SAFECOMP 2013
Toulouse

Program Information

24-27 September, 2013

Safecomp 2013
LAAS-CNRS
7, avenue du Colonel Roche, BP 54200, 31031 Toulouse Cedex 4, France
Tel : +33 5 61336255
email : safecomp2013@laas.fr
http://www.laas.fr/SAFECOMP2013

LAAS-CNRS

INSTITUT CARNOT LAAS CNRS

Preface

On behalf of the Technical Program Committee members of the 32nd International Conference on Computer Safety, Reliability and Security (SAFECOMP2013), it is our pleasure to welcome you to Toulouse, France.

SAFECOMP is a major event that provides a forum for researchers and practitioners from all over the world to present and discuss their latest research results and experiments on the development, assessment, operation and maintenance of safety-related and safety critical computer systems. 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 dependability of computers in safety-related and safety-critical systems. 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.

This year, we received 88 submissions from 24 countries. The review and selection process followed the tradition of thoroughness and rigor of SAFECOMP. The review process is organized in two phases, mainly relying on the PC members for the evaluation of the papers. In the first phase, each submitted paper was assigned to 3 members of the PC, which was composed of 51 researchers and industrials from 16 countries (Europe, North and South America, and Asia). At the end of this phase, a PC meeting has been held in Zürich attended by 29 PC members. The selection process has been competitive with 28% acceptance rate.

The 25 papers selected in the program include 20 regular papers, and 5 practical experience reports. This year's program has been organized into 11 sessions, covering different assessment methods (testing and verification, software reliability, failure mode analysis, safety assurance) and addressing a wide variety of interesting topics (security, error control code, dependable user interfaces). The technical program is complemented with keynote presentations from three distinguished speakers. John Rushby (SRI, USA) will give a talk on logic and epistemology in safety cases, Pascal Traverse (Airbus) will address the dependability in embedded systems considering the airbus fly-by-wire system as an example, and finally Sami Haddadin (DLR, Germany) will address safe human-robot physical interaction. Additionally, a session for fast abstracts presentation is included in the program to promote interactions on novel ideas or work in progress, or opinion pieces that can address any issue relevant to SAFECOMP topics of interest.

We would like to express our deep gratitude to the PC members who devoted their time and provided their expertise to ensure the quality of the reviewing and the shepherding processes. We are also very grateful to the external reviewers for their out-standing help and assistance in the review process. Needless to add that the elaboration of the SAFECOMP 2013 technical program would not have been possible without the greatly appreciated contribution of all the authors who have submitted their work to the conference.

The support received from the EWICS TC7 committee chaired by Francesca Sagli-etti is very much appreciated. Special thanks go to Karama Kanoun for her continuous support and feedback during organization of this edition, and to Frank Ortmeier for his help based on his experience as SAFECOMP General Chair and PC Chair in 2012. We would also like to thank Friedemann Bitsch, Matthieu Roy, Marc-Olivier Killijian, Nicolas Rivière and Pascal Traverse as publication, workshops, fast abstracts, publicity, and industry liaison chairs, respectively. Also special thanks to Christoph Schmitz, who hosted the PC Meeting in Zürich, Zühlke Engineering AG. Finally, we would like to express our gratitude to Sonia de Sousa, Yves Crouzet, members of TSF research group, the LAAS-CNRS administrative and technical staff, and the sponsors for their assistance in organizing this event.

Thank you for attending the conference. We hope that you will benefit from the conference and that you will find our efforts worthwhile. We wish you a pleasant stay in Toulouse. Enjoy!

Jérémie Guiochet
General chair & program co-chair

Mohamed Kaâniche
Program co-chair

Conference Program

Overview

	Tuesday 24 September	Wednesday 25 September	Thursday 26 September	Friday 27 September
	WORKSHOP /TUTORIAL DAY	SAFECOMP DAY 1	SAFECOMP DAY 2	SAFECOMP DAY 3
8:00-8:45	REGISTRATION	REGISTRATION	REGISTRATION	REGISTRATION
8:45-9:00		WELCOME NOTE		
9:00-10:00	Workshops: SASSUR, CARS, DECS, ASCOMs / Tutorials: FM&C and SA'SE	INVITED TALK 1 John Rushby, SRI, USA	INVITED TALK 2 Pascal Traverse, Airbus, FR	INVITED TALK 3 Sami Haddadin, DLR, DE
10:00-11:00		SESSION 1 Safety requirement and assurance	SESSION 5 Software reliability assessment	SESSION 9 Dependable user interfaces
11:00:11:30	*Coffee break*	*Coffee break*	*Coffee break*	*Coffee break*
11:30-13:00		SESSION 2 Testing and verification	SESSION 6 Practical experience reports and tools I	SESSION 10 Practical experience reports and tools II
13:00-14:00	*Lunch break*	*Lunch break*	*Lunch break*	*Lunch break*
14:00-15:00		SESSION 3 Security	SESSION 7 Safety assurance in automotive	SESSION 11 Hazard and failure mode analysis
15:00-15:30			SESSION 8 Error control codes	
15:30-16:00	*Coffee break*	EWICS presentation		Closing session / SAFECOMP 2014
16:00-16:30		Fast abstracts 60"		
		Coffee break	Bus transfer to AIRBUS	
16:30-17:00		SESSION 4 Fast Abstract Posters		
17:00-17:30			AIRBUS A380 Visit	
17:30-18:30				
18:30-19:00	WELCOME COCKTAIL at TOULOUSE CITYHALL (salle des Illustres)	GUIDED CITY TOUR	Bus transfer to Toulouse downtown	
19:00-19:30			APÉRITIF / DRINKS	
19:30-20:00		WINE TASTING		
20:00			BANQUET	

