# imdea software institute

**science and technology** for developing better software

institute
imdea
software

# annual report 2013

# foreword

foreword

**Manuel Hermenegildo**
Director, IMDEA Software Institute
March 15, 2014

annual report
2013

The IMDEA Software Institute was created by the Madrid Regional Government under the strong belief that quality research in technology-related areas is the most successful and cost-effective way of generating knowledge, sustainable growth, and employment. This is more relevant currently than ever, and software-related technology indeed has an immense potential for raising industrial competitiveness, opening whole new business areas, creating high added-value jobs, and, ultimately, improving quality of life. Today, the Institute is a vibrant, exciting reality, reaching significant milestones towards its goals of excellence in research and technology transfer.

Without any doubt, the main strength of the Institute is its people: its researchers and support staff. The Institute has been very successful in attracting to Madrid top talent worldwide, including now 21 faculty (one half-time), 8 postdocs, 16 research assistants, and a number of interns, from 16 different nationalities. They joined after working at or obtaining their Ph.D. degrees from 32 different prestigious centers in 8 different countries, including Stanford U., Carnegie Mellon U., or Microsoft Research in the US, INRIA in France, U. of Cambridge in the UK, the Max Planck Software Institute in Germany, or ETH in Switzerland, to name just a few. In addition, 106 international researchers have visited and given talks at the Institute to date.

During 2013 Institute researchers have published 60 refereed articles (in some of the top venues in the field, such as POPL, ACM TOPLAS, CRYPTO, IEEE S&P, USENIX Security, CSF, JCS, FM, CAV, TPLP, ICFP, ICLP, ICALP, etc.), given 16 invited talks and 20 invited seminars and lectures, and participated in 43 program committees and 14 boards of journals and conferences, in addition to being conference and program chairs of 4 conferences. The Institute has received 8 best paper awards or mentions in the last 3 years.

The Institute has also participated during 2013 in 27 funded research projects and contracts and received 13 fellowships. 13 of the projects are international (11 funded by the EU, 1 by the US ONR and Stanford U., and 1 by the Danish Research Council), 9 are direct industrial funding, and in general 15 (68%) involve collaboration with a large number of companies which include Atos, Siemens, Deimos, AbsInt, Microsoft, Fredhopper, Telefonica, Boeing, Thales, and Logicblox (and many others in other recent projects, such as France Telecom, SAP, Trusted Logic, Airbus, Alcatel, Daimler, or EADS). The Institute is also working on the commercialization of the ActionGUI technology developed by its Modeling Lab in collaboration with ETH Zurich.

The Institute has also developed further its strategic partnership with Telefonica, Indra, Atos, BBVA, UPM, and BSC, leading the Spanish Associate Partner Group of the European Institute of Technology (EIT) ICT Labs, of which the IMDEA Software Institute is the first Associate Partner in Spain. The Institute has also strengthened its collaborations with Microsoft leading to the establishment of a Microsoft Research–IMDEA Software Joint Research Center.

Finally, 2013 has marked the first complete year in the Institute's new building. The official opening ceremony was also held this year, chaired by the President of the Madrid Government, Ignacio González.

Many thanks once more to all who have contributed to all these achievements, and very specially to the Madrid Regional Government for their continuing vision and support.

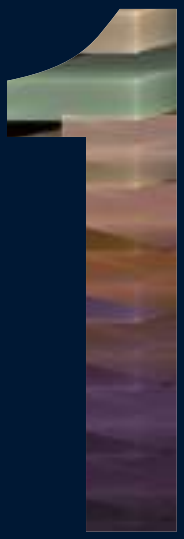
# table of contents

table of contents

annual report

2013

# general presentation





annual report 2013

## 1.1 Profile

The IMDEA Software Institute (Madrid Institute for Advanced Studies in Software Development Technologies) is a non-profit, independent research institute promoted by the Madrid Regional Government (CM) to perform research of excellence in the methods, languages, and tools that will allow the cost-effective development of software products with sophisticated functionality and high quality, i.e., which are safe, reliable, and efficient.

The IMDEA Software Institute is part of the Madrid Institute for Advanced Studies (IMDEA) network, an institutional framework created to foster social and economic growth in the region of Madrid by promoting research of excellence and technology transfer in a number of strategic areas (water, food, energy, materials, nanoscience, networks, and software) with high potential impact.

