

SAFECOMP 2010

29th International Conference on Computer Safety, Reliability and Security

Vienna, Austria, Schönbrunn Palace Conference Centre

Sept. 14-17, 2010

Conference Programme



Welcome to SAFECOMP 2010!

Safecomp 2010 Key Theme

Critical Embedded Systems - Challenges and Risks

Organized by



OESTERREICHISCHE
COMPUTER GESELLSCHAFT[®]
AUSTRIAN
COMPUTER SOCIETY



AIT
AUSTRIAN INSTITUTE
OF TECHNOLOGY

www.ocg.at/safecomp2010 , www.safecomp.org

The venue: City of Vienna, Schönbrunn Palace Conference Centre

Vienna, the capital of Austria, located at the Danube, often described as Europe's cultural capital, is a city of unique charm and flair. With about 2 million inhabitants in the area, it's still a metropolis, but not too large. Vienna is attractive to tourists as a romantically imperial city, with a long historical background and many sightseeing opportunities, and as a city of music, art and culture. Vienna is full of life, and according to Mercer's 2009 Quality of Living survey, it ranks now first in worldwide quality of living. It may be less well known that Vienna is a City of Science as well, with many research facilities. Vienna is a "green" city – almost surrounded by the green belt of the Vienna Woods, and with many large parks, like the Prater, Lobau, Danube Island, Schönbrunn Park, Stadtpark and so on. Vienna is easy to reach by public transport (railways, airplanes), and provides a very good hotel infrastructure.

The conference venue is the Schönbrunn Palace Conference Centre in the former Apothecaries Wing on the east side of the imperial palace, just one minute to walk from the Underground Station "Schönbrunn". Nevertheless, contemporary interior design and latest technology are provided for the conference facilities.

About SAFECOMP

Since it was established in 1979 by the European Workshop on Industrial Computer Systems, Technical Committee 7 on Reliability, Safety and Security (EWICS TC7), **SAFECOMP** has contributed to the progress of the state-of-the-art in dependable application of computers in safety-related and safety-critical systems.

SAFECOMP is an annual event covering the state-of-the-art, experience and new trends in the areas of safety, security and reliability of critical computer applications.

SAFECOMP provides ample opportunity to exchange insights and experience on emerging methods, approaches and practical solutions. It is a one-stream conference without parallel sessions, allowing easy networking.

Past SAFECOMP Conferences took place in Stuttgart (Germany, 1979), West Lafayette (USA, 1982), Cambridge (UK, 1983), Como (Italy, 1985), Sarlat (France, 1986), Manchester (UK, 1987), Fulda (Germany, 1988), Vienna (Austria, 1989), Gatwick (UK, 1990), Trondheim (Norway, 1991), Zürich (Switzerland, 1992), Poznan (Poland, 1993), Anaheim (USA, 1994), Belgirate (Italy, 1995), Vienna (Austria, 1996), York (UK, 1997), Heidelberg (Germany, 1998), Toulouse (France, 1999), Rotterdam (The Netherlands, 2000), Budapest (Hungary, 2001), Catania (Italy, 2002), Edinburgh (UK, 2003), Potsdam (Germany, 2004), Fredrikstad (Norway, 2005), Gdansk (Poland, 2006), Nuremberg (Germany, 2007), Newcastle (UK, 2008) and Hamburg (Germany, 2009).

SAFECOMP Conference Contacts:

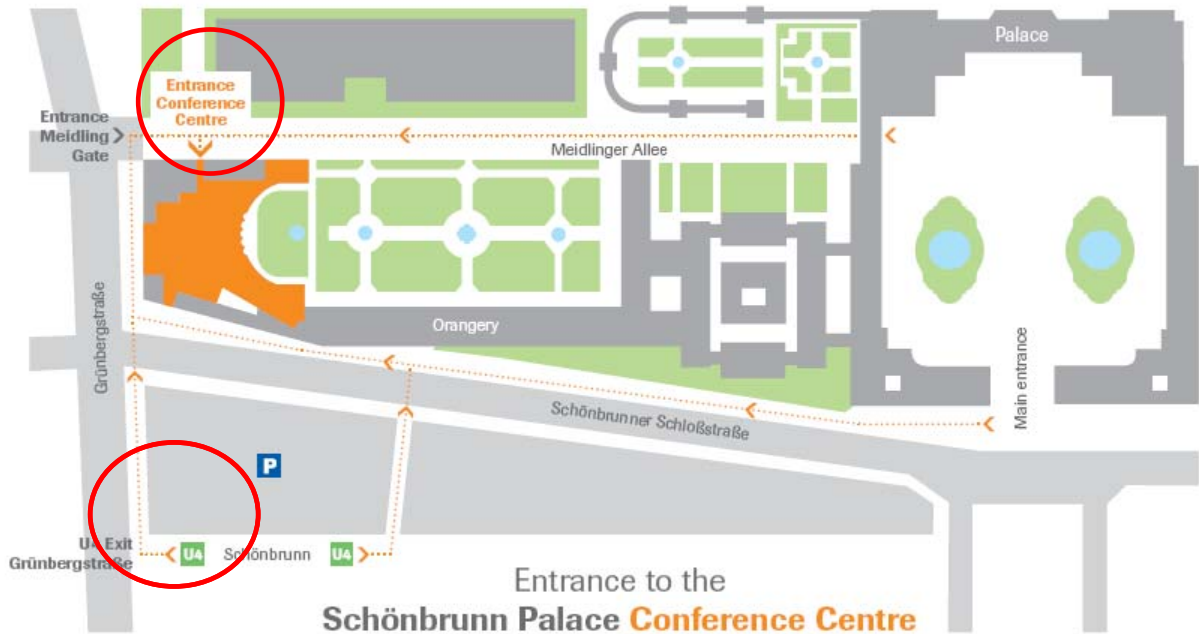
Erwin Schoitsch, AIT Austrian Institute of Technology,

