidance, will establish the initial technology objectives and the demonstration environment that will form the foundation of CHISSA. Guidance from industry, academia, and other Federal agencies is requested in this call for White Papers.

CHISSA will enable immediate and direct guidance, collaboration, and technology transfer of high integrity software system technology among universities, industry, and government. NIST will be responsible for facilitating collaboration and technology transfer. The scope of work performed under the auspices of CHISSA will include research, technology assessment, and technology transfer.

Specific goals are to:

- identify research topics which will potentially have a high payoff for industry.
- identify and address the issues that arise between software and other system components.
- identify technology already in use in actual applications and assess its applicability to other application domains.
- identify and provide facilities for accelerated technology transfer.
- identify methods for and encourage promotion of continuous training in the area of high assurance s software systems for engineers and scientists.
- determine how to structure a CHISSA demonstration facility.

White Papers will be used by the NIST CHISSA Director and the Steering Committee to help select a small set of areas within CHISSA's broader chatter for initial focus. A White Paper should not be a proposal for funding. The White Papers will be used to develop a research agenda, plan workshops and conferences, determine possible CHISSA partners, determine strategies for technology transfer, and develop a proposed Cooperative Research and Development Agreement (CRADA) between CHISSA and its partners.

A White Paper should do at least one of the following:

- identify one or more problems in producing high integrity software systems.
- identify one or more technologies needed by industry to produce high integrity software systems.

White Papers should clearly describe the importance of the effort to industry. If a technology is involved, the maturity of the technology, and the steps needed to transition it to industry should be discussed.

Submissions from industry should identify problems where the state-of-the-practice is inadequate, and where known research efforts fall short of the mark in addressing the real issues. In all cases the White Paper should describe CHISSA's role in bridging the gap.

A White Paper may propose a specific short- or long-ten-n project for collaboration. A White Paper may propose collaborative programs in areas identified in the examples in this announcement; White Papers in other innovative areas of high integrity software system technology are also welcome. Examples of specific areas of interest to CHISSA include, but are not limited to:

- methods for the modeling, analysis, and certification of high integrity attributes (timeliness, fault-tolerance, safety, security).

- methods for assessing the correctness, consistency, and completeness of requirements specifications.
- methods for ensuring that the implementation correctly implements the requirements specification.
- methods for achieving dependability in real-time distributed environments.
- methods for ensuring safety, security, or performance in critical systems, particularly in the presence of faults, unpredictable workloads, or operator errors.
- identification of the best or acceptable practices for the software engineering of dependable systems.
- methods for validating and testing dependable software based systems.

CHISSA will create an environment for highly productive focused research and development through coordination of efforts between research and industry. CHISSA will provide a major forum in which alternative theories and results can be openly discussed and evaluated.

CHISSA will share designs, prototypes, tests and measurement techniques with American industry, helping the private sector to implement highly dependable systems and products.

CHISSA will use its close working relationships with academia, industry, and government centers to enable coordination of efforts and utilization of the most modem and efficient ideas, tools, and techniques available.

While CHISSA invites White Papers to be submitted at any time, the Steeling Committee will develop CHISSA's initial focus and research agenda from those submitted no later than January 21, 1995:

Please submit White Papers to the CHISSA Director:

Mrs. Dolores Wallace, CHISSA Director
National Institute of Standards and Technology
Room B266, Technology Building
Gaithersburg, MD 20899
E-mail: dwallace@nist.gov
Fax: (301) 926-3696
Tel: (301) 975-3340

The Steering Committee consists of representatives of industry, academia, and government:

Mr. John Dehn - Loral Corporation
Ms. Helen Gill - National Science Foundation
Dr. George Gilley - Aerospace Corporation
Mr. Charles Howell - Mitre Corporation
Dr. John Knight - University of Virginia
Mr. Gary Koob - Office of Naval Research
Dr. John Salasin - Advanced Research Projects Agency
Dr. Fred Schneider - Cornell University
Dr. Dan Siewiorek - Camegie Mellon University
Dr. Charles Weinstock - Software Engineering Institute

Return to Jan-95 Reliability Society Newsletter

IEEE Reliability Society Newsletter
Editor: Bruce Bream
Associate Editor: Dave Franklin

Reliability Society
NEWSLETTER
January 1995

EDCC-1 Report

Report of the First European Dependable Computing Conference EDCC-1

The First European Dependable Computing Conference EDCC-1 was held in Berlin, Germany, from October 4 to 6, 1994. A total of 122 researchers from Europe and overseas met in the Berliner Congress Center to present and discuss research results in the field of reliability and safety of computing systems.

