SAFECOMP82 - Second International Workshop on Safety and Reliability of Industrial Computer Systems

Bergman, Sten

1982

CODEN:LUTFD2/(TFRT-8038)/01-20/(1982)

SAFECOMP82

Second International Workshop on Safety and Reliability of Industrial Computer Systems

Sten Bergman

DEPARTMENT OF AUTOMATIC CONTROL
LUND INSTITUTE OF TECHNOLOGY

October 1982

LUND INSTITUTE OF TECHNOLOGY
DEPARTMENT OF AUTOMATIC CONTROL
Box 725
S 220 07 Lund 7 Sweden

Document name
Travel report

Date of issue
October 1982

Document number
CODEN:LUTFD2/(TFRT-8038)/01-20/(1982)

Author(s)
Sten Bergman

Supervisor

Sponsoring organization

Title and subtitle

Summary - Safecomp82, Second International Workshop on Safety and Reliability of Industrial Computer Systems

Abstract

SAFECOMP82 - addressed practices and procedures in the area of:

1. Specification Languages
2. Operating Systems
3. Man-Machine Interfaces
4. Hardware/Software redundancy
5. Verification and Validation
6. Hardware Software Maintenance

This summary briefly discuss the presented papers and the following discussions, with respect to the six sessions.

Key words

Classification system and/or index terms (if any)

Supplementary bibliographical information

ISSN and key title

ISBN

Language
English

Number of pages
1-20

Security classification

Recipient's notes

Distribution: The report may be ordered from the Department of Automatic Control or borrowed through the University Library 2, Box 1010, S-221 03 Lund, Sweden, Telex: 33248 lubbis lund.

SUMMARY OF SAFECOMP82 - SECOND INTERNATIONAL WORKSHOP ON SAFETY AND RELIABILITY OF INDUSTRIAL COMPUTERS, PURDUE UNIVERSITY, 11 - 14 OCT 1982.

by

Sten Bergman

Department of Automatic Control
Lund University of Technology

BACKGROUND

The goal of the workshop was to focus on six major issues, developed by international committees like IFAC, IEE and ISA, directed to the following objectives:

- To review and evaluate software and hardware design principles and practices, affecting safety and impacting reliability, quality and cost.
- To characterize the current state of safety related hardware and software engineering in the process control industri.
- To achive formalised thinking and conclusions on critical issues, raised by the process control community.

The general purpose of the workshop was thus to bring together at an international level, experienced and recognized experts in the field of computer system safety and reliability. The workshop was held at Purdue University, Indiana, USA and visitied by 70 persons, representing 10 countries. The following issuses were discussed:

Specification languages, Operating systems, Man-Machine Interface, Hardware/Software redundancy, Verification and Validation and Hardware/Software maintenance.

This summary will briefly discuss the presented papers and the

conclusions from the following discussions with respect to the six sessions.

SESSION 1 - SPECIFICATION LANGUAGE

Two papers were presented in this session. The first paper, "Specification transformations in the program development", presented by prof. Matsumoto, Thosiba Co, defined the program development process as a series of transformations from the requirements, to the last step which results in computer executable code. Three models were adopted, namely: The requirements model, the control and data-flow model and the program structure model. Prof Matsumoto stated, that by this model in mind the programmers could work efficiently and given the development tools both the system safety could be increased and cost cutted. The different modules could be supported by a database and program module library.

In the second paper "Specification languages and computer aided development support techniques to achieve reliable and safe systems: present status and future directions ", prof. Lauber, University of Stuttgart, presented a similar concept. However, in his model was the program development process not described as a series network, but more as three interconnected procedures, addressing: Conceptual development, Operational development and Auxiliary development. Before these stages could be applied, the definition of system goals and the analysis of system specification and requirements have to be done. Prof. Lauber presented a CAD package (EPOS80) supporting system specification and code generation. The package, which is commercially available, runs on minicomputers and presents information in the form of hierarchy diagrams of all system modules, data-flow diagrams, control-flow diagrams, Nessi-Schneider diagrams, Petri-nets, Time-diagrams and Block diagrams. System safety and fault avoidance are thus increased by using tools implemented in EPOS80 to check the consistency and completeness of all requirements in the specification.

