

SAFECOMP'99

18th International Conference on Computer Safety, Reliability and Security

Toulouse
France

September 27-29, 1999

P
R
O
G
R
A
M
M
E

<http://www.laas.fr/safecomp>



European
Network of
Clubs for
REliability and
Safety of
Software

SAFECOMP'99

the 18th International Conference on Computer Safety, Reliability and Security
Toulouse, France, September 27-29, 1999

About the Conference

SAFECOMP is an annual event reviewing the state of the art, experiences and new trends in the areas of computer safety, reliability and security.

SAFECOMP was initiated by EWICS (European Workshop on Industrial Computer Systems) in 1979 and since then has been held in Germany (Stuttgart, Fulda, Heidelberg), USA (Washington, Lafayette, Anaheim), UK (Cambridge, Manchester, Gatwick, York), France (Sarlat), Italy (Como, Belgirate), Austria (Vienna), Switzerland (Zürich), Norway (Trondheim) and Poland (Poznan).

The conference focuses on critical computer applications. It is intended to be a platform for technology transfer between academia, industry and research institutions.

Papers are presented on all aspects of computer systems in which safety, reliability and security are important. Industrial sectors include, but are not restricted to medical devices, avionics, space industry, railway and road transportation, process industry, automotive industry, power plants and nuclear power plants. Contributions come from research in industrial applications and experiences and licensing.

Conference site

LAAS-CNRS

Complexe scientifique de Rangueil

7, avenue du Colonel Roche

31077 Toulouse Cedex 4 - France

Phone: +(33) 5 61 33 62 00 - Fax: +(33) 5 61 55 35 77

<http://www.laas.fr>

Toulouse

Toulouse is situated in south-west France, 680 km from Paris. Toulouse is the Capital of the "Midi-Pyrénées" Region, the largest French province. With a population of 650000, Toulouse is pink and green: old pink bricks and green gardens with lots of pretty fountains and even barges going through the "Canal du Midi". Already bustling 2 000 years ago, the city boasts rare architectural and artistic heritage including in particular the Basilica Saint-Sernin (11th century), Saint-Etienne's Cathedral (12th century), the Church and Cloister of the Jacobins (13th century) and the Capitoul (18th century). Toulouse is the European Capital of aeronautics and space, and a leading center in industry, technology and research. With a wealth of educational institutions that include universities and several research laboratories covering all spheres of knowledge, Toulouse has the second largest university in France and ranks among the top university cities in Europe. The climate in Toulouse is usually temperate around the time of the Conference.

Information about Toulouse is available at: <http://www.mairie-toulouse.fr/>

Sunday, 26th September

18:00-19:00 **Registration at Grand Hôtel de l'Opéra (Place du Capitole)**

19:00 **Welcome Reception at Grand Hôtel de l'Opéra**

Monday, 27th September

08:15 **Bus departure from Place Wilson**

08:30-09:00 **Registration (LAAS-CNRS)**

09:00-09:30 **Opening Session**

Welcome of the General Chair, Programme Committee Chair and EWICS-TC7 Chair

09:30-10:30 **Invited Talk: Diversity for Dependability** — J. C. Laprie (LAAS-CNRS, F)

10:30-11:00 **Coffee break**

11:00-12:30 **Session 1: Assessment and Certification** (Chair: U. Voges, Institut für Angewandte Informatik, D)

- **A Systematic Approach to Safety Case Maintenance** — T. Kelly, J. McDermid (University of York, UK)
- **SQUALE Dependability Assessment Criteria** — Y. Deswarte, M. Kaënich (LAAS-CNRS, F), P. Corneillie (CR2A-DI, F), J. Goodson (Admiral, UK)
- **Assessment of Safety-Critical Digital Architectures, the ACRuDAProject** — G. Sonneck, E. Schoitsch (ARCS, A)

