Two Decades of Formal Methods for Industrial Critical Systems

Radu Mateescu

Inria – Univ. Grenoble Alpes - LIG

Formal Methods for Industrial Critical Systems

http://fmics.inria.fr

FMICS: oldest active WG of ERCIM

*Following an initial successful workshop bringing together ERCIM members interested in formal verification, held in Pisa in **December 1992**, **Stefania Gnesi** and **Diego Latella**, CNR, Pisa, proposed to create an ERCIM working group dedicated to **Formal Methods for Industrial Critical Systems** (**FMICS**). Although at that time, model checking was in its early days, the early ERCIM FMICS community was already aware of the great potential of formal verification techniques.*

Aim of FMICS

The main objectives of the WG are:

- To bring together scientists mainly (but not only) of ERCIM institutions, who are active in the field of formal methods and are willing to exchange their experience in the **industrial usage** of **formal methods**.
- To coordinate efforts in the transfer of the **formal methods** technology and knowledge to the **industry**.
- To promote research and development for the improvement of **formal methods** and **tools** with respect to their **usage** in the **industry**.

The above objectives will be met by means of:

- **Workshops** where the participation of industrial professionals will be solicited.
- **Development projects** with **industrial partners**.
- **Research projects** and researchers **mobility**.

FMICS WG Board and Coordination

FMICS WG Board:

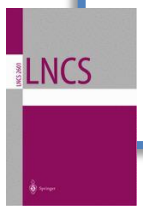
- Alvaro Arenas (STFC)
- Lubos Brim (CRCIM): Liaison with ERCIM board
- Alessandro Fantechi (University of Firenze)
- Hubert Garavel (INRIA): Dissemination and Web site
- Stefania Gnesi (ISTI-CNR): "Formal Methods" handbook coordination
- Diego Latella (ISTI-CNR)
- Tiziana Margaria (University of Potsdam): European projects
- Pedro Merino (University of Malaga): Relation with industry and standardization bodies
- Jaco van de Pol (CWI): **Vice-chair**, journal special issues and liaison with other WGs

Next FMICS Chair: Tiziana Margaria

Former FMICS Chairs :

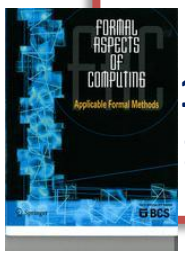
- **Diego Latella** (August 1996 - July 1999)
- **Hubert Garavel** (July 1999 - July 2002)
- **Stefania Gnesi** (July 2002 - November 2005)
- **Pedro Merino** (November 2005 - October 2008)
- **Alessandro Fantechi** (November 2008 - October 2011)
- **Radu Mateescu** (November 2011 – October 2014)

Twenty FMICS Yearly Workshops

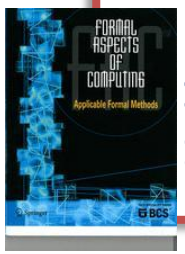
FME Oxford 1996	ICALP Cesena 1997	Amsterdam 1998	FLoC Trento 1999	Berlin 2000
CAV Paris 2001	ICALP Malaga 2002	ERCIM Trondheim 2003	ASE Linz 2004	ESEC/FSE Lisbon 2005
 CONCUR Bonn 2006	 CAV Berlin 2007	 ASE L'Aquila 2008	 FM Eindhoven 2009	 ASE Antwerp 2010
 RE Trento 2011	 FM Paris 2012	 SEFM Madrid 2013	 FLORENCE Florence 2014	 FM Oslo 2015

Journal Special Issues

FMSD
12(2)
1998



FAC
10(4)
1998



FAC
10(5-6)
1998

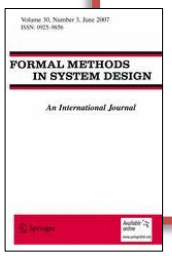
SCP
36(1)
2000

SCP
(on
track)