EDCC-1 started a new pan-European conference series on hardware and software dependability. It complements the world-wide Fault-Tolerant Computing Symposium series (FTCS) to stress the importance of Europe's universities, research institutes and industry. Future EDCC's will be held every two or three years in different European countries, to establish a permanent meeting point for researchers from all over the world.

EDCC is the continuation of two conference series that were held independently in the formerly separated Europe -- the national series "Fault-Tolerant Computing Systems" organized by the German interest group on fault-tolerant computing systems and the series "Fault-Tolerant Systems and Diagnostics" held in various east-European countries. The choice of Berlin as the EDCC-1 conference location can be taken as a symbol for the scientific opening and cooperation in the field of dependable computing.

The field of dependable computing covers all the techniques for specifying, designing and validating computer systems that can be justifiably relied upon. The faults and imperfections that are a fact of life in any complex technical development process or system must be considered from the outset so that specific counter-measures and/or fault-tolerance techniques can be envisaged. These issues are becoming more and more important since our society is becoming increasingly dependent on computer-controlled systems. In some applications, computer system failures can lead to injury or loss of human life. Even in non-safety-critical applications, computer failures are highly undesirable since they can lead to expensive down-times and repair costs.

EDCC aims to be a high quality conference series with a rigorous paper review process. For this first edition, 106 full-length papers were submitted and sent to 5 different referees for review. Most papers (91.5%) received 4 or more reviews and all papers were reviewed by at least 3 referees. Finally, 34 papers with authors from 16 different countries were selected to be presented at the conference and included in the proceedings (published as no. 852 in the Springer Verlag Lecture Notes in Computer Science series). The technical sessions at the conference covered the following areas:

- hardware fault detection and fault tolerance;
- software testing and software diversity;
- fault tolerance techniques, parallel and distributed systems;
- fault injection, measurement and evaluation.

Also, a panel was held on "future directions of dependable computing'", with panelists from both industry and academia.

The topics presented during EDCC-1 pointed out that fault tolerance must be implemented in an efficient way and must not

disturb other desired system properties -- a challenge that arises with each new type of computing system. It was also stressed that validation the dependability of complex systems requires a combination of assessment methods that must be made as accurate as possible.

The new EDCC conference series has been put on a broad international basis. The first event in Berlin was organized by the German "Fault-Tolerant Computing Systems" joint interest group of the Society for Informatics (GI), the Society for Information Technology (ITG) and the Society for Measurement and Automation Technology (GMA). International support was given by several other organizations from different European countries, the European Community and world-wide technical societies:

- the AFCET "Dependable Computing" Working Group, France;
- the AICA "Dependability of Computer Systems" Working Group, Italy;
- the IEEE Technical Committees on Fault-Tolerant and Real-Time Computing;
- the IFIP 10.4 Working Group on Dependable Computing and Fault Tolerance;
- the EWICS TC7 "Safety, Reliability and Security" Technical Committee;
- the EC-ESPRIT Basic Research Network of Excellence on Distributed Computing System Architecture (CaberNet);
- the "Dependable IT Systems" Working Group of GI;
- the "Test and Reliability of Circuits and Systems" Working Group of GI;
- CEPIS, the Council of European Professional Informatics Societies.

The organization of EDCC-1 was in the hands of Prof. Dr. Klaus Echtle, Universitat Dortmund (General Co-Chair), Prof. Dr. Dieter Hammer, Humboldt-Universitat Berlin (General Co-Chair); Dr. David Powell, LAAS-CNRS, Toulouse (Program Chair), Prof. Dr. Erik Maehle, Universitat Paderborn (Publicity Chair), Dr. Volker Schanz, ITG in VDE, Frankfurt (Finance Chair), Dr. Jacob Abraham, University of Texas, Austin (International Liaison Chair), Dr. Yoshi Tohma, Tokyo Institute of Technology, Tokyo (International Liaison Chair).