erwin.schoitsch@ait.ac.at

Conference Secretariat: ocg@ocg.at

Web Site: www.ocg.at/safecomp2010 , www.safecomp.org

**Schönbrunn Palace Conference Center,
Apothecaries' Wing, nearest entrance Grünbergstraße,
Meidlinger Gate, 1130 Vienna (U4 Metro Schönbrunn)**



How to reach Schönbrunn Palace Conference Center? (marked by ○)



(Map Vienna Airport Lines):

From Airport:

Take S7 railway or CAT (fast train) to Wien-Mitte, then by Underground U4 (direction Hütteldorf) to Schönbrunn.

Or take Airport Bus to Schwedenplatz, then U4 (direction Hütteldorf) to Schönbrunn.

From Railway Westbahnhof:

Take U6 (direction Alterlaa or Siebenhirten) to Längenfeldgasse, then U4 (direction Hütteldorf) to Schönbrunn

From Railway Wien-Meidling (Südbahn):

Take U6 (direction Floridsdorf) to Längenfeldgasse, then U4 (direction Hütteldorf) to Schönbrunn.

Map of Conference Rooms



**PROCEEDINGS are published as
 SPRINGER LNCS 6351**

**They are available as part of the participant's
 conference package!**



WLAN available: SSID: SKBguest, Password: tz.schoenbrunn

Conference Program

Daily Keynotes (9:30 – 10:15)

Wednesday, 15th Sept.:

"System of Systems Challenges"

(Hermann Kopetz - Vienna University of Technology, Austria)

Thursday, 16th Sept.:

"Murphy Was An Optimist"

(Kevin Driscoll - Honeywell Laboratories, USA)

Friday, 17th Sept.:

"Process Control Security: go Dutch! (united, shared, lean and mean)"

(Eric Luijff - TNO, The Hague, The Netherlands)

SAFECOMP Programme Overview

Monday, September 13	Tuesday, September 14		Wednesday, September 15	Thursday, September 16	Friday, September 17
<i>EWICS TC 7 Meeting</i>	<i>Tutorials, Workshops</i>		<i>Conference</i>	<i>Conference</i>	<i>Conference</i>
		8:00-8:30	Registration	Registration	Registration
		8:30-9:00	Registration	Session 4	Session 8
		9:00-9:30	Welcome Addresses		
EWICS TC7	Workshops	9:30 - 10:15	Keynote 1 (invited)	Keynote 2 (invited)	Keynote 3 (invited)
Meetings		10:15-10:45	Coffee Break	Coffee Break	Coffee Break
Open for free to all	Tutorials	10:45-12:45	Session 1	Session 5	Session 9
interested in		12:45-14:00	Lunch	Lunch	Lunch
EWICS TC7 Work	EWICS TC7	14:00-16:00	Session 2	Session 6	Session 10
and Subgroups		16:00-16:30	Coffee Break	Coffee Break	Closing Session
(see www.ewics.org)		16:30-18:00	Session 3	Session 7	Coffee and Wrap Up
				Guided Tour	
		19:00		Schönbrunn Palace	
				Dinner	
		20:00	Welcome Reception	Schönbrunn Palace	
			City Hall Cellar	Gloriette	

Preconference - Monday 13th - Tuesday 14th Sept.

EWICS TC 7 Meeting

Monday, 13th Sept.: TechGate, Donau-City-Straße 1, TechGate Tower, 5th floor,
AIT-Safety & Security Department (U1 Metro station Kaisermühlen-VIC)

Tuesday, 14th Sept.: at SAFECOMP Conference Venue,
Schönbrunn Palace Conference Center,
Room 4 (Rudolf) and Room 3 (Josef II, as break-out room)

Free of charge, for details see <http://www.ewics.org>.