12:30-13:00 **Poster Session PSI: Safety Assessment and Human Factors** (Chair: U. Voges, Institut für Angewandte Informatik, D)

- **Safety Evaluation of a Train Leader Telephone System** — G. Dahll (Institute for Energy Technology, NO)
- **Validating Formal Verification using Safety Analysis Techniques** — R. deLemos, A. Saeed (University of Newcastle upon Tyne, UK)
- **Evaluating the Contribution of Desktop VR for Safety-Critical Applications** — C. Johnson (University of Glasgow, UK)
- **Human Performance Reliability in the Design-for-Usability Life Cycle for Safety Human-Computer Interfaces** — L.V.L. Filgueiras, L. Gualberto (Escola Politécnica da Universidade de São Paulo, BR)
- **The Impact of Different Media on Safety and Usability of Interactive ATC Applications** — F. Paternò, C. Santoro, (CNUCE – CNR, I), S. Tahmassebi (CENA, F)

13:00-14:30 **Lunch**

14:30-16:00 **Session 2: Human Factors** (Chair: A. Rizzo, University of Siena, I)

- **Patterns for Safer Human-Computer Interfaces** — A. Hussey (University of Queensland, AU)
- **Impact of Communications on Systems Dependability - Human Factor Perspectives** — L. Rognin (University of Limerick, IRL), J.P. Blanquart (LIS, F)
- **A Method for Operator Error Detection based on Plan Recognition** — J. Mo, Y. Crouzet (LIS / LAAS-CNRS, F)

16:00-16:30 **Coffee break and Exhibition of Posters PS1**

16:30-17:30 **Session 3: Safety Assessment** (Chair: J. Trienekens, University of Technology Eindhoven, NL)

- **Hierarchically Performed Hazard Origin and Propagation Studies** — Y. Papadopoulos, J. A. McDermid (University of York, UK)
- **Hardware Redundant Vital Computers - Demonstration of Safety on the Basis of Current Standards** — H. Krebs (TÜV Rheinland, D), S. Mitra (Lloyds Register of Shipping, UK)

18:00 **Mayor Reception**

Tuesday, 28th September

08:15 **Bus Departure from Place Wilson**

09:00-10:00 **Invited Talk: Software Reliability Engineering in Industrial Contexts** — J.D.Musa (Software Reliability Engineering and Testing Courses, USA)

10:00-10:30 **Poster Session PS2: Design for Safety** (Chair: E. Schoitsch, ARCS, A)

- **System and Software Safety Analysis for the ERAControl Computer** — P.G. Berthuisen, W. Kruidhof (Fokker Space B. V., NL)
- **Safety Markup Language: Concept and Application** — C. F. Fan (Yuan-Ze University, TW), S. Yih (Inst. of Nuclear Energy Research, TW)
- **Extendable Ground-to-Air Communication Architecture for CoDySa** — A. Pakstas (University of Sunderland, UK), I. Shagaev (Inst. for Control Sciences, RU)
- **Hierarchical Reliability and Safety Models of Fault Tolerant Distributed Industrial Control Systems** — J.C. Campelo, P. Yuste, F. Rodríguez, P. Gil, J.J. Serrano (Technical University of Valencia, E)
- **The Development of a Commercial “Shrink-Wrapped Application” to IEC61508 Safety Integrity Level 2: the DUST-EXPERT Story** — T. Clement, I. Cottam, P. Froome, C. Jones (Adelard, UK)

10:30-11:00 **Coffee break and Exhibition of Posters PS2**

11:00-13:00 **Session 4: Verification and Testing** (Chair: T. Skramstad, Det norske Veritas, NO)