Prof Lauber was rather optimistic and he thought that in the future, by using efficient computer aided design packages all sofware faults could be removed. He also pointed out a number of successfull projects with safety related issues, to which this technique had been applied, Railway control, aircraft landing system , turbine monitoring etc.

The conclusion of the following discussion was that a number of promising concepts now exists. Also a great hope was addressed to

future expert systems which should handle the transformations from specification (natural language) into computer understandable language (high level languages).

SESSION 2 - MAN-MACHINE INTERFACE ISSUES

In this session the reasons for having human operators, in contrast to full automation, were discussed. Also topics concerning operator workload during emergencies and the need for standardized human-process interface were presented.

A rather detailed description of MMI problems, connected to CRT was given in the first paper "Four views of human-process interface", given by R. Shirly, Foxboro Co.

In the second presentation, L.Beltracchi, NRC, presented MMI problems associated with nuclear safety display panel systems and associated regulatory aspects.

In the following discussion many ideas on the operators role in safety systems were discussed. Also here were future "expert-systems" supposed to be of significant help for an operator in a stressed situation as a decision aid.

It was also pointed out that more often operators have a more complex model of the plant, than the designer. It was suggested by some of the participants, especially those representing utilities, that operators should design their own MMI interfaces. Good results have been obtained.

Summing up the session the main points were that the most recent advances in MMI technology is the use of ergonomics in the design and the technological development of new display systems.

Among the more promising concepts for the future, the human cognitive process modelling, AI expert-systems and data management systems were pointed out.

Another technique which also was mentioned, was to adopt pattern recognition for better alarm-handling. As the remaining problems in this area alarms and system complexity were highlighted.

SESSION 3 - OPERATING SYSTEM ISSUES

In this session, addressed to how operating system could achieve safety three papers were presented.

The first paper, " The contribution of operating system to safe and highly available systems", presented by T. lalive D'epinay, Brown Bovery, described how system architecture and operating system construction are related. The computer network architecture was described in terms of processors, nodes, pools and networks. It was also presented how the use of high-level languages not only could increase the quality of software, but also increase system safety and efficiency.

The operating system could be seen at two levels. The first level visible to the user defining functions for process synchronization, process management and communication. The second level, non-visible to the user containing functions for dispatching, scheduling and low-level communications. It was pointed out that operating system kernels can be constructed without too much complexity.

The second paper, "Reliability and safety considerations in operating systems for process control", given by P. Griem, Foxboro Co., addressed the safety aspects in process control systems (e.g. Foxboro SPECTRUM). Different aspects on multi-loop controllers, operation modes and operating systems functions were presented.

In the third paper, R. Andersson, August System Inc., presented "A technique for reaching agreement in triplicated systems". By using three computers in a triplicated system and a special technique for communication error detection the overall system MTBF could be increased from 1 year to 300 000 years.

The discussion from this session pointed out some more promising concepts. Examples were that more and more functions now are realized directly in hardware, due to the complex LSI designs. Also the redundancy at chip level was pointed out as an recent advance. Other advances in the technology stressed such possibilities as operating systems direct in LSI, distributed data bases and effective communications. Also the use of simple kernels in operating systems was mentioned.

SESSION 4 - HARDWARE SOFTWARE REDUNDANCY

In this session three papers were presented concerning the design of fault tolerant systems. Both hardware and software problems were addressed. In the first paper, J. Goldberg, SRI, presented "The use of redundancy for for reliable design and realization". A variety of redundancy techniques were suggested. First algorithmic redundancy as a technique to achieve robustness with respect to sensor failures and computational errors. Second, time redundancy in the form of computational roll-back, as a method for reducing some realization faults and temporarily errors. Third, error detection and masking by n-fold replication, which is the most used one. Fourth, reconfiguration redundancy, to prevent accumulation of permanent realization failures.

In the second paper, J. Wensley, August Systems Inc., presented "Fault handling in the August System series 300", which is a commercial process computer, designed to be fault tolerant.

The basic concept in this system is to triplicate the processors, and by a asynchronous check procedure compare both transmitted and recieved data. If a failure is detected a special hardwired majority voter will isolate the failing processor.

