<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Room 2004</th>
<th>Room 2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00-12:30</td>
<td>Tutorial 1: Introduction to Cryptography and Authentication Protocols</td>
<td>Room 2004</td>
<td>Room 2005</td>
</tr>
<tr>
<td></td>
<td>Jonathan Moffett</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:30-14:00</td>
<td>Tutorial 2: Software Process Improvement for SMEs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ato Trân Khanh, Erwin Schoitsch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:00-17:30</td>
<td>Tutorial 3: Explaining IEC 61508</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Felix Redmill</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17:30-20:00</td>
<td>Welcome reception - Brasserie “De Tijdgeest”</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Wednesday, October 25**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Room 2004</th>
<th>Room 2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00-9:30</td>
<td>Opening session</td>
<td></td>
<td></td>
</tr>
<tr>
<td>09:30-10:30</td>
<td>Invited Paper: Tom Gilb</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00-12:30</td>
<td>Session 1: Verification and Validation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:30-13:00</td>
<td>Poster Session 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:00-16:00</td>
<td>Session 2: Software Process Improvement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:00-16:25</td>
<td>Poster Session 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17:00-18:30</td>
<td>Session 3: Formal Methods</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Thursday, October 26**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Room 2004</th>
<th>Room 2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00-10:00</td>
<td>Invited Paper: Maarten Steinbuch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00-11:00</td>
<td>Session 4: Safety Guidelines, Standards and Certification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:30-13:00</td>
<td>Session 5: Hardware Aspects</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:00-16:00</td>
<td>Panel Session: Dependability Issues in Medical Systems - Surgical Robots</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16:30-17:30</td>
<td>Session 6: Safety Assessment I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17:30-18:30</td>
<td>Session 7: Design for Safety</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20:00-24:00</td>
<td>Conference Dinner</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Friday, October 27**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Room 2004</th>
<th>Room 2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:00-10:00</td>
<td>Invited Paper: Peter Ladkin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00-11:30</td>
<td>Session 9: Transport &amp; Infrastructures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:00-13:30</td>
<td>Session 9: Safety Assessment II</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13:30-14:00</td>
<td>Closing Session</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14:30-18:00</td>
<td>Tutorial 5: Risk Management for Systems Engineering: some unconventional approaches</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tom Gilb</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SAFECOMP 2000
the 19th International Conference on Computer Safety, Reliability and Security
Rotterdam, The Netherlands, October 24-27, 2000

About the Conference
SAFECOMP was initiated by EWCSTC7 (European Workshop on Industrial Computer Systems, Technical Committee 7) in 1979 and since then has been held in Germany (Stuttgart, Fulda, Heidelberg), UK (Cambridge, Manchester, Galway, York), USA (West Lafayette, Anasahem), Italy (Como, Belgrato), France (Largat, Toulouse), Austria (Vienna), Norway (Trondheim), Switzerland (Zürich) and Poland (Poznan). The conference focuses on critical computer applications. It is intended to form a platform for technology transfer between academia, industry and research institutions.

SAFECOMP is an annual 2½ day-event reviewing the state of the art, experiences and new trends in the areas of computer safety, reliability and security regarding dependable applications of computer systems. The one-stream programme provides ample opportunity to exchange insights and experiences on emerging methods and practical applications across the borders of the disciplines represented by participants.

Conference Venue
SAFECOMP 2000 and tutorials will take place in Conference Centre Engels in the Groothandelsgebouw, Stationsplein 45, entrance A next to the Central Station, with a splendid view over the city [http://www.conventions.rotterdam.nl/map/engelsmap.html]. Phone: ++31 10 4119550, fax: ++ 31 10 4139421.

Rotterdam
Rotterdam is a modern city, full of activity. Its harbour, the largest in the world, turns it into an international centre of trade, business and culture. The city centre is famous for its daring new architecture, as well as for the historic buildings in Delfshaven and the old harbour. Together with Oporto, Rotterdam will be the cultural capital of Europe in 2001, and deservedly. The city is rich in art, its contribution to photography and film is renowned and the museum Boijmans-Van Beuningen enjoys international recognition. Theatres, cinemas and concert halls provide Rotterdam with a lively nightlife. The abundant presence of restaurants and pubs of all nationalities give Rotterdam the special global atmosphere in which everyone finds a place.