- **Safety Verification of ADA95 Programs Using Software Fault Trees** — S.Y. Min, Y.K. Jang, S.D. Cha, Y.R. Kwon, D.H. Bae (Korea Advanced Institute of Science and Technology, KR)
- **Programming Rule Static Verification for Reliable Software** — P. Robert (ISOscope, F)
- **Automated Black-Box Testing with Abstract VDM Oracles** — B.K. Aichernig (Technische Universität Graz, A)
- **Towards Statistical Control of an Industrial Test Process** — G. Lombardi, E.Peciola (Ericsson, I), R. Mirandola (Università “Tor Vergata”, I), A. Bertolino, E.Marchetti (IEI – CNR, I)

13:00-14:30 **Lunch**

14:30-16:00 **Session 5: Design for Safety** (Chair: A. Costes, LAAS-CNRS, F)

- **Choosing Effective Methods for Diversity-how to Progress from Intuition to Science** — P. Popov (City University, London, UK), A. Romanovsky (University of Newcastle upon Tyne, UK), L. Strigini (City University, London, UK)
- **A First Step Towards the Integration of Accident Reports and Constructive Design Documents** — C. Johnson (University of Glasgow, UK)
- **A Holistic Design Concept to Improve Safety Related Control Systems** — M. Wimmer (University of Siena, I), M.A. Sujana (University of Karlsruhe, D), A. Rizzo (University of Siena, I)

16:00-16:30 **Coffee break**

16:30-18:00 **Session 6: Dependability Analysis and Evaluation** (Chair: R. Genser, Technical University of Vienna, A)

- **Comparing Fault Trees and Bayesian Networks for Dependability Analysis** — A. Bobbio, L. Portinale (Università del Piemonte Orientale “A. Avogadro”, I), M. Minichino, E. Ciancamerla (ENEA, I)
- **FlexFi: a Flexible Fault Injection Environment for Microprocessor-Based Systems** — A. Benso, M. Rebaudengo, M. Sonza Reorda (Politecnico di Torino, I)
- **Structural Software Reliability Estimation** — S. Kuball, J. May, G. Hughes (University of Bristol, UK)

19:30 **Visit of Toulouse Space Museum “Cit  de l’Espace” and Banquet**

Wednesday, 29th September

- 08:15** **Bus Departure from Place Wilson**
- 09:00-10:00** **Invited Talk: Standards for Airborne Systems Safety - A Consistent and Integrated Approach** — J. M. Nogue (Aerospatiale Airbus, F)
- 10:00-10:30** **Poster Session PS3: Formal Methods and Security** (Chair: S. Wittman, BA für Sicherheit in der Informationstechnik, D)
- **Hazard Analysis in Formal Specification** — K. Sere, E. Troubitsyna (Turku Centre for Computer Science, FIN)
 - **Modeling Safety-Critical Systems with Z and Petri Nets** — M. Heiner (Brandenburgische Technische Universität Cottbus, D), M. Heisel (Otto-von-Guericke-Universität Magdeburg, D)
 - **On Formal Languages for Sequences of Authorization Transformations** — Y. Bai, V. Varadharajan (University of Western Sydney Nepean, AU)
 - **Scheduling Fault-Tolerant Programs on Multiple Processors to Maximize Schedule Reliability** — I. Czarnowski, P. Jedrzejowicz, E. Ratajczak (Gdynia Maritime Academy, PL)
- 10:30-11:00** **Coffee break and Exhibition of Posters PS3**
- 11:00-13:00** **Session 7: Formal Methods** (Chair: R. Bloomfield, Adelard, UK)
- **Formal Design of Distributed Control Systems with Lustre** — P. Caspi (VERIMAG, F), C. Mazuet (Schneider Electric, F), Rym Salem (VERIMAG, F), Daniel Weber (Schneider Electric, F)
 - **Formal Specification and Development of a Safety-Critical Train Management System** — A. Chiappini (Ansaldo Segnalamento Ferroviario, I), A. Cimatti (IRST, I), C. Porzia, G. Rotondo (Ansaldo Segnalamento Ferroviario, I), R. Sebastiani, P. Traverso, A. Villaflorita (IRST, I)
 - **Formal Validation of the GUARDS Inter-Consistency Mechanism** — C. Bernardeschi (Università di Pisa, I), A. Fantechi (Università di Firenze, I), S. Gnesi (IEI - CNR, I)
 - **A Graphical Environment for the Specification and Verification of Reactive Systems** — A.K. Bhattacharjee, S.D. Dhodapkar (Bhabha Atomic Research Centre, IN), S. Seshia, R.K. Shyamasundar (School of Technology and Computer Science, IN)
- 13:00-14:30** **Lunch**
- 14:30-16:00** **Session 8: Security** (Chair: P. Daniel, GEC Marconi Secure Systems Ltd., UK)
- **Dependability Requirements and Security Architectures for the Healthcare/Medical Sector** — G. Trouessin (CESSI/CNAMTS, F)
 - **Three-Pass Hybrid Key Establishment Protocol based on ESIGN Signature** — S. M. Lee, T. Y. Kim (Korea University, KR)
 - **Integration of Safety and Security Requirements** — D. Eames (RAF, UK), J. Moffett (University of York, UK)
- 16:00-16:30** **Closing Session**
Safecomp'99 Review
Presentation of Safecomp 2000