In the third paper, "Alternative designs of fault tolerant systems", presented by W. Foster, Stratus Computer Inc., the design approach of highly fault tolerant computer system was described. The Stratus/32 computer system uses hardware duplex design and failure detection. In a redundant system, four CPU's thus acts as one CPU. In every clock cycle, comparison of processor output is done on each board. If an error is detected, this board is stopped and by a special diagnostics residing in firmware the faulty board is exercised. If the failure was of transient nature, the board is resynchronised with the other board and taken into operation again. By storing a log in EPROM, on each board, the history of each reparable unit can be tracked.

The conclusions from this session were that commercially available fault tolerant computer systems now exist and that fault-tolerance can be made transparent to the application engineers. One reason is of cource the very cheap hardware which gives the opportunity of system diversity. Also the structural design of high-level languages like PASCAL, ADA, PL/M etc was pointed out as promizing for achieving safety and highly reliable designs. However, as the remaining problems in this area the unsolved licence problem and the need for high-level

specification requirements was mentioned. Another problem, also discussed was the CRT and human interface redundancy as well as how complex system should be tested to validate the requirements.

SESSION 5 - VERIFICATION AND VALIDATION

Three papers were presented in this session addressed to software verification and validation in safety related systems. The first paper, "Experiences in validation and verification in nuclear applications", N. Thomas, Science Application Inc., presented the state-of-the-art in system development for nuclear applications. Different specifications, both in hardware, software and system-integration was highlighted. Also methodology was presented.

The second paper "Software validation and verification methodology in the nuclear field in Germany 1982", given by U. Voges, Kernforschungszentrum Karlsruhe, addressed the use of distributed micro-processors in safety oriented reactor shut-down system, applied to a German breeder-reactor (KNK II). By using a network, consisting of 12 microprocessors and a high degree of inter-processor communication, the time between production and detection/isolation of errors can be minimized without decreasing the overall-system availability. By self-testing in software, running in processor spare-time, a high degree of error detection and correction can be achieved. Implementation languages were also diversed to PASCAL, PL/M and IFTRAN (Structured Fortran) in order to eliminate some programming and compiler common mode errors. Software validation used automated testing tools, like RXVP80, which could do both static and dynamic analysis of the programs.

It was mentioned that system validation is going to be done by running the system in "open-loop", parallel with a hardwired licenced system.

The third paper, presented by E.Miller, Software Research Asc., addressed the "State-of-the-art in validation and verification technology". This presentation was first highlighting typical faults and problems associated with software systems. It was pointed out that the accumulated number of software problems, not only depends on the total number of executable code lines, but also how program structuring (modularization) was made.

By code inspection 80 % of the errors are normally detected in each pass. Automatic methods can also be applied, both in a static and

dynamic environment.

In the discussion, J. Taylor, RISO, presented a method for fault tree and cause consequence analysis for software validation. He pointed out the increasing need for automatic systems, aiding the system designer and presented a CAD-package, developed for mini-computers at RISO, which has been successfully applied to both nuclear and other safety-related systems.

The conclusion from this session was that there now exists a number of development tools and that system engineers more and more uses a full life-cycle and diversity approach in system engineering. Among the more promising concepts also path-domain testing techniques was suggested. Also the use of adaptive alarms was mentioned. However, there still exists a number of areas which require more research, like formal time-handling verification in RT-systems, the structure problem in system requirements and in "how people make errors".

SESSION 6 - HARDWARE AND SOFTWARE MAINTENANCE

Two papers were presented in this session. The first paper "Dynamic error detection for fault isolation and data integrity", was presented by D. Bossen, IBM. In the processor IBM 3081, a new concept for transient fault detection is applied. The main idea is to check every logical function performed, on bit-level, to isolate a fault or malfunction to a specific Field Repairable Unit (FRU). By this method both a high data integrity and a transparent recovery from intermittent failures are achieved. By grouping different failures into a FRU-base and applying symptom checking and pattern classification one may isolate a failure to a specific FRU, on a probabalistic basis. By using different maintenance strategies (e.g. best economy) optimization could be done.

It was pointed out that only 20 - 30 % hardware overhead was needed to cover more than 90 % of the errors.