## 1.2 Motivation and Goals

It is difficult to overstate the importance of software in both our daily lives and in the industrial processes which, running behind the scenes, sustain the modern world. Indeed, software is the enabling technology behind many devices and services which are now essential part of our lives and on which we depend: cell phones, cars, banking, flight control, the stock market, digital television, medical equipment – not to mention tablets, computers, and the Internet itself. This pervasiveness explains the global figures around software and the IT services sector: according to the Global Industry Guide, the global software market had an estimated value of 293.000 M€ in 2011, which is estimated to grow to 396.000 M€ by 2016. According to European Commission data, in 2012 and 2013 the ICT sector accounted for 6% of EU GDP and approximately eight million jobs. In fact, the forecasts by the major market analysts, such as Gartner, Forrester, IDC and the International Monetary Fund (IMF), show that compared with a fall of the average global GDP growth rate in 2013, which is estimated at 2.6-2.9%, the estimated IT market growth is much more vigorous, between 4.2 and 6%, while the estimates of the software market growth are still higher, at approximately 6.5%. This vividly illustrates the huge potential of the software industry to drive economic growth and create jobs.

Given the economic relevance of software and its pervasiveness, errors and failures in software can have high social and economic cost: the results of malfunctioning software can range from being annoying (e.g., having to reboot), through posing serious social and legal problems (e.g., privacy and security leaks), to having high economic cost (e.g., software failures in financial markets and software-related product recalls) or even being a threat to human lives (e.g., a malfunctioning airplane or medical device). Unfortunately, developing software of an appropriate level of reliability, security, and performance, at a reasonable cost is still a challenge today. Some degree of correctness can be achieved by careful


*Modern cars and trucks contain as many 100 million lines of computer code. This software runs on more than 30 on-board computers and controls vital functions, including the brakes, engine, cruise control, and stability systems. It is under increasing scrutiny in the wake of recent problems with major manufacturers and it is currently impossible to fully test.*

human or machine-assisted inspection at very high monetary costs, but the risk of errors produced by human mistakes will still be lurking in the dark. Reducing software errors in a cost-effective manner is therefore a task better left to automatic tools. These tools are, however, extremely hard to produce and pose scientific and technological challenges. At the same time, the ubiquity of software makes tacking these challenges a potentially highly profitable endeavor, since solutions to these challenges can have a significant and pervasive impact on productivity and on the general competitiveness of the economy.

The main mission of the IMDEA Software Institute is to tackle this challenge by performing research of excellence in methods, languages, and tools that will allow the cost-effective development of software products with sophisticated functionality and high quality, i.e., secure, reliable, and efficient. This research focus includes all phases of the development cycle (analysis, design, implementation, validation, verification, maintenance); its distinguishing feature is the concentration on approaches that are rigorous and at the same time allow building practical tools.

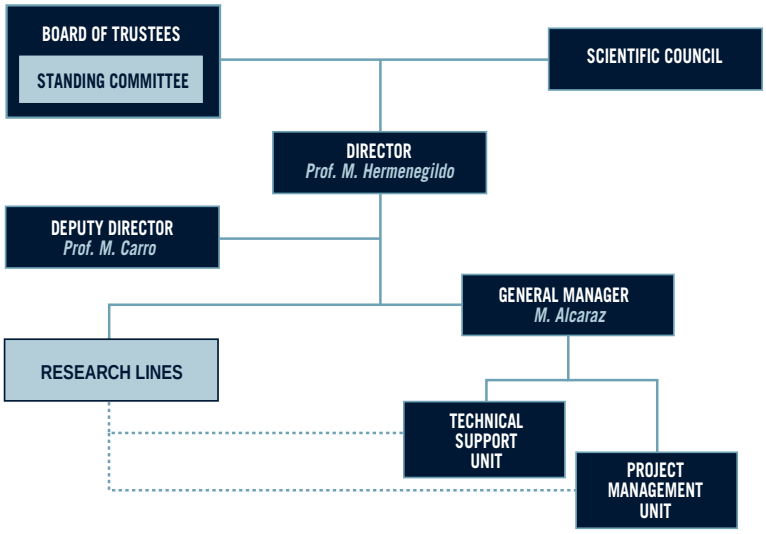
In order to achieve its mission, the IMDEA Software Institute gathers a critical mass of worldwide, top-class researchers, and at the same time develops synergies between them and the already significant research base and industrial capabilities existing in the region. Indeed, most of the IT-related companies in Spain (and, specially, their research divisions) are located in the Madrid region, which facilitates collaboration and technology transfer. Thus, the IMDEA Software Institute materializes the opportunity of grouping a critical mass of researchers and industrial experts, allowing for significant improvement in the impact of research.