Registration

All persons attending the conference will be required to register. As the conference facilities are limited, registrations will be served in a first-come, first served basis. Please register by returning the enclosed Registration Form. Registration can also be made by Fax or e-mail. In this case, it will be valid only after the payment has arrived.

Registration Forms are to be sent to:

Mme Sylvie Barrouquère

ADERMIP, 3, Avenue Didier Daurat - 31400 Toulouse, France

Phone: +(33) 5 62 47 49 89 — Fax: +(33) 5 61 80 81 75

e-mail: barrouqu@cict.fr

Registration Fees

Speaker	Before May 31	
	2100 FF	
	Before August 27	After August 27
EWICS-TC7 Member	2600 FF	3100 FF
Non-Member	3100 FF	3600 FF
Student*	2100 FF	2600 FF

* Students must attach a proof of student status to their Registration Forms.

Registration fees cover admission to the conference, conference proceedings, coffee breaks, lunches, welcome receptions, visit to "Cité de l'Espace" and the Banquet.

Information and Registration Desk

An information and registration desk will be available at:

- Grand Hôtel de l'Opéra, Sunday September 26, from 18:00 and during the reception
- LAAS, during the conference, from 8:30.

Payment

Payments are accepted in French Francs:

- By credit card (CB, Visa, Eurocard or Mastercard)
- By Bank Draft or check payable to ADERMIP, bank account 12719500200 at BANQUE COURTOIS, Toulouse Rémusat, branch reference agence 10268, bank identification 0250 key 49
- For French organizations only, by purchase order payable to ADERMIP.

Please mention "SAFECOMP'99", your name and Address on the Bank Draft, or purchase order.

Cancellation

Refunds of 50% will be made if a written request is received before August 27, 1999. No refunds will be made for cancellations received after this date.

Social Events

- **September 26:** Welcome Reception at Grand Hôtel de l'Opéra (Place du Capitole)
- **September 27:** Mayor Reception
- **September 28:** Visit of Toulouse Space Museum "Cité de l'Espace" and Banquet.

Information about "Cité de l'Espace" can be found at <http://www.cite-espace.com>

Transportation

• Access to Toulouse

Toulouse is about 1 hour from Paris by air, 5 hours by rail (TGV via Bordeaux) and 7 hours by freeway. There are about 40 flights daily between Toulouse and Paris. There are also daily flights between Toulouse and Lyon, Marseille, Nice, Strasbourg, Amsterdam, Brussels, Geneva, London, Madrid, Milan, Munich.

A public bus, which departs every 20 minutes, is available between the airport and the city center (Fare: about 25 FF.).

Taxi fare is around 130 FF to City center, 180 FF to LAAS.