Tutorials
Leading researchers and practitioners will present half-day tutorials on the Tuesday October 24, and one on Friday afternoon, October 27, directly following the Conference. Five tutorials are offered:

Tuesday, October 24, 9:00 – 12:30 h.
Tutorial 1: Introduction to Cryptography and Authentication Protocols
Jonathan Moffett, University of York (UK)
The explosive increase in Internet traffic, and its expansion to e-commerce, has brought a whole host of security concerns and their solutions. It is hard to get the threats and protection measures into perspective. How much should you be concerned whether you have got 40-bit or 128-bit encryption? What is the difference between Symmetric and Public-Key Encryption? What is the purpose of Public Key Infrastructure?
This tutorial is an introduction to the basics of Cryptography and Authentication Protocols for those with little previous experience of the area. It will cover: fundamentals of cryptography; symmetric encryption algorithms (including DES); public-key encryption algorithms (including RSA); applications of encryption; key distribution and public-key infrastructure; authentication protocols and their problems; practical consequences for internet security.
Dr. Jonathan Moffett is a Lecturer in the Computer Science Department at the University of York, England. He was a member of the Distributed Systems Engineering group at Imperial College, London from 1986-92. His previous experience has been as a systems consultant on large commercial systems, including acting as computer controls and security adviser at Esso Europe Inc, and as consultant to one of the London Clearing Banks, for whom he wrote their computer security standards.

Tuesday, October 24, 14.00 – 17.30 h.
Tutorial 2: Software Process Improvement for Small and Medium-sized Enterprises (SMEs): experiences in the ISA-EUNET Project
Jos Trienekens, TU Eindhoven and KEMA (NL); Erwin Schoitsch, ARCS (A)
Over the last few years many SMEs have made their first steps regarding the improvement of software processes. In this tutorial the partners of the ISA-EUNET project will present recently developed approaches for SPI in SMEs and will report on relevant experiences from successful SPI projects in real-life business situations. A particular emphasis will be given to the subject of how to start measurement in SMEs to determine the effectiveness of SPI activities. The development of small and practical measurement programs on the basis of the well-known Goal Question Metric approach will be addressed. Further also methods on tutoring and mentoring SPI in SMEs will be presented.
The tutorial will be given by dr.ir. Jos Trienekens c.s. and Dipl.-Ing. Erwin Scholtsch and is based on experiences in the Isa-Eunet project. Isa-Eunet is a high-tech software EUropean lean NETwork of experts in Safety Applications to support directly SMEs at regional level. The tutors are active in the field of software process improvement regarding the development of intensive software systems for safety applications.

Tuesday October 24, 14:00 – 17:30 h.

Tutorial 3: Explaining the International Standard IEC 61508
Felix Redmill, Redmill Consultancy (UK)

The international standard, IEC 61508, addresses the functional safety of programmable safety-related systems. It is a ‘meta standard’, to be used as a basis of sector-specific standards, but where these do not yet exist, it is also intended for direct use. It defines the way in which we need to think and act towards safety throughout a system's life cycle.

IEC 61508 was influential even as a draft. Now that it is a standard, customers are demanding that suppliers conform to it. Suppliers are under pressure from their customers to deliver systems which meet the technical programme, but also legal frameworks will expect adherence to it. It is therefore of considerable importance.

This tutorial will explain what the standard is, what its objectives are, how it sets out to achieve its objectives, and how it will affect the way in which we manage safety. It will explain the technical principles on which the standard is based, and the management necessary for conformity with the standard.

The tutorial will be presented by Felix Redmill, who has run numerous courses on IEC 61508, both in-house and in public, and has been invited by many professional organisations to provide education on the standard.

Tutorial 4: Dependability and EMC
Bernard Jover (Schneider Electric, Grenoble, F)

Electromagnetic Compatibility (EMC) plays an important part in the vulnerability and dependability of electronic systems. Concomitant electromagnetic (EM) disturbances could, at the end, reduce performances of these systems. Apparatus are tested with different normative EMC immunity tests. These tests are done one after the other. In fact, EM disturbances could appear simultaneously, and the apparatus response could be completely different from the Lab test results (often lower). When electronic systems are subjected to EM disturbances, information integrity (data or signal) has to be preserved in the case of critical systems or high availability. The object of this tutorial is to introduce this concept between dependability and EMC.

The tutor, Bernard Jover, is an EMC expert at Schneider Electric company. He has extensive experience in the field of EMC and EM hardening (lightning and NEMP) for a range of clients in the process industry, transport, electricity distribution, nuclear and defence sectors. He contributes, as EMC expert, to a working group in CENELEC TC 215 dealing with electrical safety for electrotechnical aspects of telecommunications equipment inside and outside buildings.

Friday October 27, 14:30 – 18:00 h.

Tutorial 5: Risk Management for Systems Engineering: some unconventional approaches
Tom Gilb, Result Planning (N)

This tutorial will expose you to a set of risk analysis, specification and control methods which the lecturer has deep personal and practical experience with. The major topics are:
• Requirements Engineering specification: quantifying all qualities for trackability.
• System Design: the use of Impact Estimation Tables to analyse and control Risk.
• Specification Quality Control: deep early numeric QC of contracts, bids, proposals and all engineering specification, including software engineering.
• Evolutionary Project Management: early numeric rapid feedback for risk learning and control.