Workshops, Tutorials

Tuesday, 14th Sept.: Schönbrunn Palace Conference Center

Workshop 1 (9:00 – 18:00): Room 7 (Maria Antoinette)

**S&D4RCES – International Workshop on Security and Dependability for
Resource Constrained Embedded Systems**

Workshop 2 (9:00 – 17:30): Room 2 (Sisi)

**ERCIM/DECOS/MOGENTES - Dependable Embedded Systems: Model-based
Design and Validation (Automated Test Case Generation)**

R3-COP Workshop (11:00 – 17:00): Room 6 (Franz Stephan) (On invitation only)

Tutorial 1 (9:00 – 12:30): Cancelled

Integration and Complexity of Flight Systems - The Role of Data Buses

Tutorial 2 (14:00 – 17:30): Cancelled

**Goal directed Specification, Measurement and Certification of Functionality,
Integrity, Privacy, Safety and Security**

Workshop and tutorial participants are eligible for the reduced “Early Bird” registration fee even after expiration of the deadline!

Exhibition

A Technical Exhibition and Tool Fair is open during the whole conference in the communication area where coffee breaks and lunches take place

Main Conference - Wednesday 15th - Friday 17th Sept.

Wednesday, Sept. 15th (Room 1, Maria Theresia)

9:00 - 9:30 Welcome Addresses

- Lisbeth Mosnik, Austrian Federal Ministry of Transport, Innovation and Technology
- Francesca Saglietti, EWICS Chair, University of Erlangen-Nuremberg, Germany
- Gerald Futschek, Technical University of Vienna, President of the Austrian Computer Society, Austria
- Erwin Schoitsch, Conference Chair, AIT Austrian Institute of Technology, Austria

9:30 - 10:15 Keynote I

(Session chair: Erwin Schoitsch, AIT, Austria)

System of Systems Challenges

Hermann Kopetz, Vienna University of Technology, Austria

10:15 - 10:45 Coffee Break

10:45 - 12:45 Session 1: System Analysis

(Session chair: Odd Nordland, SINTEF, Norway)

Reliability Analysis of Safety-Related Communication Architectures

Oliver Schulz, Jan Peleska, University of Bremen, Germany

On the Safety Implications for e-Governance: Assessing the Hazards of Enterprise Information Architectures in Safety-Critical Applications

Christopher Johnson, Stefan Raue, University of Glasgow, Scotland, UK

Variability Management of Safety and Reliability Models: An Intermediate Model towards systematic Reuse of Component Fault Trees

Carolina Gomez, Peter Liggesmeyer, TU Kaiserslautern, Germany; Ariane Sutor, Siemens Corp. Research, Munich, Germany

QoS Analysis of Weighted Multistate Probabilistic Networks via Decision Diagrams

Roberta Terruggia, Andrea Bobbio, University Piemonte Orientale, Italy

12:45 - 14:00 Lunch

14:00 - 16:00 Session 2: Safety Cases and Certification

(Session chair: Rolf Schumacher, Consultant Safety Certification, Germany)

Comparison between IEC 60880 and IEC 61508 for Certification Purposes in the Nuclear Domain

Jussi Lahtinen, Jukka Ranta, Hannu Harju, VTT, Finland; Mika Johansson, Risto Nevalainen, Tampere University of Technology, Finland

Deriving Safety Cases for Hierarchical Structure in Model-Based Development

Nurlida Basir, Bernd Fischer, University of Southampton, UK; Ewen Denney, NASA Ames Research Center, USA

Assurance of Automotive Safety - A Safety Case Approach
Robert Palin, Jaguar Land Rover, Coventry, UK; Ibrahim Habli, Univ. of York, UK

How to "Survive" a Safety Case According to ISO 26262
Torsten Dittel, Ford, Cologne, Germany; Hans-Jörg Aryus, SystemA Engineering, Immenstaad, Germany

16:00 - 16:30 Coffee Break

16:30 - 18:00 Session 3: Aerospace

(Session chair: Peter Ladkin, Bielefeld University, Germany)

Benchmarking Software Requirements Documentation for Space Application
Paulo Veras, Rodrigo P. Pontes, Emilia Villani, Aeronautical Institute, São José dos Campos-SP, Brazil; Ana Maria Ambrosio, National Institute for Space Research, São José dos Campos-SP, Brazil; Henrique Madeira, Marco Vieira, Aeronautical University of Coimbra, Portugal

Verifying Mode Consistency for On-Board Satellite Software
Alexei Iliasov, Alexander Romanovsky, University of Newcastle, UK; Elena Troubitsyna, Linas Laibinis, Abo University, Finland; Kimmo Varpaaniemi, Pauli Väisänen, Dubravka Ilic, Timo Latvala, Space Systems Finland, Finland

Computational Concerns in the Integration of Unmanned Airborne Systems into Controlled Airspace
Christopher Johnson, University of Glasgow, Scotland, UK