• From downtown to LAAS-CNRS

By bus: A free special bus between downtown and the Conference Site will be organized. This bus will depart from "Place Wilson", in front of "Cinema Gaumont" at 8:15 and will return to downtown at the end of the Conference day.

By car: LAAS-CNRS is about 20 minutes car ride away from downtown.

Information about how to get to LAAS-CNRS is available on the internet at:

<http://www.laas.fr/images/plan.gif>

Accommodation

A list of hotels offering special prices is available at:

<http://www.laas.fr/Actualites/hotels.html>

Downtown hotels are situated close to "Place Wilson", "Place Jeanne d'Arc" or "Place du Capitole". Choosing a hotel in the city will give you easy access to the wide range of activities the city offers.

For your reservation, please contact DIRECTLY the hotel of your choice mentioning LAAS, and confirm your reservation by fax.

Language

The language of the Conference is English (no simultaneous translation).

Proceedings

SAFECOMP'99 proceedings are published by Springer Verlag in the Lecture Notes in Computer Science (<http://www.springer.de/comp/lncs/index.html>) and distributed during the conference.

Extended versions of the best papers accepted for the Conference will be published in a Special Section of the Journal "Reliability Engineering and System Safety" (an international journal published by Elsevier and devoted to the development and application of methods for the enhancement of the safety and reliability of complex technological systems).

Tourist Information

Information about Toulouse can be found at: <http://www.mairie-toulouse.fr/>

For additional information, please contact:

Office du Tourisme, Donjon du Capitole, 31000 Toulouse

Phone: +(33) 5 61 11 02 22 — Fax: +(33) 5 61 22 03 63

General Chair: Karama Kanoun, LAAS-CNRS, F

Programme Committee Chair: Alberto Pasquini, ENEA, I

EWICS-TC7 Chair: Gerd Rabe, TÜV Nord, D

Programme Committee

S. Anderson	UK	P. Daniel	UK	M. Van der Meulen	NL
O. Andersen	DK	W. Ehrenberger	D	J. Rainer	A
A. Bertolino	I	R. Genser	A	F. Redmill	UK
H. Bezecny	D	J. Gorski	PL	F. Saglietti	D
P. Bishop	UK	D. Inverso	USA	E. Schoitsch	A
R. Bloomfield	UK	J. Järvi	FIN	I. Smith	UK
S. Bologna	I	M. Kaâniche	F	T. Skramstad	NO
F. Cara	F	F. Koornneef	NL	J. Trienekens	NL
Y. Crouzet	F	V. Maggioli	USA	U. Voges	D
F. Dafelmair	D	C. Mazet	F	S. Wittmann	D
G. Dahll	N	C. Mazuet	F	A.J. Zalewski	USA

Organizing Committee

Alain Costes, F	Massimo Felici, I	Mohamed Kaâniche, F
Yves Crouzet, F	Marie-Thérèse Ippolito, F	Karama Kanoun, F

Contact

For the organizational aspects of the conference, please contact:

Marie-Thérèse Ippolito

LAAS-CNRS - 7, Avenue du Colonel Roche

31077 Toulouse Cedex-4 — France

Phone: +(33) 5 61 33 62 74 — Fax: +(33) 5 61 55 35 77

e-mail: louis@laas.fr

Information about SAFECOMP'99 is available at: <http://www.laas.fr/safecomp>

Sponsors and Co-sponsors

The European Workshop on Industrial Computer Systems (EWICS-TC7)

LAAS-CNRS

ENCRESS

IFIP WG 5.4 and WG 10.4

ENEA

IFAC

Austrian Computer Society (OCG)

Institut National Polytechnique de Toulouse

Université Paul Sabatier, Toulouse

Related event

FM'99: World Congress on Formal Methods, 20-24 September 1999, Toulouse, France

<http://www.cert.fr/fm99>. Contact: Dines Bjorner (e-mail: db@it.dtu.dk)