Conference Program

Wednesday 25 September 2013

Room: Salle de Conférences

8:00-8:45	REGISTRATION
8:45-9:00	WELCOME NOTE: Jean Arlat, Director of LAAS-CNRS; Jérémie Guiochet (General Chair)
9:00-10:00	INVITED TALK 1: **Logic and Epistemology in Safety Cases.** John Rushby, SRI, USA (Chair: Mohamed Kaâniche)
	SESSION 1: Safety requirements and assurance (Session chair: Tim Kelly)
10:00-10:30	**Comparative conformance cases for monitoring multiple implementations of critical requirements.** Janusz Gorski, Aleksander Jarzebowicz and Jakub Miler
10:30-11:00	**A Formal Basis for Safety Case Patterns**. Ewen Denney and Ganesh Pai
11:00-11:30	Coffee break
	SESSION 2: Testing and verification (Session chair: Francesca Saglietti)
11:30-12:00	**Testing Autonomous Robot Control Software using Procedural Content Generation.** James Arnold and Rob Alexander
12:00-12:30	**Fine-grained implementation of fault tolerance mechanisms with AOP: to what extent?** Jimmy Lauret, Jean-Charles Fabre and Hélène Waeselynck
12:30-13:00	**Formalisation of an Industrial Approach to Monitoring Critical Data.** Yuliya Prokhorova, Elena Troubitsyna, Linas Laibinis, Dubravka Ilic and Timo Latvala
13:00-14:00	Lunch break
	SESSION 3: Security (Session chair: Robert Stroud)
14:00-14:30	**Protecting Vehicles Against Unauthorised Diagnostics Sessions Using Trusted Third Parties.** Pierre Kleberger and Tomas Olovsson
14:30-15:00	**Vulnerability Analysis on Smart Cards using Fault Tree.** Guillaume Bouffard, Bhagyalekshmy N Thampi and Jean-Louis Lanet
15:00-15:30	**Does Malware Detection Improve With Diverse AntiVirus Products? An Empirical Study.** Ilir Gashi, Vladimir Stankovic, Michel Cukier and Bertrand Sobesto
15:30-16:00	EWICS presentation
	SESSION 4: Fast Abstracts 60 seconds (Session chair: Marc-Olivier Killijian)
16:00-16:30	Fast abstracts 60" talks
	Coffee break
16:30-17:30	Fast abstract posters to be announced
18:30-20:00	GUIDED CITY TOUR and WINE TASTING

Conference Program

Thursday 26 September 2013

Room: Salle de Conférences

8:00-9:00 REGISTRATION

9:00-10:00 INVITED TALK 2: **Embedded Systems Dependability (fly-by-wire).** Pascal Traverse, Airbus, FR
(Chair: Karama Kanoun

SESSION 5: Software reliability assessment (Session chair: Jean-Paul Blanquart)

10:00-10:30 **Software fault-freeness and reliability predictions.** Lorenzo Strigini and Andrey Povyakalo.

10:30-11:00 **Does Software have to be Ultra Reliable in Safety Critical Systems?** Peter Bishop.

11:00-11:30 Coffee break

SESSION 6: Practical experience reports and tools I (Session chair: Frank Ortmeier)

11:30-12:00 **The SafeCap Platform for Modelling Railway Safety and Capacity.** Alexei Iliasov, Ilya Lopatkin and Alexander Romanovsky.

12:00-12:30 **Embedded System Platform for Safety-critical Road Traffic Signal Applications.** Thomas Novak and Christoph Stoegerer

12:30-13:00 **Low-level Attacks on Avionics Embedded Systems.** Anthony Dessiatnikoff, Vincent Nicomette, Eric Alata and Yves Deswarte

13:00-14:00 Lunch break

SESSION 7: Safety assurance in automotive (Session chair: Mario Trapp)

14:00-14:30 **Safety Cases and their role in ISO 26262 Functional Safety Assessment.** Ibrahim Habli, John Birch, Helen Monkhouse, Roger Rivett, Dave Higham, John Botham, Rob Palin, Ben Bradshaw and Peter Jesty

14:30-15:00 **Structuring Safety Requirements in ISO 26262 using Contract Theory.** Jonas Westman, Mattias Nyberg and Martin Törngren

SESSION 8: Error control codes (Session chair: Phil Koopman)

15:00-15:30 **Flexible Unequal Error Control Codes with SelectableError Detection and Correction Levels.** Luis-J. Saiz-Adalid, Pedro-J. Gil-Vicente, Juan-Carlos Ruiz-García, Daniel Gil-Tomás, J.-Carlos Baraza and Joaquin Gracia-Morán.

15:30-16:00 **Safety Transformations: Sound and Complete?** Ute Schiffel

17:00-18:30 AIRBUS A380 Visit

19:00 APÉRITIF / DRINKS

20:00 BANQUET

Conference Program

Friday 27 September 2013

Room: Salle de Conférences

8:00-9:00 REGISTRATION

9:00-10:00 INVITED TALK 3: **It is (almost) all about human safety: a novel paradigm for robot design, control, and planning.** Sami Haddadin, DLR, DE (Chair: David Powell)

SESSION 9: Dependable user interfaces (Session chair: Floor Koornneef)

10:00-10:30 **Understanding functional resonance through a federation of models: preliminary findings of an avionics case study.** Célia Martinie, Philippe Palanque, Alberto Pasquini, Martina Ragosta, Mark Alexander Sujan and David Navarre.

10:30-11:00 **Model-based development of the Generic PCA infusion pump user interface within PVS.** Paolo Masci, Anaheed Ayoub, Paul Curzon, Insup Lee, Oleg Sokolsky and Harold Thimbleby.

11:00-11:30 Coffee break

SESSION 10: Practical experience reports and tools II (Session chair: Andrea Bondavalli)

11:30-12:00 **Characterization of Failure Effects on AADL Models.** Bernhard Ern, Viet Yen Nguyen and Thomas Noll

12:00-12:30 **Derived Hazard Analysis Method for Critical Infrastructures.** Thomas Gruber, Georg Neubauer, Andreas Weinfurter, Petr Böhm and Kurt Lamedschwandner

12:30-13:00 **A Study of the Impact of Single Bit-Flip and Double Bit-Flip Errors on Program Execution.** Fatemeh Ayatolahi, Behrooz Sangchoolie, Roger Johansson and Johan Karlsson

13:00-14:00 LUNCH BREAK

SESSION 11: Hazard and failure mode analysis (Session chair: Amund Skavhaug)

14:00-14:30 **OpenMADS: An Open Source Tool for Modeling and Analysis of Distributed Systems.** Ermeson Andrade, Marcelo Alves, Rubens Matos, Bruno Silva and Paulo Maciel

14:30-15:00 **A Controlled Experiment on Component Fault Trees.** Jessica Jung, Andreas Jedlitschka, Kai Hoefig, Dominik Domis and Martin Hiller.