20:00 Welcome Reception

City Hall, Restaurant Wiener Rathauskeller

Thursday, Sept. 16th (Room 1, Maria Theresia)

8:30 - 9:30 Session 4: Error Detection

(Session chair: Uli Siebold, Fraunhofer EMI, Germany)

Residual Error Probability of Embedded CRC by Stochastic Automata
Frank Schiller, Tina Mattes, TU Munich, Germany

ANB- and ANBDMem-Encoding: Detecting Hardware Errors in Software
Ute Schiffel, Andre Schmitt, Martin Süßkraut, Christof Fetzer, TU Dresden, Germany

9:30 - 10:15 Keynote II

(Session chair: Erwin Schoitsch, AIT, Austria)

Murphy Was An Optimist

Kevin Driscoll - Honeywell Laboratories, USA

10:15 - 10:45 Coffee Break

10:45 - 12:45 Session 5: Validation and Verification

(Session chair: Francesca Saglietti, University of Erlangen-Nuremberg, Germany)

Field Test Methods for a Co-operative Integrated Traffic Management System
Thomas Gruber, Egbert Althammer, Erwin Schoitsch, AIT Austrian Institute of Technology, Austria

100% Coverage for Safety-Critical Software - Efficient Testing by Static Analysis
Daniel Kästner, Reinhold Heckmann, Christian Ferdinand, AbsInt GmbH, Saarbrücken, Germany

MODIFI: A MODEL-Implemented Fault Injection Tool
Rickard Svenningsson, Jonny Vinter, Henrik Eriksson, SP Technical Research Inst. of Sweden, Sweden; Martin Törngren, KTH Stockholm, Sweden

Automated Test Coverage Measurement for Reactor Protection System Software Implemented in Function Block Diagram
Eunyoung Jee, Insup Lee, University of Pennsylvania, USA; Suin Kim, KAIST, Daejeon, Rep. of Korea; Sungdeok Cha, Korea University, Seoul, Rep. of Korea

12:45 - 14:00 Lunch

14:00 - 15:00 Session 6: Testing

(Session chair: Bettina Buth, HAW Hamburg, Germany)

Overcoming Non-determinism in Testing Smart Devices: a Case Study
Peter Bishop, CSR City University and Adelard, London, UK; Lukasz Cyra, Adelard, London, UK

Software Testing by People with Autism
Sjaak Brinkkemper, Suzanne Haanappel, Utrecht University, The Netherlands

15:00 - 16:00 EWICS TC7 presentation

(Session chair: Francesca Saglietti, EWICS Chair)

EWICS TC7 Subgroup Presentations

16:00 - 16:30 Coffee Break

16:30 - 18:00 Session 7: Critical Infrastructure - Smart Grid

(Session chair: Frank Ortmeier, University Magdeburg, Germany)

Information Flow Analysis of Energy Management in a Smart Grid
Ravi Akella, Bruce McMillin, Missouri University of Science and Technology, USA

Integrated Cyber-Physical Fault Injection for Reliability Analysis of the Smart Grid
Sahra Sedigh, Bruce McMillin, Ayman Faza, Missouri University of Science and Technology, USA

A Metric for Measuring the Strength of Inter-dependencies
Silvia Ruzzante, Elisa Castorini, Elena Marchei, Vincenzo Fioriti, ENEA, Roma, Italy

18:30 - 19:10 Guided Tour

The guided tour through Schoenbrunn Castle will take you through the rooms of the palace showing you the apartments of Emperor Franz Joseph and Empress Elisabeth, as well as the magnificent ceremonial rooms in the central part of the palace. Afterwards a panorama train will take you to Gloriette, the belvedere of Schoenbrunn Castle, where the conference dinner will be held.

19:30 Conference Dinner

Schoenbrunn Palace, Gloriette

Friday, Sept. 17th (Room 1, Maria Theresia)

8:30 - 9:30 Session 8: Security and Safety

(Session chair: Wolfgang Ehrenberger, University of Appl. Sciences Fulda, Germany)

Security Analysis of Open Building Automation Systems

Wolfgang Granzer, Wolfgang Kastner, Vienna University of Technology, Austria

A UML Profile for Requirements Analysis of Dependable Software

Denis Hatebur, ITESYS GmbH and University Duisburg-Essen, Germany; Maritta Heisel, University Duisburg-Essen, Germany

9:30 - 10:15 Keynote III

(Session chair: Udo Voges, KIT, Germany)

Process Control Security: go Dutch! (united, shared, lean and mean)

Eric Luijff, TNO, The Hague, The Netherlands

10:15 - 10:45 Coffee Break

10:45 - 12:45 Session 9: Safety Engineering I

(Session chair: Meine van der Meulen, DNV, Høvik, Norway)

Model-Based Safety Engineering of Interdependent Functions in Automotive Vehicles Using EAST-ADL2