In the second paper, J.M. Rata, Electricitee' de France, presented the strategies for "Hardware and software maintenance at EDF". The need for a general policy is obvious. By introduction of computers in all new power plants and replacing all old hardware with processor systems, EDF have to face the problem of maintenance of in total

14 000 processors, spread to more than 15 plants. One problem mentioned, was how to handle diversity also in maintenance, so common mode failures not was introduced in diversed systems. EDF normally work with the supervisory control functions, using a special high-level language and CAD-system support, which produce flow-sheets, documentation, code-checks etc.

In the discussion of this session, the redundant technology was pointed out as a recent advance being applied. Also, remote diagnostics and the reduction of electro-mechanical parts was mentioned as an advance.

Among the more promising concepts for the future, AI expert system for configuration, diagnosis, fault detection and detection of design failures was pointed out. Another concept mentioned, was to understress the computers and the use of simulation techniques also for maintenace.

CONCLUSIONS

The workshop highlighted a number of very important issues, connected to computer control and safety. System design, hardware software, MMI, verification, validation and maintenance were coverd in the same conference. That gave a good over all picture of 'the state of the art' in these technologies. However, it was pointed out that all the topics addressed by this workshop also are covered by other IFAC workshops and conferences, addressing each specific area.

The next workshop in this serie, SAFECOMP83, will be held at Cambridge, England, during 20 - 22 sept 1983. Call for papers is appended.

AGENDA

SAFECOMP '82

INTERNATIONAL PURDUE WORKSHOP

ON SAFETY AND RELIABILITY OF

INDUSTRIAL COMPUTER SYSTEMS

Purdue University
West Lafayette, Indiana 47907

October 11-14, 1982

Monday, October 11, 1982

AM
09:00 - 09:05 Introduction & Discussion on the Workshop Program

First Session

09:05 - 10:35 Specification Language Issues

Chairman: Professor Daniel Teichroew
Department of Industrial Engineering
University of Michigan

Paper: "Specification Transformations in the Program Development"

Author: Yoshihiro Matsumoto
Shuichi Yamamoto
Tatsuji Tanaka
Isao Sugiyai

Affiliation: Toshiba Corporation

Paper: "Specification Languages & Computer Aided Development Support Techniques to Achieve Reliable and Safe Systems: Present Status and Future Directions"

Author: Professor Rudolf Lauber
Institute for Control Engineering & Process Automation
University of Stuttgart

10:35 - 10:50 Coffee Break

10:50 - 11:30	Panelist Discussion

Panelists:

1) M. G. Dahll
Institute for Energiteknikk
OECD Halden Reactor Project
Halden Norway

2) Professor C. U. Ramamoorthy
Department of Computer Science & Engineering
University of California

3) Dr. Sandro Bologna
CNEN CSN - Casaccia
Italian Nuclear Energy Commission
Rome, Italy

Coordinator: Dr. Sabina Saab
Director of Software Quality Department
General Research Corporation

11:30 - 12:10	Group Discussion
12:10 - 01:30	Lunch

Second Session

PM
01:30 - 03:00 Man-Machine Interface Issues

Chairman: Professor William Rouse
Center for Man-Machine Systems Research
Georgia Institute of Technology

Paper: "Four Views of the Human Process Interface"

Author: Richard S. Shirley
The Foxboro Company

Paper: "Man-Machine Interface Considerationns for CRT (Safety Parameter Display Systems Used in Nuclear Power Plants)"

Author: Dr. Linda Lund
Lund Consulting Inc.
Michigan

Panelists: 1) Dr. John O'Brien
EPRI
Palo Alto, California

2) Dr. David Woods
Westinghouse R & D
Pittsburgh, PA

Coordinator: Leo Beltracchi
Human Factors Engineering
Nuclear Regulatory Commission

03:00 - 03:15 Coffee Break

03:15 - 04:00 Panel Discussion

04:00 - 04:45 Group Discussion

Tuesday, October 12, 1982

Third Session

AM
08:30 - 10:00 Operating Systems Issues

Chairman: Dr. James Schoeffler
Chairman & Professor of the Department of Computers and Science Information
Cleveland State University

Paper: "The Contribution of Operating Systems to Safe and Highly Available Systems"

Author: Dr. Th. Lalive d'Epinay
Brown-Boveri Corporation

Paper: "Reliability & Safety Considerations in Operating Systems for Process Control"

Author: Mr. Paul Greim
Foxboro Company

Paper: "A Technique for Reaching Agreement in Triplicated Systems"

Author: R. L. Anderson
Vice President, Product Development
August Systems Inc.