15:00-15:30 **DFTCalc: A Tool for Efficient Fault Tree Analysis.** Florian Arnold, Freark Van der Berg, Dennis Guck, Marielle Stoelinga and Axel Belinfante

15:30-16:00 Closing session / SAFECOMP 2014

Committees

General Chair: Jérémie Guiochet (LAAS-CNRS, Univ. Toulouse, FR)

EWICS TC7 Chair: Francesca Saglietti (Univ. of Erlangen-Nuremberg, DE)

Program Co-Chairs: Mohamed Kaâniche (LAAS-CNRS, Univ. Toulouse, FR) Jérémie Guiochet (LAAS-CNRS, Univ. Toulouse, FR)

Publication Chair: Friedemann Bitsch (THALES Transportation Systems GmbH, DE)

Local Organizing Committee: Yves Crouzet (LAAS-CNRS, Univ. Toulouse, FR), Sonia De Sousa (LAAS-CNRS, Toulouse, FR)

Fast Abstract Chair: Marc-Olivier Killijian (LAAS-CNRS, Univ. Toulouse, FR)

Workshop Chair: Matthieu Roy (LAAS-CNRS, Univ. Toulouse, FR)

Publicity Chair: Nicolas Rivière (LAAS-CNRS, Univ. Toulouse, FR)

Industry Liaison Chair: Pascal Traverse (EADS-Airbus, Toulouse, FR)

International Program Committee

Anderson, Stuart (U. Edinburgh, UK)
Bieber, Pierre (ONERA, FR)
Bitsch, Friedemann (THALES Transportation Systems, DE)
Blanquart, Jean-Paul (Astrium, FR)
Bloomfield, Robin (Adelard, UK)
Bologna, Sandro (AIIC, IT)
Bondavalli, Andrea (U. Florence, IT)
Braband, Jens (Siemens AG, DE)
Casimiro, Antonio (U. Lisbon, PT)
Cotroneo, Domenico (Federico II U. Naples, IT)
Cukier, Michel (U. Maryland, US)
Daniel, Peter (EWICS - TC7, UK)
Denney, Ewen W. (SGT / NASA, US)
Ehrenberger, Wolfgang (Hochschule Fulda, DE)
Felici, Massimo (HP Labs, UK)
Flammini, Francesco (Ansaldo STS, IT)
Gorski, Janusz (U. Gdansk, PL)
Grunske, Lars (U. Stuttgart, DE)
Guiochet, Jérémie (LAAS-CNRS, U. Toulouse, FR)
Halang, Wolfgang (Fernuniversitaet in Hagen, DE)
Heisel, Maritta (U. Duisburg-Essen, DE)
Johnson, Chris (U. Glasgow, UK)
Jonsson, Erland (U. Chalmers, SE)
Kaâniche, Mohamed (LAAS-CNRS, U. Toulouse, FR)
Kanoun, Karama (LAAS-CNRS, U. Toulouse, FR)
Karlsson, Johan (U. Chalmers, SE)
Kelly, Tim (U. York, UK)
Knight, John (U. Virginia, US)
Koopman, Phil (Carnegie Mellon University, US)
Koornneef, Floor (Tech U. Delft, NL)
Lindskov Hansen, Soren (Novo Nordisk A/S,DK)
Moraes, Regina (U. Campinas, BR)
Motet, Gilles (Foundation for an Industrial Safety Culture, FR)
Nanya, Takashi (Canon, JP)
Nordland, Odd (Sintef, NO)
Ortmeir, Frank (U. Magdeburg, DE)
Palanque, Philippe (IRIT, U. Toulouse, FR)
Paulitsch, Michael (EADS IW, DE)
Romano, Luigi (U. Naples Parthenope, IT)
Romanovsky, Alexander (U. Newcastle, UK)
Rugina, Ana (ESA, NL)
Saglietti, Francesca (U. of Erlangen-Nuremberg, DE)
Schmitz, Christoph (Zühlke Engineering AG, CH)
Schoitsch, Erwin (AIT Austrian Institute of Technology GmbH, AT)
Skavhaug, Amund (NTNU, NO)
Steininger, Andreas (TU Vienna, AT)
Sujan, Mark (Warwick medical school, UK)
Trapp, Mario (Fraunhofer IESE, DE)
Troubitsyna, Elena (U. Abo Akademi, FIN)
Van der Meulen, Meine (DNV, NO)
Weaselynck, Hélène (LAAS-CNRS, U. Toulouse, FR)

Conference Invited talk

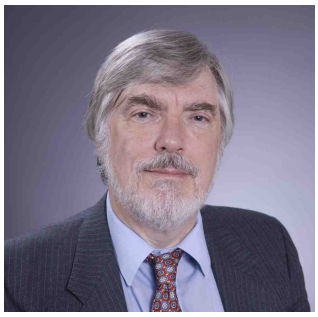
INVITED TALK 1

Wednesday 25 September 2013, 9:00 - 10:00

John Rushby, Program director, SRI Intern. Computer Science Laboratory, USA

http://www.csl.sri.com/users/rushby/

Logic and Epistemology in Safety Cases



Abstract: A safety case must resolve concerns of two different kinds: how complete and accurate is our knowledge about aspects of the system (e.g., its requirements, environment, implementation, hazards) and how accurate is our reasoning about the design of the system, given our knowledge. The first of these is a form of epistemology and requires human experience and insight, but the second can, in principle, be reduced to logic and then checked and automated using the technology of formal methods. We propose that reducing epistemic doubt is the main challenge in safety cases, and discuss ways in which this might be achieved.

Biography : Dr. John Rushby is a Program Director and SRI Fellow with the Computer Science Laboratory of SRI International in Menlo Park California, where he leads its research program in formal methods and dependable systems. He joined SRI in 1983 and served as director of its Computer Science Laboratory from 1986 to 1990. Prior to that, he held academic positions at the Universities of Manchester and Newcastle upon Tyne in England. He received BSc and PhD degrees in computing science from the University of Newcastle upon Tyne in 1971 and 1977, respectively. His research interests center on the use of formal methods for problems in the design and assurance of safe, secure, and dependable systems. John Rushby received the IEEE Harlan D Mills Award in 2011 "for practical and fundamental contributions to Software & Hardware Reliability with seminal contributions to computer security, fault tolerance, and formal methods" and, together with Sam Owre and N. Shankar, the CAV Award in 2012 "for developing PVS (Prototype Verification System) which, due to its early emphasis on integrated decision procedures and user friendliness, significantly accelerated the application of proof assistants to real-world verification problems."

INVITED TALK 2

Thursday 26 September 2013, 9:00 - 10:00

Pascal Traverse, Airbus Cockpit & flight ops. R&T Program leader, France

Embedded Systems Dependability (fly-by-wire)

Abstract: Safety is the priority in aviation. The reason is obvious: people's lives are at stake and this is ingrained in the industry (operators and manufacturers, regulation agencies).Instead of a wide description of the systems safety process, which is generally known and well documented, we will rather focus on a few important points, not always part of conventional wisdom. We intend to show that safety process is fully embedded in design, that the ubiquitous and magic number of 10-9 is only a tiny part of the solution, the multiple dimensions of the issue and the overall resilience of the process. This will be supported by examples taken from Airbus Fly-by-Wire system, typical of critical embedded systems and encompassing multiple dependability features. Architecture is highly fault-tolerant while fault prevention and removal is always in focus.