FMSD
19(2)
2001

SCP
46(3)
2003

STTT
5(2-3)
2004



FMSD
30(3)
2007

STTT
(on
track)

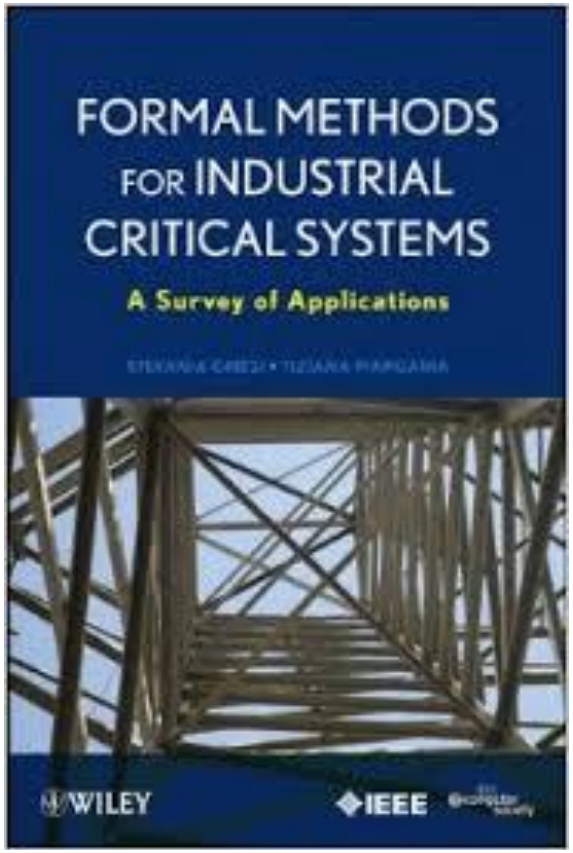
STTT
11(5)
2009

SCP
76(2)
2011

SCP
78(7)
2013

STTT
16(6)
2014

FMICS Book



Editors: Stefania Gnesi, Tiziana Margaria

Wiley-IEEE, 2013, 292 pages

Today, formal methods are widely recognized as an essential step in the design process of industrial safety-critical systems. In its more general definition, the term formal methods encompasses all notations having a precise mathematical semantics, together with their associated analysis methods, that allow description and reasoning about the behavior of a system in a formal manner. […]

The purpose of the book is threefold: to reduce the effort required to learn formal methods, which has been a major drawback for their industrial dissemination; to help designers to adopt the formal methods which are most appropriate for their systems; and to offer a panel of state-of-the-art techniques and tools for analyzing critical systems.

FMICS in ERCIM News

- ERCIM News No.25 - April 1996
  report by D. Latella and S. Gnesi
- ERCIM News No.26 - July 1996
  report by D. Latella
- ERCIM News No.31 - October 1997
  report by S. Gnesi and D. Latella
- ERCIM News No.34 - July 1998
  report by Diego Latella
- ERCIM News No.39 - October 1999
  Towards Reliable Computer Systems?
  by D. Latella, S. Gnesi, and H. Garavel
- ERCIM News No.47 - October 2001
  report by H. Garavel
- ERCIM News No.47 - October 2001
  How can I be sure that my DVD player understands my TV?
  by W. Fokkink, I. van Langevelde, B. Luttik, and Y. Usenko
- ERCIM News No.54 - July 2003
  report by T. Arts and W. Fokkink
- FMICS receives the ERCIM Working Group Award 2003
- ERCIM News No. 67 – October 2006
  report by L. Brim and M. Leucker
- ERCIM News No. 75 – October 2008
  Special theme *Safety-Critical Software*
  Editors: P. Merino and E. Schoitsch
- ERCIM News No.91 - October 2012
  report by R. Mateescu
- ERCIM News No.92 - January 2013
  report by A. Fantechi, F. Flammini, and S. Gnesi