Return to Jan-95 Reliability Society Newsletter

IEEE Reliability Society Newsletter
Editor: Bruce Bream
Associate Editor: Dave Franklin

Reliability Society
NEWSLETTER
January 1995

RESPONSE TO RELIABILITY SURVEY

by Sam Keene

Eight detail responses have been received in response to the failure rate prediction survey. The survey questions were mailed to select cross section of reliability practioners. They have also been published in the October issue of the IEEE Reliability Society newsletter. The breakdown of responses received so far is shown below per category of questionnaire document:

Your feedback on these findings is welcomed. This study will continue into better prediction techniques and better failure prevention methods. This reliability investigator is very interested in 2-way networking with interested practioners as these studies progress. Please express your interest to Sam Keene, can best be contacted by mail: 3081 15th Street, Boulder, Colorado 80304, or by e-mail at Sam_Keene@stortek.com.

2.1 Product Definition

Respondent	#	1.2 Application	1.3 Product size	1.4 Software KSLOC
1.1 Government-Aerospace	2	Weather, NASA	All sizes	Up to 1 MSLOC
1.1 Defense	3	Avionics, radar, satellites	FRU, SRU, subsystem	Varies
1.1 Commercial	4v	Computer products, industrial products	PCs to Mainframes, boards, chassis	Up to 500 KSLOC, Up to 70 KSLOC
1.1 Medical	1	Embedded controls on medical equipment	Bread box chassis	Up to 5 KSLOC

2.2 Reliability Estimation Process

Prediction Characteristic	Use
Prediction models used	Modified Mil HDBK-217 (9 responses) Belcore (1), sometimes British Telecom, NPRD-91, NASA uses additionally: Praise, QAR tracking, Relcalc, Relex, Spreadsheet PRACA
Customization techniques	Manufacturer's field and test data, RACs operational translation; apply evolutionary product history. Generate own pi quality factor (.5 to 2), about an order of magnitude less than MIL-HDBK-217 to fit operational field experience.
Who uses model output ?	Marketing, design, logistics, field support, reliability engineers

Use of data	Life Cycle Cost estimate, reliability engineers to assess if product meets its goals, establish sparing needs, estimate maintenance support, conduct trades, program design reviews, marketing to "sell" reliability and use of redundancy
How do you estimate software reliability?	Based upon experience scaled to the extent of new code, IEEE standard 982 is a starting point
Relative contribution of software to product failure rate	Significant factor; one of the largest, especially on larger systems, some people dont measure it in cases where it is not specified, substantial contribution but data is rare, software and hardware failures are often reported by different means.
What improvements would you like to see?	Would like better field data via on-board telemetry to capture environment and procedures, time changes in failure rates (Weibull), keep up with technology changes, integrate with CAD files, major product manufacturers cooperating to share data to upgrade MIL-HDBK-217
How satisfied are you with your prediction approach?	Good (acceptable) based on the cost and ease of using it, predictions come out both higher and lower when using it, would like the prediction to have more influence on the design. Most everyone feels improvements would be welcomed, better component models, parameters such as humidity are missing.

2.3 Prediction Validation

Characteristic	Results
How do you validate your predictions ?	Compare to field operations data, accelerated testing on new products, factory testing, perform simulations. Some folks dont have the opportunity or feedback to validate their data. They might be building one of a kind systems and do not have the benefit of experience that comes with evolutionary product development.
How close do your predictions come ?	Two vendors have consistently come within +/- 15% of field operations on like products, some predictions underestimate, some overestimate. Another vendors predictions come with 5% using a modified MIL-HDBK-217 model after taking out induced failures. One developer finds failures enter the constant failure region after one metric year (10 Khrs). Wear-out only observed on non-electronic parts (in the large).

2.4 Failure Drivers

Different developers mentioned these in order of importance:

- Design robustness (lack of), No Defect Found (NDF), supplier quality problems, manufacturing
- All (design, requirements, ...)
- Design, test, manufacturing, supplier quality problems, wear out
- Manufacturing (60), component problems (30), design (10)
- Design (25), manufacturing (25), supplier quality (25),

customer misuse (15), unknown (10)

- Manufacturing (40), Design (15), component quality (40), unknown (5)
- Non component drivers (85), components (15)
- A lot of problems are quality related
- Manufacturing flaws, design defects, supplier problems and NDF