Biography: Pascal Traverse doctorate was on dependable computing and was directed by the late Jean-Claude Laprie and by Jean Arlat in LAAS. He graduated before as an engineer from ENSEEIHT and after visited UCLA to work with Al Avizienis. He entered AIRBUS in 1985 and had the opportunity to participate to the design of the flight-by-wire system of the A320, the first time such a system was on a civil airplane. He then went on with the subsequent Airbus fly-by-wire developments, then leading the overall Airbus systems safety activities. Two of his patents are flying and some bits of Aviation Safety regulation are his authoring. He then focused on resilience: his own by working three years in the A380 Final Assembly Line and then Airbus Engineering' as he moved this organisation closer to manufacturing concerns. He recently took the lead of Airbus research on cockpit and flight operations. With colleagues of "CISEC" (critical embedded system society of Aerospace Valley), he recently set-up a seminar on embedded critical systems.

INVITED TALK 3

Friday 27 September 2013, 9:00 - 10:00

Sami Haddadin, Dr.-Ing. DLR, Germany
http://www.robotic.de/Sami.Haddadin

It is (almost) all about human safety: a novel paradigm for robot design, control, and planning

Abstract: Enabling robots for direct physical interaction and cooperation with humans and transferring the resulting technology to industrial and domestic real world applications is the primary goal of my research. For this, we developed new generations of impedance controlled lightweight robots (LWRs) at DLR, which are sought to act safely as human assistants in a variety of application domains such as industrial assembly and manufacturing, medical assistance, or house-hold helpers in everyone's home. The last generation of the lightweight robot was recently commercialized as the KUKA LBR iiwa, which is considered as the first representative of a new class of robots: the so-called "soft-robots". In the aforementioned applications, which aim for human environments, the primary objective is to ensure that a robot's action does not cause human injury, even in case of malfunction or user errors.

Acting and reacting safely to unforeseen events in real-time on basically all levels of abstraction is crucial in both control and planning domain. For this, a robot needs to know in particular what injury it may cause due to its actions. In order to equip a robot with such knowledge, a systematic approach for human injury analysis and prevention had to be developed that bridges the gap between robotics and injury biomechanics. For quantifying what safe behavior really means the definition of injury, as well as understanding its general dynamics is essential. We approached the problem from a medical injury analysis and biomechanical point of view such that the relation between robot mass, velocity, impact geometry and resulting injury in medical terms can be found. Due to the achieved generality of our results, this methodology has also found its way into current international standardization effort.

Algorithmically, so called "biomechanically safe velocity" and high-speed collision detection, tightly entangled with appropriate reflex reaction build the robot's real-time "safety core". The "biomechanically safe velocity" algorithm ensures truly safe robot velocities by evaluating in real-time the potential injury risk emanating from the robot's inertial and surface properties and shaping its velocity such that accidental collisions with the human body remain subcritical. Collision detection and cascaded reflex reaction schemes let the robot then react safely after a collision was sensed. Thus, subsequent potentially hazardous situations are avoided if possible and overall, entire injury prevention even in case of unforeseen collisions becomes possible. This control core builds a reliable foundation for novel real-time motion planning and collision avoidance schemes that bridge the gap between planning and control, while also exploiting the aforementioned injury knowledge in order to generate "human-safe" trajectories.

The consecutive encapsulation of all real-time algorithms into an (action-behavior) based "control core" builds then a powerful basis for human-friendly task planning, as the large variety of new features become part of a safety-oriented programming model. In this context, I will also report on our recent results in dynamic programming paradigms and provably optimal, safety-oriented planning algorithms that finally make it possible to bring novel robot control algorithms, human safety, and human-friendly task planning into alignment.

Overall, I will argue in my talk that the described human-safety oriented design, control, and planning paradigm contributes significantly to solving some fundamental problems of nowadays robotics and let "soft-robots" become a commodity in our near-future society. I will also illustrate the relevance of the field and the according technology with selected real-world implementations of our concepts such as advanced manufacturing solutions at automobile companies. Their aim is to achieve flexible production lines that involve human-robot co-working and are free of safety cages.

Biography: Sami Haddadin holds a Dipl.-Ing. degree in EE, a M.Sc. in CS from Technical University of Munich (TUM), and holds an Honours degree in Technology Management from TUM and the Ludwig Maximilian University Munich (LMU). He obtained his PhD with summa cum laude from RWTH Aachen. At the Robotics and Mechatronics Center of the German Aerospace Center (DLR) he acts as Scientific Coordinator "Human-Centered Robotics". He is a lecturer of various robotics courses at TUM. In 2011 he was a visiting scholar at Willow Garage and Stanford University. His main research topics are physical Human-Robot Interaction, nonlinear robot control, real-time motion planning, real-time task and reflex planning, robot learning, optimal control, variable impedance actuation, brain controlled assistive robots, and safety in robotics. He was in the program/organization committee of several international robotics conferences and a guest editor of International Journal of Robotics Research. He published more than 75 papers in international journals, books, and conferences. Among other things, he received five best paper and video awards at ICRA/IROS, the 2008 Literati Best Paper Award, the euRobotics Technology Transfer Award 2011, the 2012 George Giralt Award, the 2012 IEEE Transactions on Robotics King-Sun Fu Memorial Best Paper Award. Furthermore, he was a finalist of the 2009 Robotdalen Scientific Award, IROS 2010 Best Application Paper Award, and 2012 SfN BCI Award.

Fast Abstracts Program & Posters

25th September 2013 16:00-17:30

1. Fault-Tolerant Real-Time Scheduling Algorithm for Energy-Aware Embedded Systems
   C. Arar, H. Kalla, S. Kalla and B. S. Sabrina

2. Common Cause Failure Analysis for Wireless Sensor Networks
   I. Silva and L. A. Guedes, P. Portugal and F. Vasques

3. An Approach for Security Evaluation and Analysis in Cloud Computing
   T. Probst, E. Alata, M. Kaâniche, V. Nicomette, Y. Deswarte

4. Specifying Safety Monitors for Autonomous Systems
   M. Machin, J.-P. Blanquart, J. Guiochet, D. Powell and H. Waeselynck

5. Multimedia Systems as Immune System to Improve Automotive Security?
   J. Dittmann, T. Hoppe, C. Vielhauer

6. Assure-It: A Runtime Synchronization Tool of Assurance Cases
   S. Shida, A. Uchida, M. Ishii, M. Ide, and K. Kuramitsu