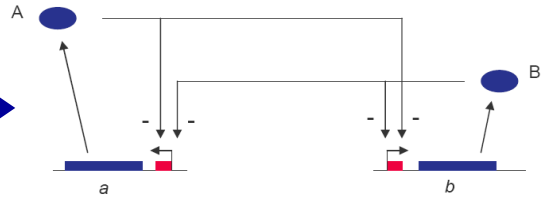
European Project EC-MOAN

FP6-NEST-PATH-COM-043235 (2007-2009)

http://www.ec-moan.org/

Escherichia Coli – MOdeling and ANalysis

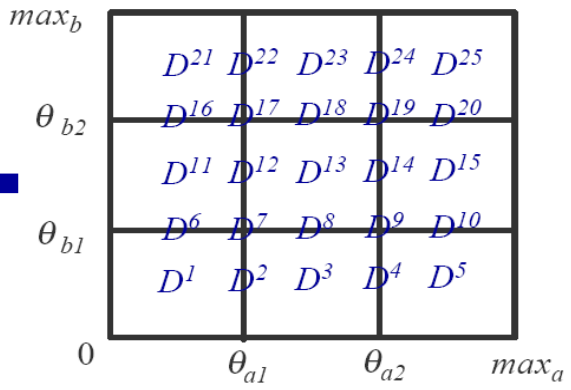
E. coli



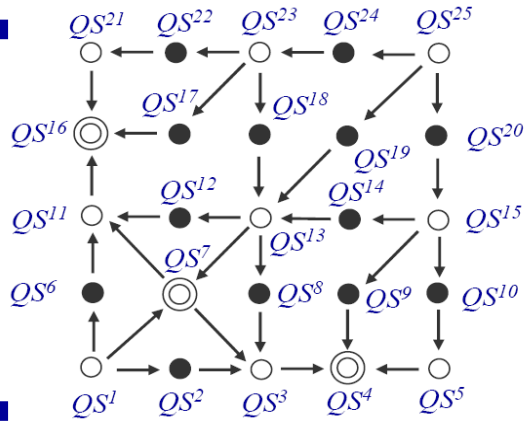
Genetic Regulatory Network

$$\dot{x}_a = \kappa_a\, s^-(x_a, \theta_{a2})\, s^-(x_b, \theta_{b1}) - \gamma_a\, x_a$$
$$\dot{x}_b = \kappa_b\, s^-(x_a, \theta_{a1})\, s^-(x_b, \theta_{b2}) - \gamma_b\, x_b$$

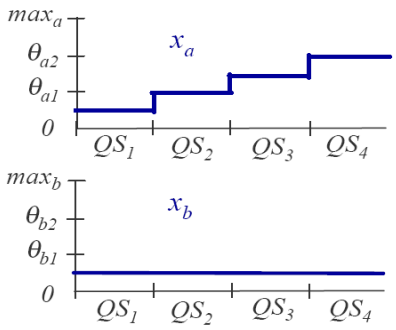
Piecewise-linear differential equations



Qualitative simulation



State-transition graph



Simulation (GNA)