## 1.3 Legal Status, Governance, and Management

The IMDEA Software Institute is a non-profit, independent organization, constituted as a Foundation. Its structure brings together the advantages and guarantees offered by a founda-

tion with the flexible and dynamic management typical of a private body. This combination is deemed necessary to attain the goals of excellence in research, cooperation with industry, and attraction of talented researchers from all over the world, while managing a combination of public and private funds. The Institute was created officially on November 23, 2006 at the initiative of the Madrid Regional Government, following a design that was the result of a collaborative effort between industry and academia, and started its activities during 2007.

The main governing body of the Institute is the **Board of Trustees**. The Board includes representatives of the Madrid Regional Government, universities and research centers of Madrid, scientists with high international reputation in software development science and technology, and representatives of companies, together with independent experts.




*Governance and management structure of the IMDEA Software Institute.*

The Board is in charge of guaranteeing the fulfillment of the foundational purpose and the correct administration of the funds and rights that make up the assets of the Institute, maintaining their appropriate returns and utility. The Board normally meets twice a year. In the interim Board-level decisions are delegated to the **Standing Committee** of the Board. The Board appoints the **Director**, who is the CEO of the Institute, among scientists with a well-established international reputation in software development science and technology. The Director fosters and supervises the activities of the Institute, and establishes the distribution and application of the available funds among the goals of the Institute, within the patterns and limits decided by the Board of Trustees. The Director is assisted by the **Deputy Director** and the **General Manager**, who take care of the legal, administrative, and financial activities of the Institute, and supervise the **Project Management** and the **Technical Support** and **Infrastructure** units which work closely with and support the **Research Lines** of the Institute. The current structure is depicted in the figure above.

The Board of Trustees and the Director are assisted in their functions by the **Scientific Council,** composed of high-level external scientists of international reputation with expertise in different areas of research covered by the Institute. The tasks of this scientific council include: to provide advice on and approve the selection of researchers; to provide advice and supervision in the preparation of yearly and longer-term strategic plans; to evaluate the performance with respect to those plans; and to give general advice on matters of relevance to the Institute.

## 1.4 Appointments to the Board of Trustees

In 2013, Rocio Albert López-Ibor, Director General for Universities and Research at the Regional Government of Madrid was appointed to the Board of Trustees, replacing Jon Juaristi who held the same position in the Regional Government until August 2013. Also during 2013, Prof. Diego Córdoba Gazolaz was appointed the representative of the Spanish High Council for Scientific Research (CSIC), taking over that duty from Prof. Carmen Peláez Martinez, who served on the Board since 2008.

## 1.5 Members of the Governing Bodies

### Board of Trustees

#### CHAIRMAN OF THE FOUNDATION

**Prof. David S. Warren**
*State University of New York at Stony Brook, USA.*

#### VICE-CHAIRMAN OF THE FOUNDATION

**Excma. Sra. Dña. Alicia Delibes Liniers**
*Vice-counselor for Education, Madrid Regional Government, Spain.*

#### MADRID REGIONAL GOVERNMENT

**Excma. Sra. Dña. Alicia Delibes Liniers**
*Vice-counselor for Education, Madrid Regional Government, Spain.*

**Ilmo. Sr. D. José María Rotellar García**
*Vice-counselor of the Treasury, Madrid Regional Government, Spain.*

**Ilma. Sra. Dña. Rocio Albert López-Ibor**
*Director General for Universities and Research, Madrid Regional Government, Spain.*

**Prof. Juan Ángel Botas**
*Deputy Director for Research, Department of Education, Madrid Regional Government, Spain. Chairman of the Standing Committee.*

#### UNIVERSITIES AND PUBLIC RESEARCH BODIES

**Prof. Narciso Martí Oliet**
*Universidad Complutense de Madrid, Spain.*

**Prof. Javier Segovia Pérez**
*Universidad Politécnica de Madrid, Spain.*

**Prof. Diego Córdoba Gazolaz**
*Consejo Superior de Investigaciones Científicas (CSIC), Spain.*

**Prof. Jesús M. González Barahona**
*Universidad Rey Juan Carlos, Madrid, Spain.*

## SCIENTIFIC TRUSTEES

**Prof. David S. Warren**
*State University of New York at Stony Brook, USA. Chairman of the Board of Trustees.*

**Prof. Patrick Cousot**
*École Normale Supérieure de Paris (ENS), France and Courant Institute, New York University, USA.*

**Prof. Luis Moniz Pereira**
*Universidade Nova de Lisboa, Portugal.*

**Prof. José Meseguer**
*University of Illinois at Urbana Champaign, USA.*

**Prof. Roberto Di Cosmo**
*Université Paris 7, France.*

## EXPERT TRUSTEES

**Mr. José de la Sota Rius**
*Managing Director, Fundación para el Conocimiento (MadrI+D), Madrid, Spain.*

**Mr. Eduardo Sicilia Cavanillas**
*Escuela de Organización Industrial, Madrid, Spain.*

## INDUSTRIAL TRUSTEES

**BBVA**
*Ms. María Carmen López Herranz. Innovation - Global Observatory & Portfolio Director at BBVA.*

Board meetings have been attended, as invitees, by representatives of the following companies:

**Telefónica I+D**
*Mr. Francisco Jariego, Director for Technology Strategy at Telefónica R&D.*

**Deimos Space**
*Mr. Miguel Belló Mora, General Director and Mr. Carlos Fernández de la Peña.*

**Atos**
*Mr. José María Cavanillas, Director Research & Innovation, and Ms. Clara Pezuela.*

## SECRETARY

**Mr. Alejandro Blázquez Lidoy**

## Scientific Council

**Prof. David S. Warren**
*State University of New York at Stony Brook, USA. Chairman of the Board.*

**Prof. María Alpuente**
*Universidad Politécnica de Valencia, Spain.*

**Prof. Roberto Di Cosmo**
*Universitè Paris 7, France.*

**Prof. Patrick Cousot**
*École Normale Supérieure de Paris (ENS), France and Courant Institute, New York University, USA.*

**Prof. Veronica Dahl**
*University Simon Fraser, Vancouver, Canada.*

**Prof. Herbert Kuchen**
*Universität Münster, Germany.*

**Prof. José Meseguer**
*University of Illinois at Urbana Champaign, USA.*

**Prof. Luis Moniz Pereira**
*Universidade Nova de Lisboa, Portugal.*

**Prof. Martin Wirsing**
*Ludwig-Maximilians-Universität, München, Germany.*

## 1.6 Headquarters Building

In 2013, IMDEA Software moved to its new headquarters building in the Montegancedo Science and Technology Park. This new building was officially inaugurated in July 2013 by Ignacio Gonzalez, President of the Government of the Madrid Region. The President was accompanied by the Secretary of State for Research, Development, and Innovation of the Ministry for Economy and Competitiveness, Carmen Vela, the Rector of the Technical University of Madrid, Carlos Conde, and the Counselor for Education, Youth, and Sports, Lucía Figar, among other personalities form industry, science, and research policy.

The new building offers an ideal environment for fulfilling the Institute's mission of research and technology transfer. It includes offices, numerous spaces for interaction and collaboration, areas for project meetings and for scientific and industrial conferences and workshops, and powerful communications and computing infrastructures. It also provides ample space for strategic activities such as the European Institute of Technology ICT Labs Madrid Co-location Center, the IMDEA Software-Microsoft Joint Research Center, and other joint research units with industry. It is highly energy-efficient, through energy-conscious design, co-generation, and full automation.



The location of the new IMDEA Software building also provides excellent access to the UPM Computer Science Department as well as to the other research centers within the Montegancedo Park. These centers include the Madrid Center for Supercomputing and Visualization (CESVIMA), the UPM Montegancedo Campus company "incubator" and technology transfer center (CAIT), the Institute for Home Automation (CEDINT), the Institute for Biotechnology and Plant Genomics (CBGP), the Center for Biomedical Technology (CTB), the Microgravity Institute, and the Spanish User Support and Operations Centre for ISS payloads (USOC). In particular, the CESVIMA houses the second largest supercomputer in Spain and one of the largest in Europe, as well as a state-of-the-art visualization cave, and is equipped for massive information storage and processing, high performance computing, and advanced interactive visualization.

The campus recently obtained the prestigious "International Campus of Excellence" label, and is the only campus in Spain to receive a "Campus of Excellence in Research and Technology Transfer" award in the Information and Communications Technologies area from the Spanish government.

# industrial and institutional partnerships



annual report 2013

## 2.1 Industrial Partnerships

The key to innovation is in incorporating new scientific results and technologies into processes and products in a way that increases industrial competitiveness, contributes to sustainable growth, and creates jobs. As a generator of new knowledge and technology in the area of ICT –which has a high economic impact– IMDEA Software is committed to fostering innovation and technology transfer in partnership with industry.

Key instruments for carrying out industrial partnerships are focused collaborations with companies in the form of collaborative projects funded through competitive public calls, and direct industrial contracts. These instruments represent an excellent vehicle for performing joint research and pushing its results towards the market. Figure 2.1 lists some of the companies with which the IMDEA Software Institute has collaborated to date in such projects and contracts (the currently active ones are described further in Chapter 5).