7. Integrating agile practices into critical software development
   K. Łukasiewicz, J. Górski

8. Outsourced Linear Algebra
   A. Kumar

9. Security-informed Safety
   R. Bloomfield and R. Stroud

10. Adequacy of Contract Grammars for Component Certification
    A. Ruiz, H. Espinoza, T. Kelly

11. Communication Integrity for Slow-dynamic Critical Embedded Systems
    A. Zammali, A. de Bonneval, Y. Crouzet

12. Robust by «Let it Crash»
    C. Woskowski, M. Trzeciecki, F. Schwedes

14. Impact of Feature Interaction on the Safety Analysis for Unmanned Avionics Product Lines
    A. L. de Oliveira, R. T. V. Braga, P. C. Masiero, I. Habli, T. Kelly

15. A Study on the Reliability Improvement Factor of Fault Tolerant Mechanisms
    J. Na, D. Lee

Workshop Program

ASCoMS — Workshop on Architecting Safety in Collaborative Mobile Systems

Room: Salle Tourmalet

9:00-9:30	**Automatic Optimisation of System Architectures using EAST-ADL.** Chen, Lönn, Mraidha, Papadopoulos, Parker, Reiser, Servat, Silva Azevedo, Tucci-Piergiovanni, Walker
9:30-10:00	**Safety Kernel for Cooperative Sensor-Based Systems.** Nóbrega Da Costa, Craveiro, Casimiro, Rufino
10:00-10:30	**Run time safety analysis for automotive systems in an open and adaptive environment.** Östberg, Bengtsson
10:30-11:00	**Content Based Routing with Directional Random Walk for Failure Tolerance and Detection in Cooperative Large Scale Wireless Networks.** Leone, Muñoz
	Coffee break
11:30-12:00	**Revisiting Gossip-style Failure Detection in Wireless Sensor Network.** Pitrey, Sailhan
12:00-12:30	**Ring Exploration with Oblivious Myopic Robots.** Datta, Lamani, Larmore, Petit
12:30-13:00	**Fail Silent Road Side Unit for Vehicular Communications.** Ferreira, Oliveira, Almeida, Cruz
	Lunch break
14:00-14:30	**Reliability Analysis of Consensus in Cooperative Transport Systems.** Villani, Fathollahnejad, Pathan, Barbosa, Karlsson
14:30-15:00	**Secure Multiparty Computation vs. Fair Exchange - Bridging the Gap.** Garbinato, Rickebusch
15:00-15:30	**Certificating Vehicle Public Key with Vehicle Attributes: A (periodical) Licensing Routine, Against Man-in-the-Middle Attacks and Beyond.** Dolev, Panwar, Segal
	Coffee break
16:00-16:30	**Model-driven development of critical perception components using Simulink break.** Brade, Zug, Kaiser
16:30-17:00	**Designing applications in dynamic networks: the Airplug Software Distribution.** Ducourthial
17:00-17:30	**COTS-Architecture with a Real-Time OS for a Self-Driving Miniature Vehicle.** Berger, Al Mamun, Hansson
17:30-18:00	**Towards lightweight logging and replay of embedded, distributed systems.** Tomaselli, Landsiedel

Workshop Program

CARS — Workshop on Critical Automotive applications : Robustness and Safety

Room: Salle de conférences

9:00-9:30	Welcome address (Workshop organizers)
9:30-11:00	**System safety** (Chair: Philippe Quéré, Renault, France)
	Ride-through for Autonomous Vehicles. Aaron Kane and Philip Koopman
	Automatic Decomposition of Safety Integrity Levels: Optimization by Tabu Search. Luis Azevedo, David Parker, Martin Walker, Yiannis Papadopoulos and Rui Esteves Araújo
	CTMCONTROL: Addressing the MC/DC Objective for Safety-Critical Automotive Software. Anila Mjeda and Mike Hinchey
11:00-11:30	*Coffee break*
11:30-12:30	**Keynote Speech** (Chair: Jean-Charles Fabre, INPT, LAAS-CNRS, France)
	Development assurance of safety critical industrial systems : a cross-domain cross-standard perspective. Jean-Paul Blanquart, ASTRIUM Satellites, Toulouse, France
12:30-14:00	*Lunch break*
14:00-15:30	**Security & Networking**
	Security of embedded automotive networks: state of the art and a research proposal. Ivan Studnia, Vincent Nicomette, Eric Alata, Yves Deswarte, Mohamed Kaâniche and Youssef Laarouchi
	Preventing Memory Errors in Networked Vehicle Services Through Diversification. Hector Marco, Juan Carlos Ruiz and David de Andrés
	Experimental evaluation of end-to-end delay in switched Ethernet application in the automotive domain. Kostas Beretis and Ieroklis Symeonidis
15:30-16:00	*Coffee break*
16:00-17:30	**Architecture & Assessment** (Chair: Mario Trapp, IESE Kaiserslautern, Germany)
	Towards Dynamic Updates In AUTOSAR. Hélène Martorell, Jean-Charles Fabre, Matthieu Roy and Régis Valentin
	Don't Judge Software by Its (Code) Coverage. Rolf Johansson, Henrik Eriksson, Hans Svensson, Kenneth Östberg, Thomas Arts, Alex Gerdes and Martin Skoglund
	On the Need of a Methodological Approach for the Assessment of Software Architectures within ISO26262. Valentina Bonfiglio, Leonardo Montecchi, Francesco Rossi and Andrea Bondavalli
17:30	End

Workshop Program

ERCIM/EWICS — Workshop on Dependable Embedded and Cyberphysical Systems

Room: Salle Europe

9:00-9:20 Welcome and introduction

ERCIM, EWICS, ARTEMIS: Embedded Systems Safety, Security and European Strategy. Chairs Erwin Schoitsch (AIT Austrian Institute of Technology), Amund Skavhaug (NTNU, Norway)

9:20-10:35 **Session "Dependable Embedded Systems Applications"**

A Reference Example on the Specification of Safety Requirements using ISO 26262. Jonas Westman (KTH, Sweden) and Mattias Nyberg (Scania, Sweden)

FlexRay demonstrator for certification. Felix Bruckmüller, Erwin Kristen (AIT, Austria) and Wilfried Kubinger (FH Technikum, Vienna)

Towards Failure Models and Error Propagation in Product Lines. Sara Bessling (Clausthal University of Technology, Germany)

10:35-11:00 *Coffee break*

11:00-12:40 **Session "Autonomous Systems and Robotics (1)"**

R3-COP - Resilient Reasoning Robotic Co-operating Systems – an introduction and overview. Wolfgang Herzner and Erwin Schoitsch (AIT Austrian Institute of Technology, Vienna, Austria)

Model-based Testing of Cooperating Robotic Systems using Coloured Petri Nets. Raimar Lill and Francesca Saglietti (University of Erlangen-Nuremberg, Germany)