Panelists:
1) Dr. Charles Rose
Department of Computer Engineering
Case Western Reserve, Cleveland

2) Dr. John Baylis
Central Electricity Research Lab
Leatherhead Surrey, England

3) Mr. W. F. Floyd
Exxon Chemicals Americas
Baytown, Texas

Coordinator: Lee Shaw
Manager of Software Engineering
Westinghouse Corporation, Pittsburgh

10:00 - 10:15 Coffee Break

10:15 - 11:00 Panelist Discussion

11:00 - 11:45 Group Discussion

11:45 - 01:30 Lunch

Fourth Session

PM
01:30 - 03:00 Hardware/Software Redundancy

Chairman: Dr. Daniel Siewiorek
Professor of Computer Science
Carnegie-Mellon University, Pittsburgh

Paper: "Fault Handling in the August Systems Series 300"

Author: J. H. Wensley, President
August Systems, Inc.
Salem, Oregon

Paper: "Alternative Designs for Fault Tolerant Systems"

Author: William E. Foster, President
Stratus Computer, Inc.

Paper: "Use of Redundancy for Reliable Design and Realization"

Author: Jack Goldberg, Director
Computer Science Laboratory
SRI International

Panelists:

1) Dr. S. B. Wright
Material Physics Division
Atomic Energy Research
Harwell, England

2) Bernard Zempolich
Deputy Technology Administration
Naval Air Systems Command Headquarters

3) To Be Announced

Coordinator: Dr. Zary Segall
Carnegie-Mellon University

03:00 - 03:15 Coffee Break

03:15 - 04:00 Panelist Discussion

04:00 - 04:45 Group Discussion

06:30 p.m. Leave for Dinner
Morris Bryant Restaurant

Wednesday, October 13, 1982

Fifth Session

AM
08:30 - 10:00 Verification & Validation

Chairman: Dr. Herbert Hecht
President SoHaR Corporation, California

Paper: "Experiences in Validation and Verification in Nuclear Applications"

Authors: N. C. Thomas and E. A. Thomas

Paper: "The State of the Art in Validation and Verification Technology"

Authors: E. F. Miller, Jr. and S. L. Gerhart

Panelists:

1) Mack Alford
TRW, Huntsville

2) Dr. Martha Branstad
National Bureau of Standards

3) Dr. J. R. Taylor
RISO National Laboratory
Denmark

4) Dipl. Math. U. Voges
Kernforschungszentrum
Karlsruhe, Germany

Coordinator: Leo Beltracchi
Nuclear Regulatory Commission
Washington, D. C.

10:00 - 10:15 Coffee Break

10:15 - 11:00 Panel Discussion

11:00 - 11:45 Group Discussion

11:45 - 01:30 Lunch

Sixth Session

PM
01:30 - 03:00 Hardware Software Maintenance Issues

Chairman: John Shebell
Group Manager - Reliability and Maintenance Program
Digital Equipment Corporation

Paper: "Dynamic Error detection for Fault Isolation and Data Integrity"

Author: Dr. Douglas C. Bossen
Senior Engineer
IBM Corporation
Poughkeepsie, NY

Paper: "Hardware/Software Maintenance"

Authors: Mr. Jean-Marie Rata
Electricite de France IMA
Paris, France

Mr. Leopold Remus
Merlin-Gerin
Grenoble, France

Panelists:

1) Mr. Richard Lang
Systems Engineer
DEC - RAM Program

2) Dr. S. B. Wright
Material Physics Division
Atomic Research
Harwell, England

3) Dr. Robertson
Manager, Customer Services Operation
Foxboro Corporation

Coordinator: Roy W. Yunker
Manager, Process Control
PPG Industries, Inc.