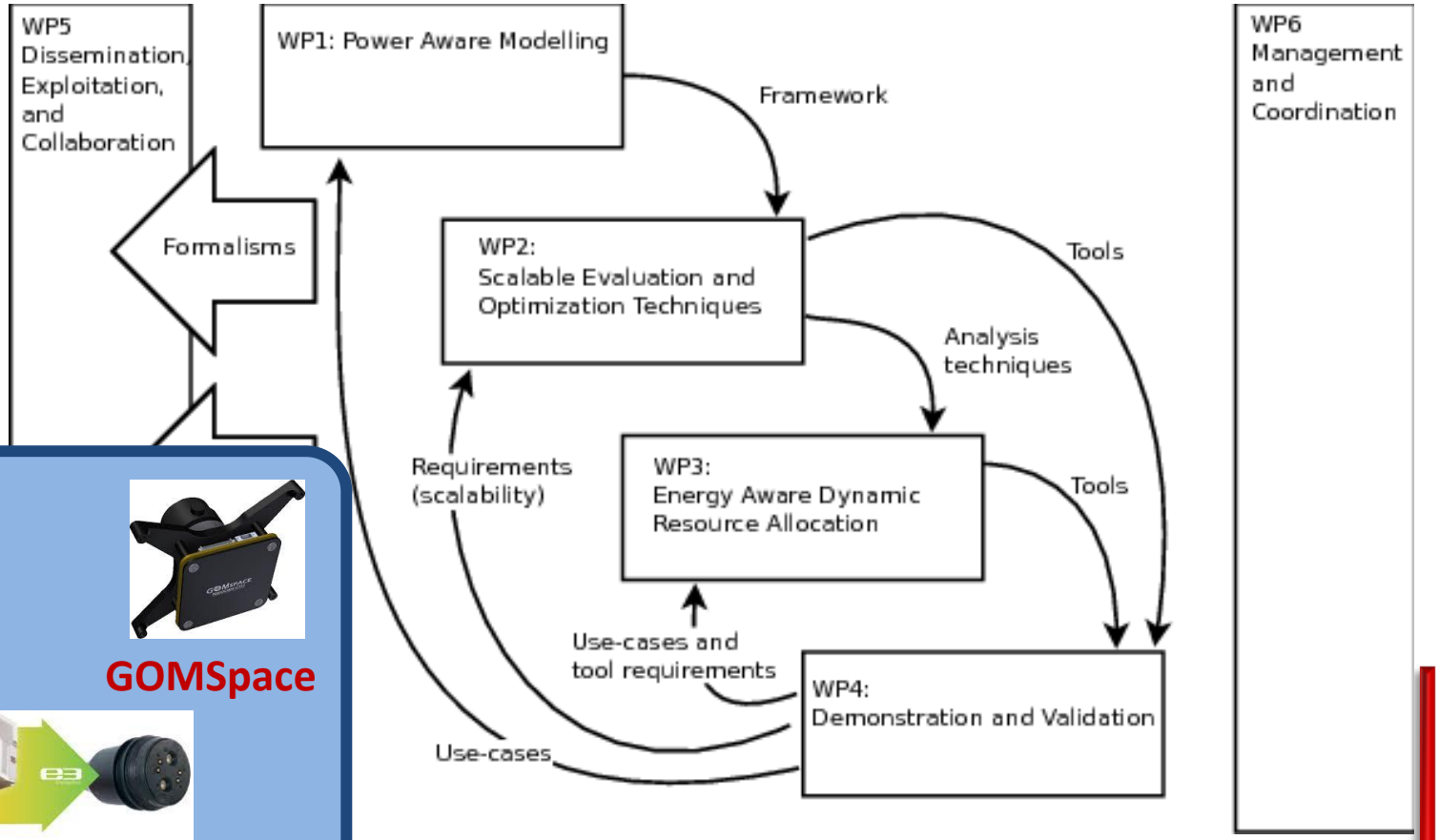
Model checking (CADP)

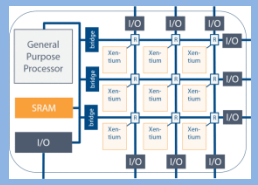
European Project SENSATION

FP7-ICT-2011-8-318490 (2012-2015)

http://www.sensation-project.eu/

Self ENergy-Supporting Autonomous computaTION





RECORE

GOMSpace

EnergyBus

Perspectives

- Concurrency becomes ubiquitous:

  Networks-on-Chip ↗ multicore computers ↗ clouds

  ➔ complexity and criticality
- Certification required (avionics, medical devices, …)
- **Formal methods** and **verification** become increasingly important in the design process
- Many events on formal methods:

  ATVA, AVOCS, CAV, ETAPS, FM, FMICS, ICFEM, IFM, ISOLA, SEFM, …

  ➔ ***carry on and tighten the links within the community***