Scenario-based Automated Evaluation of Test Traces of Autonomous Systems. Gergö Horányi, Zoltán Micskei and Istvan Majzik (Budapest Univ. of Technology and Economics, Hungary)

Designing Autonomous Robot Systems – evaluation of the R3-COP Decision Support System approach. Tapio Heikkilä, Jukka Koskinen (VTT, Oulu, Finland) and Lars Dalgaard (DTI, Odense, Denmark)

12:40-13:40 *Lunch break*

13:40-15:20 **Session "Autonomous Systems and Robotics (2)"**

Obstacle detection and mapping in low-cost, low-power multi-robot systems using an Inverted Particle Filter. Adam Leon Kleppe and Amund Skavhaug (NTNU, Trondheim, Norway)

Robust perception in everyday environments. Jan Fischer, Joshua Hampp, Georg Arbeiter (Siemens AG, Munich/Germany), Robert Eidenberger, and Kai Wurm (Fraunhofer IPA, Stuttgart/Germany)

Model-based Test-Case Generation for Testing Robustness of Vision Components of Robotic Systems. Wolfgang Herzner, Markus Murschitz and Oliver Zendel (AIT Austrian Institute of Technology, Vienna)

Overview of Simulation of Video-Camera Effects for Robotic Systems in R3-COP. Michal Kučiš, Pavel Zemčík (Brno University of Technology, Czech Republic), Oliver Zendel and Wolfgang Herzner (AIT, Vienna)

15:20-15:50 *Coffee break*

15:50-17:30 **Session "Systems Safety Analysis and Fault Tolerance"**

Combination of Safety and Security Analysis - Finding Security Problems that Threaten the Safety of a System. Max Steiner and Peter Liggesmeyer (TU Kaiserslautern, Germany)

Simple Methods for Error Detection and Correction for Low-Cost Nanosatellites. Kjell Arne Ødegaard and Amund Skavhaug (NTNU, Trondheim, Norway).

Modeling and Analysis of Safety-Critical Cyber Physical Systems using State/Event Fault Trees. Michael Roth and Peter Liggesmeyer (TU Kaiserslautern, Germany)

A Reliable Fault-Tolerant Scheduling Algorithm for Real Time Embedded Systems. Chafik Arar, Hamoudi Kalla, Salim Kalla and Riadh Hocine (University of Batna, Algeria)

17:30-17:40 Concluding remarks and Farewell

Workshop Program

SASSUR — Next Generation of System Assurance Approaches for Safety-Critical Systems

Room: Salle du Conseil

9:00-9:15	Welcome
9:15-10:00	**Keynote: Conformance cases: the approach and experiences.** Prof. Janusz Gorski (Gdansk University of Technology, Poland)
10:00-10:30	**Design of a CDD-based Fault-injection Framework for AUTOSAR Systems.** As'Ad Salkham, Antonio Pecchia and Nuno Silva.
10:30-11:00	**Software Composability and Mixed Criticality for Triple Modular Redundant Architectures.** Stefan Resch, Andreas Steininger and Christoph Scherrer.
11:00-11:30	*Coffee break*
11:30-11:45	**Principled Construction of Software Safety Cases.** Richard Hawkins, Ibrahim Habli and Tim Kelly.
11:45-12:15	**Confidence in Timing.** Daniel Kästner and Christian Ferdinand.
12:15-12:30	**Adaptive Safety Arguments and Explanation-Based Learning.** Matthew Timperley, Maizura Mokhtar and Joe Howe
12:30-14:00	*Lunch break*
14:00-14:15	**Towards a multi-view point safety contract.** Alejandra Ruiz, Tim Kelly and Huascar Espinoza
14:15-14:45	**AARL: A Criterion for Composable Safety and Systems Engineering.** Eric Verhulst, Jose Luis de La Vara, Vincenzo de Florio and Bernhard Sputh.
14:45-15:15	**VROOM & cC: a Method to Build Safety Cases for ISO 26262-compliant Product Lines.** Barbara Gallina, Antonio Gallucci, Kristina Lundqvist and Mattias Nyberg.
15:30-16:00	*Coffee break*
16:00-17:15	Industrial Panel
17:15-17:30	Wrap up

Tutorial Program

FM&C — Formal methods and certification

Room: Salle Hourgade

This tutorial is jointly organized by Aerospace Valley Formal Methods Forum and CGEE Working Group on comparison of safety standards. The objective of this tutorial is to present existing certification standards in different application domains (aeronautics, automotive, nuclear, railway, space) with a special focus on the verification means that are allowed/recommended/mandatory in these standards. Test has always been a classical verification means but formal methods are making their way into industrial practice and are handled differently by the certification standards. We propose a one- day tutorial, with the following program:

9:00-10:00 *Overview of the place of formal methods in different safety standards — Jean-Paul Blanquart (CG2E Working Group)*

Even though most safety critical application domains and applicable safety standards share a largely common view on the acceptable means for development and safety assurance, there are also variations, which are important for instance for developers of applications or support tools in several domains, or even to support discussions towards evolution of standards. We will present a synthesis of similarities and differences between safety standards for what concerns the utilization of formal methods for certification (or qualification, acceptance...) and in particular with respect to «traditional» test-based justification. Addressed domains and standards will cover aeronautics (DO-178C), automotive (ISO 26262), industrial process automation (IEC 61508), nuclear (IEC 60880), railway (EN 50128) and space (ECSS-Q-ST-80C).

10:30-11:30 *DO-178C Formal Methods Technical supplement — Virginie Wiels (Onera)*

DO-178 is the software certification standard for aeronautics. Version C of this standard has been published in 2011. It includes a specific supplement on the use of formal methods for software verification. This talk will present this supplement.

11:30-12:30 *Industrial applications of formal methods in a certified context — Emmanuel Ledinot (Dassault Aviation) and Virginie Wiels (Onera)*

This talk will present two industrial applications of formal methods for software verification.

14:00-15:30 *Formal methods and railway — Jean-Louis Boulanger (CERTIFER)*

CENELEC EN 50128:2011 is the new standard for software development in the railway domain. In both versions of this standard (2001 and 2011) the use of formal methods is highly recommended. This recommendation is linked to the software safety integrity level (called SSIL). In this talk we present different examples of use of formal methods and we discuss their impact on the different verification activities. We also discuss the combination of proof and test to demonstrate software safety.

