Preface

This year we celebrated another anniversary: after 20 years of SAFECOMP in 1999, this was the 20th SAFECOMP since its inauguration in 1979. This series of events focuses on critical computer applications. It is intended to be a platform for knowledge transfer between academia, industry, and research institutions. Papers are solicited on all aspects of computer systems in which safety, reliability, and security (applied to safety in terms of integrity and availability) are of importance.

The 20th SAFECOMP tried to cover new grounds, both thematically and geographically. The previous 19 SAFECOMPs were held in Austria (1989, 1996), France (1987, 1999), Germany (1979, 1988, 1998), Great Britain (1983, 1986, 1990, 1997), Italy (1985, 1995), Norway (1991), Poland (1993), Switzerland (1992), The Netherlands (2000), and in the USA (1981, 1992), whereas the 20th was held in Hungary.

Authors from 13 countries responded to the Call for Papers, and 10 countries were represented in the final program. The proceedings include 20 papers plus 3 invited papers, covering the areas Reliability Assessment and Security, Safety Case and Safety Analysis, Testing, Formal Methods, Control Systems, and this year covering new grounds with a special emphasis on Human-Machine Interface, Components off the Shelf, and Medical Systems.

As Program Chair of SAFECOMP 2001 I would like to thank all the authors who answered our Call for Papers, the selected ones for providing their papers in time for the proceedings and presenting them at the conference, the members of the International Program Committee for the review work and guidance in preparing the program, the General Chair and the Organizing Committee for all the visible and invisible work while preparing the conference, the sponsors and the co-sponsors for their financial and non-material support, and also all those unnamed who helped with their effort and support to make SAFECOMP 2001 a fruitful event and a success.

I hope that all those who attended the conference gained additional insight and increased their knowledge, and that those reading this collection of articles after the event will be motivated to take part in the next SAFECOMP in Catania, Italy, in 2002.

July 2001 Udo Voges

Information Age and Safety Critical Systems

István Erényi

Prime Minister’s Office, Office of Government Commissionar on IT, Budapest, Hungary
Erenyii@ikb.meh.hu

Introductory Remarks from the Organizing Committee

Scientists and software and computer engineers are coming to the event of SAFECOMP 2001, the *20th Conference on Computer Safety, Reliability, and Security* to be held in Budapest this year.

Issues and problems that are related to the safety, reliability, and security of computers, communication systems, components of the networked world have never been so much at the center of attention of system developers and users as today. The emerging world of the *eEconomy* is becoming more and more dependent on the availability of reliable data and information, control commands, and computing capacity that are used everywhere: in academia, research institutes, industry, services, businesses as well as the everyday activity of people. Huge material values, correct operation of critical systems, health and life of people may depend on the availability and validity of data, correctness of control information, fidelity of the results of processing, as well as on the safe delivery of these data to the recipients.

It is not enough to tackle problems of individual computers or communication equipment alone. The complex web of networks connected and interrelated, the huge number of active processing entities that receive and produce data to this *“world-wide-web”* make the task of ensuring safe and secure operation far more complex than in isolated, stand alone systems or smaller local networks of computers. Moreover, considerations on the technological aspects of security are no longer sufficient. We have to work out effective methods as to how to investigate the behavior of the huge interconnected world of computers and communication systems together with their users and operators with very different tasks, work traditions, skills, and educational backgrounds.

This leads us to the question of not only c*omputer safety, reliability, and security,* but the safety, reliability, and security of the accumulated and transferred k*nowledge*, i.e. knowledge management: knowledge acquisition, storage, transfer, processing, understanding, and evaluation.

When we use the term *knowledge*, we consider not only technical systems, but people, and their creativity and ability to use the data and information provided by technical means, computers, and networks. We agree with the statement of T.H. Davenport and L. Prusak, according to which *knowledge is originated from working brains*, not technical systems.

More and more countries and governments announce plans and strategies toward the establishment of an information society, *e*Economy, etc, on all continents. One may notice that some of the most crucial points in these programs or strategies are *trust, safety, confidence, and reliability* of data.

Computers, informatics, data, and knowledge processing reshape our future, change the way we live, work, communicate with each other and spend our vacation. The future, and our success or failure, depend very much on the extent to which we can include, and attract as many people as possible (hopefully everybody) into the world offered by the Internet revolution, the world of the information society. Users are very much aware of the safety of the systems upon wich their activity or their work depends. Hence their involvement is also very much dependent on their trust of and confidence in this new environment.

The conference attracts specialists working toward creating safe environment.

The Organizing Committee, the community of informatics and “knowledge” specialists hosting the conference express their gratitude to all those – organizers, invited speakers, presenters and participants – who have worked for this event, sharing the results of their research and thus making the conference a fruitful meeting.