The tutorial will provide you a powerful, practical fresh additional set of tools for improving your ability to control not only safety issues, but also for control of risks with the concurrent quality and economic factors.

Tom Gilb is the author of 8 published books in the systems and software engineering management area, some such as his 1976 Software metrics are considered landmarks today. He works as a multinational consultant for high tech and military companies and projects. He is highly original and deep in his approach to problems of managing complex systems, and has seen his methods successfully adopted as the standard for multinationals and for professional communities.
Tuesday, October 24

09:00-17:30 Tutorials 1-4 (Conference Centre Engels)
18:00-20:00 Pre-registration in Brussel’s “De Tijdgeest”
19:30-21:00 Welcome reception in Brussel’s “De Tijdgeest” (Dress-Up) stand 1E, see map

Wednesday, October 25

09:30-09:45 Registration (Conference Centre Engels)
09:30-09:35 Opening Session
Welcome of the General Chair, TU Delft, Programme Committee Chair and EWCSC TC7 Chair

10:30-11:00 Coffee break

11:00-12:00 Session 1: Verification and Validation (Chair: F. Saggeotti, Institute for Safety Technology - ISTec, D)
• Empirical Assessment of Verification on-line Diagnostics using Fault Injection — J. Napier, J. May and G. Hughes (University of Bristol, UK)
• Speeding-up Fault Injection Campaigns in VHDL Models — B. Parrotta, M. Rehulwage, N. Sonar Ramesh and M. Violante (Politecnico di Torino, I)
• Specification and Verification of a Safety Shell with Statecharts and Extended Timed Graphs — J. van Katwijk, H. twistorf (Delft University of Technology, NL), A. Skrikosou (University of California, USA), E. Andersson and J. Zalatanis (University of Central Florida, USA)

12:30-13:30 Poster Session 1 (Chair: S. Wittmann, Bundesamt für Sicherheit in der Informationstechnik, D)
• A Constant Perturbation Method to Evaluating Structural Diversity of Multi-version Software — L. Chen, J. May and G. Hughes (University of Bristol, UK)
• Expert Error: the Case of Trouble-shooting in Electronics — B. Boudard (Université de Pau, F)
• The Safety Management of data-driven Safety-Related Systems — A.R. Faulkner, P.A. Bennett, R.H. Pierce and I.H.A. Johnson (CSE International Ltd, UK)
• Software Support for Incident Reporting Systems in Safety-Critical Applications — C. Johnson (University of Glasgow, UK)

13:30-14:30 Lunch

14:00-15:00 Session 2: Software Process Improvement (Chair: J. Trinkner, TU Eindhoven and KEMA, NL)
• Deriving Quantified Safety Requirements in Complex Systems — P.A. Lindsay, D.J. Tombs (University of Queensland, AUS), A. McDermid (University of York, UK)
• Improving Software Development by using Safe Object-Oriented Development - OTCD — S. Micah, P. Moore (AVINX, F)

16:00-16:25 Posters (Chair: F. Defoort, TU Eindhoven and BFW, NL)
• A Safety Licenseable PES for SIL 4 Applications — W.A. Halg, P. Vergeer (TU Eindhoven, NL), and M. Cohnic (University of Manitoba, C)
• Safety and Security Issues in Electric Power Industry — Z. Zarekowska (Institute of Power Systems Automation, PL)
• A Method of Analysis of Fault Trees with Time Dependencies — J. Megg, P. Ströback (Technical University of Wrocław, PL)

16:25-17:00 Coffee break

17:00-18:30 Session 3: Formal Methods (Chair: M. Heisel, University of Magdeburg, D)
• A Formal Methods Case Study: using “light-weight” VDM for the Development of a Security System Module — C. Drumond (Technical University of Comenius, SL), V. Kohl, G. Sornick and M. Thonnard (Austrian Research Centers Steiermark, A)
• Formal Methods: the Problem is Education — T. Schoener (University of Manchester Institute of Science and Technology, UK)
• Formal Methods: Diffusion; Past Lessons and Future Prospects — B. Böhmert (Adtros, UK), D. Cong (ORA, CA), F. Kuhl, M. Wittmann and S. Wittmann (Bundesamt für Sicherheit in der Informationstechnik, D)

18:00-20:00 Pre-registration in Brasserie “De Tijdgeest”
18:00-20:00 Welcome reception in Brasserie “De Tijdgeest”

Thursday, October 26

09:00-10:00 Invited Paper: Safe Tech, a Control-oriented Viewpoint — M. Ströback (TU Eindhoven, NL)
09:30-10:30 Session 4: Safety Guidelines, Standards and Certification (Chair: W. Ehrbenrohr, University for Applied Science Felda, D)
• Derivation of Safety Targets for the Random Failure of Programmable Vehicle Based Systems — R. Evans (BMW Group University of Warwick, UK) and J. Meffert (University of York, UK)
• ISO/IEC 62061: a Suitable Basis for the Certification of Safety-Critical Transport Infrastructure Systems — D. Forier (CSE International Ltd, Swinburne, Australia)

11:30-11:30 Coffee break
Safety-critical Systems Club (UK)

Another useful web site is at http://www.conventions.rotterdam.nl/venues.