16:00-17h00 Panel *«Argumentation based on mixed formal/non formal evidence for the satisfaction of safety claims" animated by Gérard Ladier (Aerospace Valley) and Cyrille Comar (Adacore)*

Tutorial Program

SA$_4$SE — Security-awareness for safety engineers

Room: Salle Bardeen

OVERALL AIM OF THE TUTORIAL

To raise awareness of cyber security issues and concerns so as to help safety engineers to

- understand the risks that security threats pose to safety systems
- appreciate whether safety systems are adequately secure as well as adequately safe
- know when to seek specialised advice

LEARNING OUTCOMES

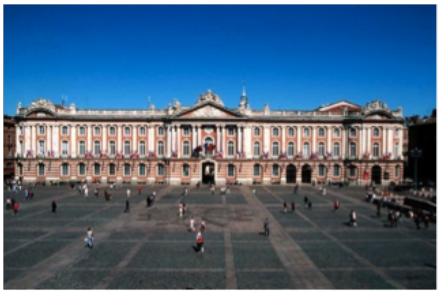
- Understand the importance of ensuring that control systems are both safe and secure
- Be informed about real world security incidents and current concerns
- Be aware of potential threats and vulnerabilities in control systems, and the controls and mitigations that are available
- Have a basic knowledge of security concepts and the principles of building secure systems
- Be aware of relevant standards and guidelines for assessing security risks
- Know when and how to seek more specialised advice about security issues

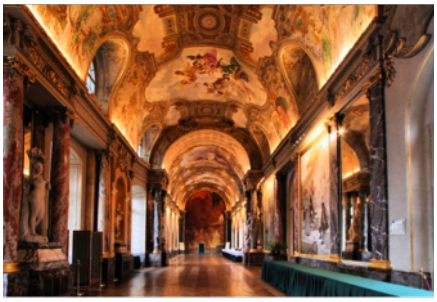
TUTORIAL CHAIR

Robert Stroud, Senior Consultant, Adelard LLP

Social Events

WELCOME RECEPTION AT TOULOUSE CITY HALL, SALLE DES ILLUSTRES





WHEN

Tuesday 24th September 2013, 18:30 to 19:30

ADDRESS

Mairie de Toulouse, 1 Place du Capitole, Toulouse

HOW TO GET THERE

Metro station Capitole, 1 minute walking

GUIDED CITY TOUR

WHEN

Wednesday 25th September 2013, 18:30 – 19:30

ADDRESS

Tourist Office, Square Charles de Gaulle (close to Toulouse City Hall and place du Capitole)

HOW TO GET THERE

Metro station Capitole, 1 minute walking

WINE TASTING

WHEN

Wednesday 25th September 2013, 19:30 – 20:30

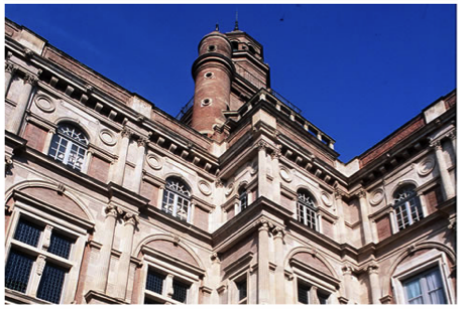
ADDRESS

47 rue Pharaon, Toulouse

HOW TO GET THERE

Metro Station Carmes, or Metro Station Jean-Jaures then 10 minutes walking

BANQUET AT HOTEL D'ASSEZAT



WHEN

Thursday 26th September 2013, 19:00

ADDRESS

Hôtel d'Assezat, Place Assezat, Toulouse

HOW TO GET THERE

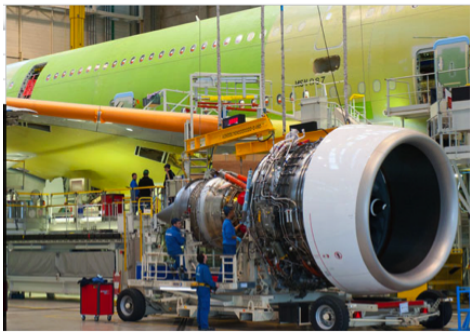
The SAFECOMP Bus will drop participants from Airbus technical visit directly downtown near hotel d'Assezat. If you plan to go on your own, it is close to the Esquirol metro station (3 minutes walking).

Social Events

TECHNICAL VISIT OF AIRBUS FINAL ASSEMBLY CHAIN

WHEN

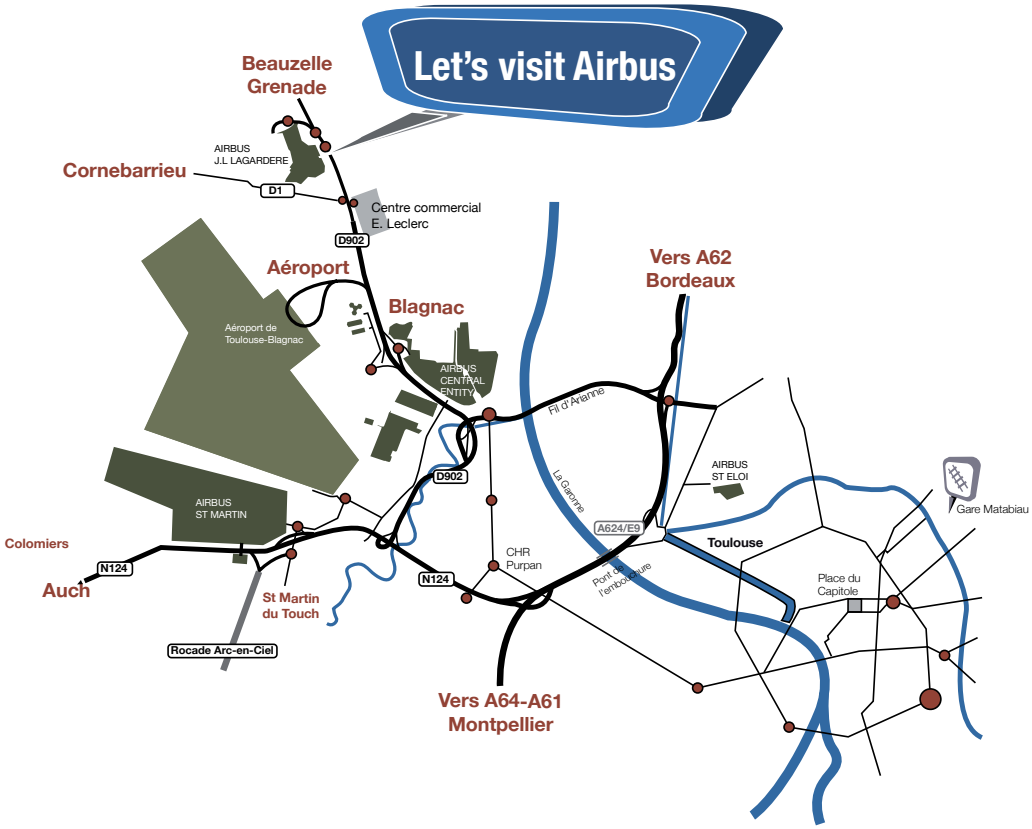
Thursday 26th September 2013



HOW TO GET THERE

The Safecomp bus will start from LAAS-CNRS at 16:15. The Airbus Visit will start at 17:00. If you plan to reach Airbus by car (30 to 40 minutes from LAAS-CNRS):