Committees

International Program Committee

Stuart Anderson	GB	
Helmut Bezecny	DE	
Robin Bloomfield	GB	
Andrea Bondavalli	IT	
Helmut Breitwieser	DE	
Peter Daniel	GB	
Bas de Mol	NL	
István Erényi	HU	
Robert Garnier	FR	
Robert Genser	AT	
Chris Goring	GB	
Janusz Gorski	PL	
Erwin Großpietsch	DE	
Maritta Heisel	DE	
Chris Johnson	GB	
Mohamed Kaaniche	FR	
Karama Kanoun	FR	
Floor Koornneef	NL	
Vic Maggioli	US	
Odd Nordland	NO	
Alberto Pasquini	IT	
Gerd Rabe	DE	(EWICS Chair)
Felix Redmill	GB	
Francesca Saglietti	DE	
Erwin Schoitsch	AT	(General Chair)
Ian Smith	GB	
Meine van der Meulen	NL	
Udo Voges	DE	(IPC Chair)
Marc Wilikens	IT	
Rune Winther	NO	
Stefan Wittmann	DE	
Janus Zalewski	US	
Zdislaw Zurakowski	PL	

Organizing Committee

István Erényi	HU	(Local Chair)
Emese Kövér	HU	
Erwin Schoitsch	AT	
Mária Tóth	HU	

External Reviewers

Marc Mersiol	FR
Thomas Ringler	DE
Mark A. Sujan	DE
Helene Waeselynck	FR

List of Contributors

Jean Arlat
LAAS-CNRS
7, Avenue du Colonel Roche
31077 Toulouse Cedex 4
France
arlat@laas.fr

Cláudia Betous-Almeida
LAAS-CNRS
7, Avenue du Colonel Roche
31077 Toulouse Cedex 4
France
almeida@laas.fr

Friedemann Bitsch
Institute of Industrial Automation and Software Engineering
University of Stuttgart
Pfaffenwaldring 47
70550 Stuttgart
Germany
bitsch@ias.uni-stuttgart.de

Andrea Bondavalli
Univ. of Firenze
Dip. Sistemi e Informatica
V. Lombroso 6/17
I-50134 Firenze
Italy
andrea.bondavalli@cnuce.cnr.it

Thierry Boyer
Technicatome
BP 34000
13791 Aix-en-Provence Cedex 3
France
tboyer@tecatom.fr

Thomas Bürger
Institut für Steuerungstechnik der Werkzeugmaschinen und Fertigungseinrichtungen
Universität Stuttgart
Seidenstr. 36
70174 Stuttgart
Germany

Roy B. Carter
NNC Ltd.
Booths Hall
Chelford Road
Knutsford, Cheshire WA16 8QZ
UK

Paul Caspi
VERIMAG
2, rue de Vignate
F-38610 Gières
France
caspi@imag.fr

Amine Chohra
IEI/CNR
Via Moruzzi 1
I-56100 Pisa
Italy
chohra@iei.pi.cnr.it

Tadeusz Cichocki
Adtranz Zwus
Modelarska 12
40-142 Katowice
Poland,
tadeusz.cichocki@pl.transport.bombardier.com

Felicita Di Giandomenico
IEI/CNR
Via Moruzzi 1
I-56100 Pisa
Italy
digiandomenico@iei.pi.cnr.it

Dacfey Dzung
ABB Corporate Research Ltd.
CH-5405 Baden-Dättwil
Switzerland
dacfey.dzung@ch.abb.com

Rainer Faller
exida.com L.L.C
Wildenholzener Strasse 26
81671 München
Germany
Rainer.Faller@exida.com

Hans R. Fankhauser
Bombardier Transportation, Propulsion & Controls Division
SE-72173 VÄSTERÅS
Sweden
hans.r.fankhauser@se.transport.bombardier.com

John Fox
Advanced Computation Laboratory
Imperial Cancer Research Fund
Lincoln's Inn Fields
London WC2A 3PX
UK
jf@acl.icnet.uk

Julio Gallardo
Safety Systems Research Centre
Department of Computer Science University of Bristol
Merchant Venturers Building
Woodland Road
Bristol BS8 1UB
UK

Piotr Gawkowski
Institute of Computer Science
Warsaw University of Technology
ul. Nowowiejska 15/19
Warsaw 00-665
Poland
gawkowsk@ii.pw.edu.pl

Manfred Gingerl
ARCS
A-2444 Seibersdorf
Austria
manfred.gingerl@arcs.ac.at

Janusz Górski
Technical University of Gdańsk
Narutowicza 11/12
80-952 Gdańsk
Poland
jango@pg.gda.pl

Bjørn Axel Gran
OECD Halden Reactor Project
P.O.Box 173
N-1751 Halden
Norway
bjorn.axel.gran@hrp.no

Atte Helminen
VTT Automation
P.O.Box 1301
FIN-02044 VTT
Finland
atte.helminen@vtt.fi

Georg Hoever
Siemens AG
Corporate Technology, CT PP 2
Simulation and Risk Management
81730 München
Germany
Georg.Hoever@mchp.siemens.de