Anders Sandberg, Mecel AB, Gothenburg, Sweden; Martin Törngren, DeJiu Chen KTH Stockholm, Sweden; Henrik Lönn, Lei Feng, Ramin Tavakoli-Kolagari, Volvo Technology, Gothenburg, Sweden; Rolf Johansson, Mentor Graphics, Gothenburg, Sweden; Sandra Torchiaro, CRF, Orbassano, Italy; Andreas Abele, Continental Automotive, Regensburg, Germany

Experiences in Applying Formal Verification in Robotics

Dennis Walter, Holger Täubig, Christoph Lüth, German Research Institute for AI, Bremen, Germany

Evolving a Safe System Design Iteratively

*Alexandre Mota, Adriano Gomes, Joabe Jesus, Federal University of Pernambuco, Brazil;
Edson Watanabe, Felipe Ferri, Embraer, Brazil*

An Approach to Using Non Safety-Assured Programmable Components in Modest Integrity Systems

Peter Bishop, CSR City University and Adelard, London, UK; Kostas Tourlas, Nick Chozos, Adelard, London, UK

12:45 - 14:00 Lunch

14:00 - 16:00 Session 10: Safety Engineering II

(Session chair: Maritta Heisel, University Duisburg-Essen, Germany)

Development of High-Integrity Software Product Lines Using Model Transformation

Stuart Hutchesson, John McDermid, Aero Engine Controls, Derby & University of York, UK

A Novel HAZOP Study Approach in the RAMS Analysis of a Therapeutic Robot for Disabled Children

Thomas Gruber, Petr Böhm, AIT Austrian Institute of Technology, Austria

The Right Degree of Configurability for Safety-Critical Embedded Software in Variable Message Signs

Thomas Novak, Christoph Stoegerer, SWARCO FUTURIT, Perchtoldsdorf, Austria

INDEXYS, A Logical Step Beyond GENESYS - INDustrial EXploitation of the genesYS cross-domain architecture

Andreas Eckel, Christian Fidi, TTTech, Vienna, Austria; Roman Obermaisser TU Vienna, Austria; Paul Milbredt, Audi AG, Germany; Zaid Al-Ars, Delft University of Technology, The Netherlands; Stefan Schneelee, EADS Germany GmbH, Germany; Bart Vermeulen, NXP Semiconductors Netherlands B.V., The Netherlands; György Csertan, OptXware Research and Development Ltd., Hungary; Christoph Scheerer, Thales Rail Signalling Solutions GesmbH, Austria; Neerai Suri, Abdelmajid Khelil, Technical University of Darmstadt, Germany; Gerhard Fohler, Technical University of Kaiserslautern, Germany

16:00 - 16:30 Closing Session (session chair: Erwin Schoitsch)

Announcement of SAFECOMP 2011

Best Paper Award

Closing Remarks and Farewell

16:30 - 17:00 Coffee and Wrap Up

Workshops and Tutorials - Programmes and Descriptions

Workshop 1 (full day, 9:00 – 18:00): Room 7 (Maria Antoinette)

S&D4RCES – International Workshop on Security and Dependability for Resource Constrained Embedded Systems

Contact: Brahim HAMID, IRIT- University of Toulouse, France

The main focus of S&D4RCES is on the topic of making security and dependability expert knowledge available to Resource Constrained Embedded Systems (RCES) engineering processes. Special emphasis will be devoted to promote discussion and interaction between researchers and practitioners focused on the particularly challenging task to efficiently integrate security and dependability solutions within the restricted available design space for RCES. Furthermore, one important focus is on the potential benefits of the combination of model-driven engineering with pattern-based representation of security and dependability solutions.

The workshop aims to bring together researchers from various fields involved in the development and deployment of RCES with a particular focus on the transfer of results from fundamental research to the industrial development of RCES. We believe that the synergy between researchers working in different aspects of this area will produce important benefits. The objective of this workshop is to foster an exchange of ideas among practitioners, researchers and industry involved in the deployment of secure and dependable resource-constrained embedded systems. The exchange of concepts, prototypes, research ideas, and other results which contribute to the academic arena and also benefit business and industrial communities, is of particular interest. Some of the topics that we seek to include in the workshop are related to the development of models and tools to support the inclusion of security and dependability (SD) issues into the RCES engineering process.