Village Aéroconstellation
Rue Franz Joseph Strauss - 31700 BLAGNAC
Latitude : 43°39'16" North (43.654440780859666)
Longitude : 01°21'45" East (1.3625226648040866)

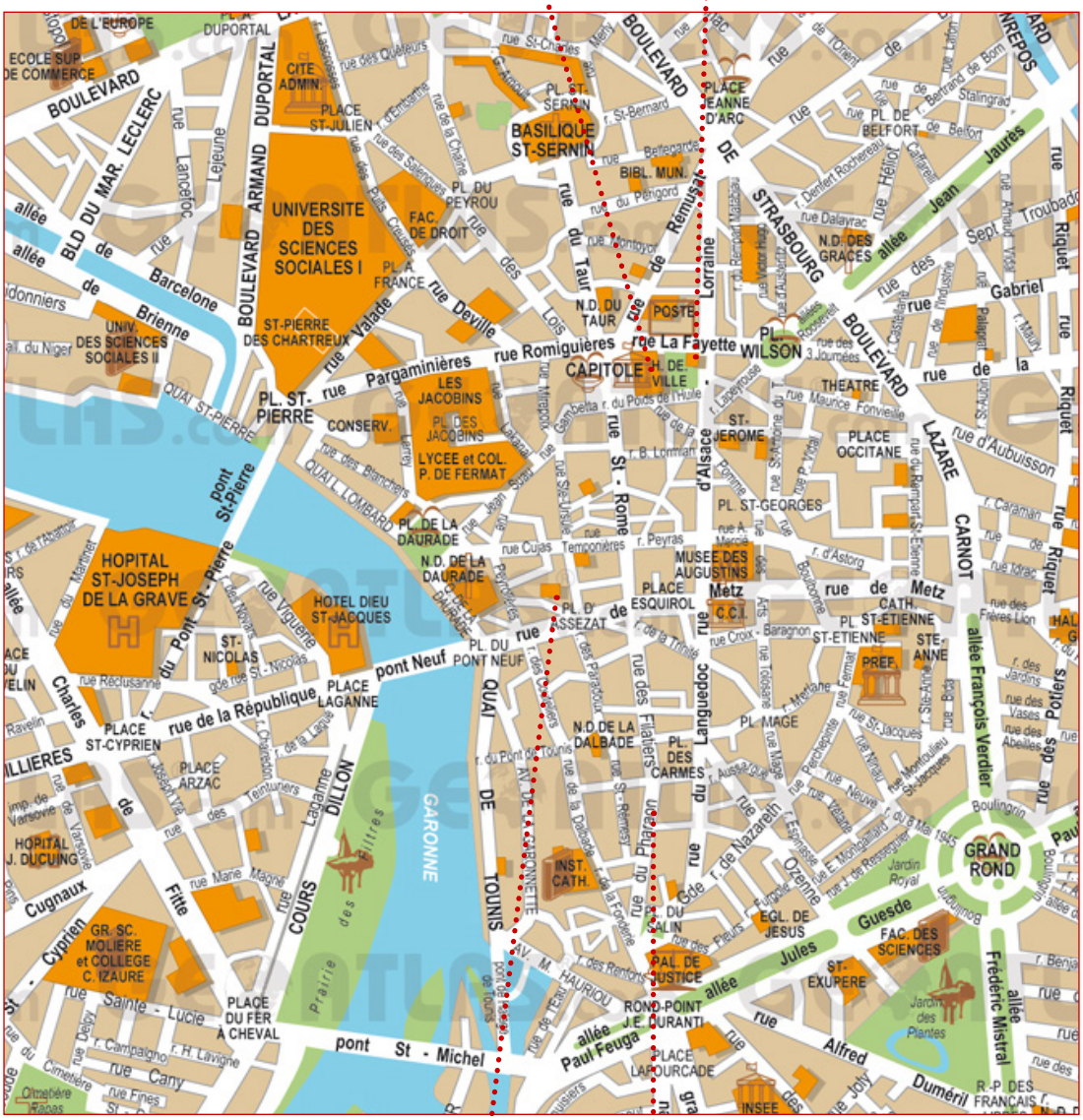


Overview Map

Welcome Reception, Guided city Tour meeting point, Wine tasting, Banquet, SAFECOMP bus stop

TOULOUSE CITY HALL
(Welcome Reception)
Address: 1 Place du Capitole, Toulouse

TOURIST OFFICE
(Guided City Tour)
Address: Square Charles de Gaulle (close to Toulouse City Hall and place du Capitole)



HOTEL D'ASSEZAT
(Banquet)
Address: Place d'Assezat, Toulouse

WINE TASTING
Address: 47 rue Pharaon

Sponsoring Institutions

- European Workshop on Industrial Computer Systems Reliability, Safety and Security
- Laboratory for Analysis and Architecture of Systems, Carnot Institute
- Centre national de la recherche scientifique
- International Federation for Information Processing
- Université Paul Sabatier
- University of Toulouse
- Région Midi-Pyrénées
- Communauté urbaine Toulouse Metropole
- Mairie de Toulouse
- Sciences et Technologies pour l'Aéronautique et l'Espace
- Airbus EADS
- Institut national des sciences appliquées de Toulouse
- European Research Consortium for Informatics and Mathematics
- Austrian Institute of Technology
- Société de l'Electricité, de l'Electronique et des Technologies de l'Information et de la Communication
- Word competitiveness Cluster in Aeronautics, Space and Embedded Systems, of Midi-Pyrenées and Aquitaine
- Informationstechnische Gesellschaft
- German Computer Society
- Austrian Computer Society
- European Network of Clubs for Reliability and Safety of Software-Intensive Systems

Contacts

Secrétariat SAFECOMP 2013
LAAS-CNRS — TSF Group
7 avenue du Colonel Roche
BP54200
31031 Toulouse Cedex 4, France

email: safecomp2013@laas.fr
Tel: +33 5 61336255
Contact: Sonia De Sousa

Printed in LAAS-CNRS, France, 2013
Editorial Board: Dominique Daurat, Jérémie Guiochet
Manufacturing: Christian Berty