Gordon Hughes
Safety Systems Research Centre
Department of Computer Science University of Bristol
Merchant Venturers Building
Woodland Road
Bristol BS8 1UB
UK

Andrew D. John
NNC Ltd.
Booths Hall
Chelford Road
Knutsford, Cheshire WA16 8QZ
UK
Andrew.John@nnc.co.uk

Ole-Arnt Johnsen
MoreCom
Norway
oaj@morecom.no

Mohamed Kaâniche
LAAS-CNRS
7, Avenue du Colonel Roche
31077 Toulouse Cedex 4
France
kaaniche@laas.fr

Karama Kanoun
LAAS-CNRS
7, Avenue du Colonel Roche
31077 Toulouse Cedex 4
France
kanoun@laas.fr

Silke Kuball
Safety Systems Research Centre
Department of Computer Science University of Bristol
Merchant Venturers Building
Woodland Road, Bristol BS8 1UB
UK
Silke.Kuball@bristol.ac.uk

Ulrich Laible
Institut für Steuerungstechnik der Werkzeugmaschinen und Fertigungseinrichtungen
Universität Stuttgart
Seidenstr. 36
70174 Stuttgart
Germany
ulrich.laible@isw.uni-stuttgart.de

Yannick Le Guédart
LAAS-CNRS
7, Avenue du Colonel Roche
31077 Toulouse Cedex 4
France

Oliver Mäckel
Siemens AG
Corporate Technology, CT PP 2
Simulation and Risk Management
81730 München
Germany
Oliver.Maeckel@mchp.siemens.de

István Majzik
Dept. of Measurement and
Information Systems
Budapest University of Technology and Economics
Műegyetem rkp. 9
H-1521 Budapest
Hungary
majzik@mit.bme.hu

John H. R. May
Safety Systems Research Centre
Department of Computer Science
University of Bristol
Merchant Venturers Building
Woodland Road
Bristol BS8 1UB
UK

Christine Mazuet
Schneider Electric
Usine M3
F-38050 Grenoble Cedex 9
France
christine_mazuet@mail.schneider.fr

Martin Naedele
ABB Corporate Research Ltd.
CH-5405 Baden-Dättwil
Switzerland
martin.naedele@ch.abb.com

Odd Nordland
SINTEF Telecom and Informatics
Systems Engineering and Telematics
NO-7465 Trondheim
Norway
Odd.Nordland@informatics.sintef.no

Zsigmond Pap
Dept. of Measurement and Information Systems
Budapest University of Technology and Economics
Műegyetem rkp. 9
H-1521 Budapest
Hungary
papzs@mit.bme.hu

Alberto Pasquini
ENEA
Via Anguillarese 301
00060 Roma
Italy
pasquini@casaccia.enea.it

András Pataricza
Dept. of Measurement and Information Systems
Budapest University of Technology and Economics
Műegyetem rkp. 9
H-1521 Budapest
Hungary
pataric@mit.bme.hu

Stefano Porcarelli
Univ. of Pisa
Computer Engineering Dep.
Via Diotisalvi 2
I-56126 Pisa
Italy
stefano.porcarelli@guest.cnuce.cnr.it

Günter Pritschow
Institut für Steuerungstechnik der Werkzeugmaschinen und Fertigungseinrichtungen
Universität Stuttgart
Seidenstr. 36
70174 Stuttgart
Germany

Felix Redmill
22 Onslow Gardens
London N10 3JU
UK
Felix.Redmill@ncl.ac.uk

Christian Reumann
ARCS
A-2444 Seibersdorf
Austria
christian.reumann@arcs.ac.at

Natacha Reynaud Paligot
Schneider Electric
Usine M3
F-38050 Grenoble Cedex 9
France
natacha_reynaud-paligot@mail.schneider.fr

Antonio Rizzo
University of Siena
Via dei Termini 6
53100 Siena
Italy
rizzo@unisi.it

John Rushby
Computer Science Laboratory
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025
USA
rushby@csl.sri.com

Luca Save
University of Siena
Via dei Termini 6
53100 Siena
Italy
save@media.unisi.it

Gerald Sonneck
ARCS
A-2444 Seibersdorf
Austria
gerald.sonneck@arcs.ac.at

Janusz Sosnowski
Institute of Computer Science
Warsaw University of Technology
ul. Nowowiejska 15/19
Warsaw 00-665
Poland
jss@ii.pw.edu.pl

Michael Stanimirov
ABB Corporate Research Ltd.
CH-5405 Baden-Dättwil
Switzerland
michael.stanimirov@ch.abb.com

Ioannis Vakalis
EC-Joint Research Centre
Institute for Systems, Informatics &
Safety
TP 210
21020 Ispra (Va)
Italy
ioannis.vakalis@jrc.it

Rune Winther
Faculty of Computer Sciences
Østfold University College
Os Allé 11
N-1757 Halden
Norway
rune.winther@hiof.no

Günther Zoffmann
ARCS
A-2444 Seibersdorf
Austria
guenther.zoffmann@arcs.ac.at