03:00 - 03:15 Coffee Break

03:15 - 04:00 Panelist Discussion

04:00 - 04:45 Group Discussion

Thursday, October 14, 1982

Final Session

AM 08:30 - 11:45	Recommendations on Issues from the Previous Six Sessions
	Chairman: Dr. Alex Long
	Group Participation
11:45	Dr. Baylis - Plans for SafeComp III

R. W. Yunker
Chairman - SafeComp '82

RWY/dml

INTERNATIONAL PROGRAMME COMMITTEE
Dr. J.A. Baylis (U.K.) (Chairman)
Dr. T. Anderson (U.K.)
Mr. P.A. Bennett (U.K.)
Dr. S. Bologna (Italy)
Mr. D.R. Bristol (USA)
Mr. G. Dahll (Norway)
Mr. B.K. Daniels (U.K.)
Dr. W. Ehrenberger (Germany)
Dr. H. Frey (Switzerland)
Dr. R. Genser (Austria)
Mr. E. Johnson (U.K.)
Mr. J.M. Rata (France)
Mr. H. Ryland (U.K.)
Dr. B.J. Sterner (Sweden)
Mr. U. Voges (Germany)
Mr. R.W. Yunker (USA)

SECRETARIAT
Computing and Control Division
The Institution of Electrical Engineers
Savoy Place
London WC2R 0BL
U.K.

Telephone: 01-240-1871 Ext. 260
Telex: 261176

IEE

IFAC

Call For Papers

SAFECOMP '83

Third International Workshop on Achieving Computer Safe Real Time Systems

Venue: Queens College Cambridge, England

Date: 20-22 September 1983

Hayley conflict with IFAC

SAFECOMP '83

Sponsored by the International Federation of Automatic Control (IFAC), and organised by the Institution of Electrical Engineers for the United Kingdom Automatic Control Council, in association with the International Federation for Information Processing (IFIP), the European Workshop on Industrial Computer Systems, the British Computer Society and the National Centre of Systems Reliability, U.K.

AIM

The safe operation of computer systems, in both their software and hardware, continues to be a key issue in many real time applications. These applications include the monitoring and control of high energy processes, of public transportation systems, and of communication and information systems. Over recent years much has been learnt concerning the achievement of reliable on-line computer systems, in software engineering, in hardware and in management techniques. The aim of the workshop is to report and discuss the most recent advances and will be of interest to experts working in the above fields. The workshop is the third in this series sponsored by IFAC.

SCOPE

Contributions which fall within the aim of the workshop are welcome. Recommended topics are:-

* System integrity objectives and surveillance
* System reliability assessment
* Operating systems and system architecture
* Methods for the development of specifications
* Software quality assurance and fault avoidance
* Software verification and validation
* Hardware/software redundancy and fault tolerance
* Reliability of services/peripherals
* Human factors
* Standards and documentation
* Achieved reliability/safety — case studies
* Guarantees of reliability and manufacturer's liability.

Contributions on other topics relevant to the aims of the workshop will be considered.

CONTRIBUTIONS

Those wishing to offer contributions for the workshop are invited to submit a synopsis of approximately one page by:

30th November 1982

The results of pre-selection by the International Programme Committee will be communicated to authors by:

31st January 1983

Full papers (in English only) must be typed on special sheets provided. On notification of pre-selection, papers will be required in reproducible form by:

31st May 1983

Full papers should not be more than 4000 words of text, or less if illustrations or tables are included. All accepted papers will appear in the preprints of the workshop, prepared by the IFAC publisher.

WORKING LANGUAGE

The working language of the workshop is English and simultaneous translation facilities will not be available.

REGISTRATION

Registration forms and further programme details will be made available a few months before the event and will be sent to those who complete and return the attached reply form. Early registration is recommended.

To: Miss R. da Gama
Computing and Control Division
IEE
Savoy Place
London WC2R 0BL
UK

Telephone: 01-240-1871 Ext. 260
Telex: 261176

I wish to offer a contribution provisionally entitled:

. . . . . .

. . . . . .

Please send me . . . . . copies of the programme and registration form when these are available.

Name : . . . . . .

Address: . . . . . .

. . . . . .

. . . . . .

Telephone: . . . . . Telex: . . . . . .