2.5 Prediction Concerns and Observations

1. Mil-HDBK-217 considers only design and not process, e.g. manufacturing problems. There is historic controversy over this text [1,2]. It is easier to criticize than replace. There are valid criticisms of its use of constant failure rates. IBM has its own data base of part failure rates called ALORS. They test their piece parts and do Weibull analysis of the test results. Field data is then analyzed in order to validate the test data. A step-wise failure characterization is then made of the component failure rate over time. A lot of companies cannot afford to do these component characterizations. So MIL-HDBK-217 affords simplicity of use and a common failure rate baseline. Three out of ten people responding to the survey indicated they have been able to successfully tailor the 217 data to closely predict their field data. They all have the advantage of working with an evolutionary product line. This gives them a good calibration point for calibrating their use of the failure rate handbook.
2. Commercial quality pi factor is too high. One company uses a pi-factor of 2 to 3 instead of 10 (cf. ceramic capacitors) for commercial parts as given in the handbook. Another uses .7 to 1.0 typically but applies this only random failures (common cause) after factoring out the special cause and NDF problems. The apparent fraction of the common cause failure portion runs about 25% of all failures. Since the company using the 2-3 factor accounts for all problems, this scaling seems consistent between the two companies.
3. Plastic devices have become preferred and superior to ceramic, but the handbook does not reflect this.
4. Power IC's should have a higher failure rate than low power ICs. This developer uses a power transistor failure rate of order of .6 for power ICs rather than the handbook guidance and uses op amp rate of the order of .003 per the handbook guidance. The smaller number is deemed more appropriate for low power ICs.
5. Current prediction techniques account only for breakage and not adjustments.
6. One respondent said that wear out failures were not seen on his product. If they were, he asserted, they would really be a design failure since preventative maintenance should be designed to cover such cases.
7. Failure rates typically have a bathtub shape with more personality than the constant rate shown by the failure rate texts. One supplier has found that it takes a metric year (10K hours) to come out of the falling failure rate period in order to achieve the constant rate period.
8. No defect found (NDF) or could not duplicate (CND) are a major finding (30-60%) of returned FRUs analyzed at the depot. It is believed that this is more of a logistics concern than a reliability concern. NDF's likely come from the service person pulling too many FRUs to assure the right one was replaced.
9. Solder joint reliability should be affected by the length of the leads being soldered.
10. The breakdown and priority of the failure drivers will depend upon the level of applicable system integration. The higher the level of the system, the greater the impact of proper requirements, system management factors, robust design, software, etc. At the component level or the lowest level the reliability problem it comes down to its

simplest dimension. Hardware and material concerns dominate at the part level.

11. One developer suggested that both the traditional failure rate approaches such as MIL-HDBK-217 and Belcore have their merits. Perhaps these techniques can be expanded into more parallel methods to take advantage of the detail of information available. This would extend the two levels of analysis (parts count and part stress) currently provided by MIL-HDBK-217. The more data available the greater the depth of analysis applied.
12. One respondent mentioned that the complexity of the physics of failure will keep many people from using that approach.

2.6 Respondents to the Survey

The following twelve organizations have contributed substantial perspective to this survey:

- Government-Aerospace: NOAA, NASA
- Defense: Arinc, GI, Aerojet
- Commercial: *Unisys, Storage Technology, DEC (Europe), Innovative Software Design Relex (software), Swiss Reliability Consultant, Boeing (data supplied previous to survey)
- Medical: Pfizer Labs

** Note that only four commercial developers supplied detail responses to the survey. The other two respondents supplied valuable, but more general, perspectives.*

The intention is to maintain a cross industry network of reliability professionals to dialogue and contribute to the development of the new reliability assessment model. The above mentioned organizations will form the first part of this network. The model development will also be publicized in the journals as well as in the trade press and the IEEE Reliability Society newsletter. The editor of "Reliability Review" has indicated his desire for publishing updates on the progress of the model development. The first article will be published in December 1995. This networking will stimulate further interest and awareness of this effort. The interest demonstrated so far show a willingness and benefit of reliability professionals to contribute to this effort.

2.7 Conclusions based upon the questionnaire

Mil HDBK-217 was seen to be the most universally applied failure rate reference. This is true across military, government, and commercial reliability practices. Developers have adapted it by adding in detailed manufacturer's data or test data when it is available. Those developers who have evolutionary products have been able to successfully tailor their predictions based upon field experience with their predecessor products. This adaptation has been accomplished by making suitable modification to the quality pi factor from the handbook. MIL-HDBK-217 has been embodied in automated tools delivered by suppliers of failure rate modeling tools. More is desired. The developers would like a model that keeps up better with technology. Some indicate that the constant failure rate is not truly representative. They would also like one that addresses the special cause or process concerns. A tool is also desired that proactively aids the development of a reliable design: the new model will do that.

Return to Jan-96 Reliability Society Newsletter

IEEE Reliability Society Newsletter
Editor: Bruce Bream
Associate Editor: Dave Franklin
Last Update: 10-January-1996