NVRB (NL)

A list of hotels is available at the Tourist Information web site: http://www.vvv.rotterdam.nl/engels.

ISA-EUNET

TU Eindhoven IFAC Spits
Simtech ENCRESS KEMA
Registered QualityTU Delft ESRA
Peek Traffic Systems
Computer Systems (EWICS)
CEPIS Holland
Railconsult

Austrian Computer Society (OCG)

CMG Information Technology
Holland Railconsult
KEMA Registered Quality
Peak Traffic Systems
Splits

Accommodation

A list of hotels is available at the Tourist Information web site: http://www.vvv.rotterdam.nl/engels. Another useful web site is at http://www.conventions.rotterdam.nl/venues.

Safecomp secretariat
Minke van der Putte
Deft University of Technology
Kanaalweg 2b
2628 EB Delft, The Netherlands
Tel +31 15 278 1477
Fax +31 15 278 7105
Email: safecomp2000@tbm.tudelft.nl
Home page: http://www.wtm.tudelft.nl/vk/safecomp2000

Accommodation

A list of hotels is available at the Tourist Information web site: http://www.vvv.rotterdam.nl/engels. Another useful web site is at http://www.conventions.rotterdam.nl/venues.
The 19th International Conference on Computer
Safety, Reliability and Security
Rotterdam/The Netherlands
Tuesday 24 – Friday 27 October 2000

Registration
Surname: Initials: Ms/Mr
First name (fill in only if you wish your first name to appear on your badge)
Affiliation: (max. 35 characters/shown on badge)
Department:
Address:
Postal code:
City: Country:
Telephone: Telefax: E-mail:
Accompanying person: First name/initials:

Tutorials on Tuesday, October 24 and Friday, October 27
Registration for tutorials will be on a first come/first serve basis as the available number of seats is limited.

| Tutorial 1: Introduction to Cryptography and Authentication Protocols | NLG 650 |
| Tutorial 2: Software Process Improvement for SMEs: ISA-EUNET | NLG 250 |
| Tutorial 3: Explaining the International Standard IEC 61508 | NLG 650 |
| Tutorial 4: Dependability and EMC | NLG 650 |
| Tutorial 5: Risk Management for Systems Engineering | NLG 630 |

Those who register for more than one tutorial, receive a discount of NLG 75 per additional tutorial. +/- NLG 75 (reduction)

Conference October 25-27

<table>
<thead>
<tr>
<th></th>
<th>EWICS Member</th>
<th>Non-member</th>
<th>Speaker</th>
<th>Full-time student</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before July 31</td>
<td>-</td>
<td></td>
<td>NLG 700</td>
<td>NLG 300</td>
</tr>
<tr>
<td>After July 31</td>
<td>-</td>
<td></td>
<td>NLG 1000</td>
<td>NLG 300</td>
</tr>
<tr>
<td>Before September 25</td>
<td>NLG 800</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>After September 25</td>
<td>NLG 1000</td>
<td></td>
<td>NLG 1350</td>
<td></td>
</tr>
</tbody>
</table>

Social Programme Safecomp 2000

<table>
<thead>
<tr>
<th></th>
<th>EWICS Member</th>
<th>Non-member</th>
<th>Speaker</th>
<th>Full-time student</th>
</tr>
</thead>
<tbody>
<tr>
<td>Welcome reception, October 24</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Luncheon vouchers</td>
<td>Included</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conference Dinner, October 26</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Payment

Please choose your method of payment:

- I have instructed my bank, clearly stating my name, to pay NLG ________ to:
  ABN AMRO bank, Minervaplein, Amsterdam, The Netherlands; account number 48.85.82.768 of Safecomp 2000. Swift address: ABN ANL 2A
- Debit my credit card for the amount of NLG ____________
  Cardholders name: ____________________________
  Cardholders address (if different from the other side given address): ____________________________
  Card number: ____________________________ Expiration Date: ____________________________
  Signature: ____________________________

Please return this form to:
Parthen R&S
P.O. Box 75803
1070 AV Amsterdam
Phone: +31 20 572 73 03
Fax: +31 20 572 73 11
Email: registration@parthen.nl