Thus, the workshops targets also audience from communities concentrated on security and dependability beyond the existing MODELS participants. Therefore, we will target the following research communities:

- Engineering of RCES:
 - Model-driven engineering
 - Component-based software engineering
 - Automated software engineering
 - Real-time and highly efficient embedded systems
- Security and dependability
 - SD in model-driven engineering
 - Formal methods in security
 - Security and dependability requirements specification pattern-based approaches to SD engineering

Contact:

Brahim HAMID
IRIT- University of Toulouse,
118 Route de Narbonne,
F31062 Toulouse Cedex 9,
France
phone/fax: +33 (0)5 6150 2386 / 4173
e-mail: brahim.hamid@irit.fr

S&D4RCES 2010 Workshop Program

Time	Sessions
8:30 – 9:00	Registration
9:00 – 9:15	Opening Session
9:15 – 10:15	<p><u>Session 1: research papers- Modeling</u> chair: Francesca Saglietti Enforcing Trust in Embedded Systems Using Models Christophe Jouvray, Miche SallAntonio Kung Trust in MDE Components: the DOMINO Experiment Benoît Baudry, Pierre Bazex, Jean-Charles Dalbin, Philippe Dhaussy, Hubert Dubois, Christian Percebois, Erwann Poupart, Laurent Sabatier</p>
10:15 – 10:45	Coffee Break
10:45 – 12:45	<p><u>Session 2: research papers- Formalization</u> chair: Sigrid Güergens Monitor Petri Nets for Security Monitoring Lars Patzina, Sven Patzina, Thorsten Piper, Andy Schürr Formalization of Smart Metering Requirements Andreas Fuchs, Sigrid Guergens, Donatus Weber, Christian Bodenstedt, Christoph Ruland Automated Unit and Integration Testing for Component-based Software Systems Francesca Saglietti, Florin Pinte Hierarchical Multi-Agent Protection System for NoC based MPSoCs Slobodan Lukovic, Nikolaos Christianos</p>
12:45 – 14:00	Lunch
14: 00 – 16:00	<p><u>Session 3: ongoing project and new visions</u> chair: Christian Percebois Security engineering for embedded systems -- the SecFutur vision, Sigrid Güergens, Carsten Rudolph, Antonio Mana, Simin Nadjm-Tehrani Model-Based Security and Dependability Patterns in RCES- the TERESA Approach Brahim Hamid, Nicolas Desnos, Cyril Grepet, Christophe Jouvray Towards the Integration of Advanced Engineering Paradigms into RCES: raising the issues for the Model-Driven Product-Line Case David Gonzalez, Antonio Pérez, Salvador Trujillo, Brahim Hamid Model-based management of Ubiquitous and Autonomic M2M Services architecture Khalil Drira</p>
16:00 – 16:30	Coffee Break
16:30 – 18:00	<p><u>Session 4: working and discussion</u> chairs: Brahim Hamid, Sigrid Güergens, Cyril Grepet, Salvador Trujillo, Khalil Drira</p>

Workshop 2 (full day, 9:00 – 17:30): Room 2 (Sisi)

ERCIM/DECOS/MOGENTES - Dependable Embedded Systems: Model-based Design and Validation (Automated Test Case Generation)

Workshop participation free of charge (can be attended independent from SAFECOMP)

Coffee Break and Lunch included.

Session Chairs:

Wolfgang Herzner, Erwin Schoitsch AIT Austrian Institute of Technology
Amund Skavhaug, NTNU, Trondheim

Computers are everywhere – may they be visible or integrated into every day equipment, devices, and environment, outside and inside us, mobile or fixed, smart, interconnected and communicating. Comfort, health, services, safety and security of people depend more and more on these “embedded systems”, and the impact on society as a whole is tremendous – positive and negative.

Thus dependability in a holistic manner becomes an important issue. Technology is developing very fast, and demanding challenges have to be met by research, engineering and education. Smart (embedded) systems are regarded as the most important business driver for European industry. They are a targeted research area for European Research Programmes in Framework 7 and the ARTEMIS Joint Undertaking, and in several other dedicated Programmes. Artemis (“Technology Platform for Advanced Research and Technology for Embedded Intelligence”) and EPoSS (“European Technology Platform (ETP) on Smart Systems Integration”) are the main two ETPs promoting smart embedded systems technology as their objective. Their application is not only in the traditional areas of aerospace, railways, automotive, or process industry and manufacturing, but also in services of all kind, in home appliances (smart environments, smart homes, ambient assisted living) and health care. Co-operative, distributed networked systems and resilient systems (adaptive systems maintaining dependability even in changing environments) add another dimension of functionality and complexity.

Morning session: 9:00 – 12:45

- **09:00 – 09:15** **Welcome, workshop introduction (ERCIM, EWICS)**
- **09:15 – 09:45** Remote Presence: Performing Maintenance of Offshore Wind Farms without Leaving your Office (Øyvind Netland, NTNU, Norway)
- **09:45 – 10:15** Intelligent Transport Systems on the Road: Lane sensitive navigation with NAV-CAR – goals and challenges (Egbert Althammer, Reinhard Kloibhofer, AIT, Austria)
- **10:15 – 10:45** Coffee Break
- **10:45 – 11:15** Functional Specification for a Time Management Unit (Kristoffer Gregertsen, NTNU, Norway)
- **11:15 – 11:45** ADOSE Project (Reliable Application Specific Detection of Road Users with Vehicle On-board Sensors) (Jürgen Kogler, Christoph Sulzbachner, AIT)
- **11:45 – 12:15** Exploitation of Embedded Systems Research Results via Standardization– a path towards business (Erwin Schoitsch, AIT, Austria)
- **12:15 – 12:45** Self awareness, the next concept for ubiquitous industrial sensor networks (Amund Skavhaug, NTNU, Norway)
- **12:45 – 14:00** Lunch

Afternoon Session: 14:00 – 17:30

The afternoon session is dedicated to papers on “Validation and Verification”, presenting the results of the European FP7 project **MOGENTES** (Model Based Generation of Efficient Tests for Dependable Systems, contract no. 216679), planned presentations are:

- **14:00 – 14:30** MOGENTES Overview (W. Herzner, AIT)
- **14:30 - 15:00** Modelling and Mutation Testing (UML) (R. Schlick, AIT)
- **15:00 – 15:30** Automated Test Case Generation (Harald Brandl, TU Graz)
- **15:30 – 16:00** Tool Integration (András Pataricza, Balázs Polgár, Imre Kocsis, András Kövi, Budapest University of Technology and Economics)

- **16:00 – 16:30** Coffee Break

- **16:30 – 16:30** Model based Fault Injection Tool (MIFI, MODIFI) (SP Research Institute of Sweden)
- **16:30 – 17:00** Model Checking (ETH Zurich/University of Oxford)
- **17:00 – 17:30** Plenary discussion, concluding remarks

The papers and presentation material (slides) will be published as ERCIM proceedings after the workshop.

Contacts:

Amund Skavhaug
The Norwegian University of Science and Technology
Department of Engineering Cybernetics
Skavhaug.amund@ntnu.no

Wolfgang Herzner, Erwin Schoitsch
AIT Austrian Institute of Technology,
Donau-City-Straße 1, TechGate
A-1220 Vienna, Austria
wolfgang.herzner@ait.ac.at
erwin.schoitsch@ait.ac.at

Abstracts of Key Notes

System of Systems Challenges

Hermann Kopetz
Institute for Computer Engineering
Vienna University of Technology, Austria
hk@vmars.tuwien.ac.at

Abstract. The available technology (e.g., the Internet) makes it possible to interconnect *independently developed embedded systems (legacy systems)* to form new *system-of-systems (SoS)* that promise more efficient economic processes and improved services. Examples of SoSs are *smart power distribution, car-to-car communication, or air-traffic control*. The different sub-systems of an SoS are developed according to their *unique architectural style*, are operated by *different organization* and serve their *own purposes*. The integration of the subsystems into an SoS can be static or dynamic. The *emergent properties* that come into existence by the integration of the sub-systems can be *predicted or are, at first, unforeseen*. There a number of unique challenges in the design of system of systems such as, for example: the alignment of the diverse architectural styles, the control of the emergent properties, information security, and the provision of dependable service in the face of the continuous evolution of the subsystems. This talk will elaborate on the characteristics of SoS and will focus on the mentioned research challenges that must be tackled in order to provide dependable SoS services.

Process Control Security: go Dutch! (united, shared, lean and mean)

Eric Luijff MSc
TNO Defence, Security and Safety
The Hague, The Netherlands

Abstract. International studies have shown that information security for process control systems, including SCADA, is weak. As many critical infrastructure (CI) services depend on process control systems, any vulnerability in the protection of process control systems in CI may result in serious consequences for the safety of our citizens and the security of our society, economy and ecology. Various critical sectors in The Netherlands like drinking water, energy, multinationals have identified process control security as an important theme to jointly address in the Dutch National Infrastructure against Cybercrime (NICC). A set of activities were started, such as sector-wide benchmarks, awareness raising, development of good practices, sharing of incident information, developing an acquisition standard, and red-blue team training. Mid of 2010, the Dutch Process Control Security Roadmap project took off which comprises a coordinated set of actions to raise the security barriers in the domain where information technology touches the physical world. Rather than re-inventing wheels, the Dutch approach is lean and mean trying to improve and integrate existing efforts and advancements using a united effort by for instance chief information officers, process control users, manufacturers, system integrators, EDP-auditors, education, and R&D. The results are shared with all the participants in order to reach an improved and high level of protection at the short, medium and the long time. Results are shared as well with other nations, international information exchanges and vendors aiming international acceptance and a next, shared improvement cycle.

The keynote session will highlight the approaches and show some of the results.

Murphy Was an Optimist

Kevin R. Driscoll
Honeywell International, Inc.

Abstract. Embedded, safety-critical systems often have requirements for incredibly small probabilities of failure, e.g. 10^{-9} for a one hour exposure. One often hears designers of safety-critical systems say: "We have to tolerate *all* credible faults".

However, the word "credible" in this assertion contrasts starkly with the word "incredibly" in the sentence before. In fact, there are faults and failures that most designers think can't happen which actually can and do happen with probabilities far greater than the requirements allow. The well known Murphy's Law states that: "If anything can go wrong, it will go wrong." When requirements limit failure probabilities to one-in-a-million or less, this should be re-written as: "If anything can't go wrong, it will go wrong anyway."

There are a couple of factors that lead to designers erroneously thinking that certain faults and failures are impossible; when in fact, not only are they possible, but some are actually highly probable.

One factor is that the requirements are outside any designer's experience, even when that experience includes that of colleagues. Using the literature seems like an obvious way of expanding one's (virtual) experience. However, there are two problems with this. The first problem is that people who actually design safety-critical systems are rarely given enough time to keep current with the literature. The second problem is that the literature on actual occurrences of rare failure modes is almost nonexistent. Reasons for this include: people and organizations don't want to admit they had a failure; designers feel that rare failure occurrence aren't worth reporting; and, if designers aren't given enough time to read literature, they certainly aren't given enough time to write it. Take away: Designers should fight their management for time to keep current with the literature and designers should use every report of a rare failure as an opportunity to imagine other similar modes of failure.

The other factor that leads to designers erroneously thinking that certain faults and failures are impossible stems from abstraction. The complexity of modern safety critical systems requires some form of abstraction. However, when designers limit their thinking to one level of abstraction, certain faults and failures can seem impossible, but would clearly be seen as probable if one were to examine layers below that level of abstraction. For example, a designer thinking about electrical components would not include in their FMEA the possibility that one component (e.g. a diode) could transmogrify into another component (e.g. a capacitor). But, at a lower level of abstraction, it can be seen that a crack through a diode die can create a capacitor. And, a crack is one of the most highly probable failure modes at the physical material level of obstruction.

Examples of rare but actually occurring failures will be given. These will include a number of Byzantine faults, component transmogrification, fault mode transformation (e.g. stuck at faults that aren't so stuck), the dangers of self-inflicted shrapnel, component creation via emergent properties, "evaporating" software, and exhaustively tested software that still failed.

Sponsors

City of Vienna

Federal Ministry of Transport, Innovation and Technology

Scientific Sponsors



European
Network of
Centres for
REliability and
Safety of
Software



Austrian
Association for
Research in IT

Company Sponsors/Exhibitors:

AbsInt Angewandte Informatik GmbH

Science Park 1
66123 Saarbrücken
Germany



Adelard LLP

College Building
10 Northampton Square
London
EC1V 0HB
UK



Causalis Limited

Am Petersberg 3
33619 Bielefeld
Germany



TTTech Computertechnik AG - Ensuring Reliable Networks

Schoenbrunner Strasse 7
1040 Vienna
Austria



Organization

Conference Chair

Erwin Schoitsch (AIT, Austria)

EWICS Chair

Francesca Saglietti (Univ. of Erlangen-Nuremberg, Germany)

Local Chair

Gerald Futschek (OCG, TU Vienna, Austria)

Local Organizing Committee (OCG, Austria)

Eugen Mühlvenzl

Elisabeth Waldbauer

Karin Hiebler

Christine Haas

International Programme Committee

Anderson, S. (UK)	Heitmeyer, C. (US)	Rabe, G. (DE)
Anderson, T. (UK)	Hübner, M. (DE)	Reich, S. (AT)
Ata, B. (TR)	Johnson, C. (UK)	Saglietti, F. (DE)
Bloomfield, R. (UK)	Kaâniche, M. (FR)	Schedl, G. (AT)
Bologna, S. (IT)	Kanoun, K. (FR)	Schoitsch, E. (AT)
Braband, J. (DE)	Kelly, T. (UK)	Schulze, S.-O. (DE)
Buth, B. (DE)	Knight, J.C. (US)	Seyfarth, T. (DE)
Daniel, P. (UK)	Koornneef, F. (NL)	Skavhaug, A. (NO)
Ehrenberger, W. (DE)	Kopacek, P. (AT)	Strigini, L. (UK)
Emmet, L. (UK)	Ladkin, P. (DE)	Sujan, M. (UK)
Felici, M. (UK)	Lehmann, T. (DE)	Traverse, P. (FR)
Flammini, F. (IT)	Lindskov Hansen, S. (DK)	Trienekens, J. (NL)
Genser, R. (AT)	Littlewood, B. (UK)	van der Meulen, M. (NL)
Gerstinger, A. (AT)	McDermid, J. (UK)	Weinert, A. (DE)
Gorski, J. (PL)	Nordland, O. (NO)	Wittmann, S. (BE)
Gran, B.A. (NO)	Pareigis, S. (DE)	Yüceer, R. E. (TR)
Halang, W. (DE)	Peleska, J. (DE)	Zurakowski, Z. (PL)
Heisel, M. (DE)	Pfeiffenberger, T. (AT)	
Haxthausen, A. (DK)	Pozzi, S. (IT)	