The Institute has also established long-term, *strategic partnerships* with the main stakeholders in the sector which facilitate longer-term collaboration across projects. In particular, the Institute has established close ties with Telefonica, Indra, Atos, and BBVA, which have led to a number of strategic cooperation initiatives. The Institute has established *Joint Research Units* with Telefónica and Microsoft Research, and is planning establishment of more such units with strategic partners.

Participation in Spanish and EU *Technology Platforms* is another strategically important line for the Institute's industrial collaboration. These include the Technology Clusters of the Madrid Region, the INES Spanish Platform for Software and Services, and the Internet of the Future Es.Internet Spanish platform.

Another important form of technology transfer is the *commercialization of technology* developed at the Institute. Given the controversy around software patents (and the impossibility of filing software patents in Europe) the Institute is combining the protection of its intellectual property with other innovative business models, such as those based on open-source or free software licenses, together with the licensing of such technology and the *creation of technology-based start-ups*. For example, a *software registration* has been made for the ActionGUI technology jointly developed by IMDEA Software and ETH Zürich, and active work on its commercialization is under way.

Other forms of industry collaboration include the *industrial funding of doctoral and master students* at the Institute working on industry-relevant topics (e.g., Microsoft funds research assistants working on software verification and security), *transfer of research personnel trained at the Institute to companies* (IMDEA Software-trained personnel has already been transferred to companies such as Atos, Microsoft, Google, or Logicblox), funding by industry of *research stays of Institute researchers at company premises* (e.g., Institute researchers

have made industrially-funded extended stays at Deimos Space, Microsoft Redmond in the US, or Microsoft Cambridge in the UK, and a framework agreement has been signed with Microsoft for this purpose), *access to the Institute's technology and scientific results* (e.g., researchers of the Institute have met with personnel from BBVA, Telefónica I+D, Ericsson, GMV, INDRA, IBM, Canal de Isabel II, Interligare, or Lingway, among many others, to present their main research results), access to the Institute's researchers as consultants, participation of company staff in Institute activities, etc.

| Project/Contract | Funding Entity | Industrial Partners |
|---|---|---|
| MOBIUS | FP6: IP | France Telecom, SAP AG, Trusted Labs |
| HATS | PF7: IP | Fredhopper |
| NESSoS | PF7: NoE | Siemens, ATOS |
| ES_PASS(Through an associated group at UPM.) | ITEA2, MITyC | Airbus France, Thales Avionics, CS Systèmes d'Information, Daimler AG, PSA Peugeot Citroen, Continental, Siemens VDO Automotive, EADS Astrium, GTD, Thales Transportation, and IFB Berlin |
| EzWeb | MITyC | Telefónica I+D, Alimerka, Integrasys, Codesyntax, TreeLogic, Intercom Factory, GESIMDE, Yaco, SoftTelecom |
| DESAFIOS-10 | MICINN | BBVA-GlobalNet, LambdaStream, Deimos Space |
| PROMETIDOS | Madrid Regional Government | Deimos Space, Atos Origin, BBVA-GlobalNet, Thales, Telefónica I+D |
| MTECTEST | Madrid Regional Government | Deimos Space |
| SEIF awards | Microsoft SEIF | Microsoft Research |
| PhD Scholarships | Microsoft | Microsoft Research |
| ENTRA | FP7: STREP | XMOS |
| VARIES | FP7: ARTEMIS | Barco NV, HI iberia, IntegraSys, Tecnalia, Sirris, Spicer, Fraunhofer Gesellschaft, Pure-Systems Gmbh, STiftelsen Sintef, Autronica, Franders Mechatronics Technology Centre, Atego Systems, Teknologia Tutkimuskeskus VTT, Mobisoft, HIQ Finland, Softkinetic Sensors, Macq, Metso Automation. |
| 4CaaST | FP7: IP | Telefónica I+D, SAP, France Telecom, Telecom Italia, Ericsson, Nokia-Siemens, Bull SAS, 2nd Quadrant, Flexiant |
| POLCA | FP7: STReP | Maxeler, Recore |
| Contract | AbsInt | AbsInt GmbH |
| Contract | Boeing | Boeing Research & Technology Europe |
| Contract | Telefonica | Telefonica Digital |

*Figure 2.1: Some companies with which the IMDEA Software Institute has collaborated through projects and contracts to date.*


## 2.2 Cooperation with Research Institutions

As a research organization of international reputation and impact, the Institute has developed a network of strong collaborations with universities and other research centers, in the Madrid region and world-wide. Again, an important way in which such cooperation happens is through focused collaborations in the framework of *collaborative projects* funded through competitive calls. However, the Institute has also established *longer-term, strategic partnerships through agreements* with a number of institutions in order to reach objectives that go beyond individual projects. At present the Institute has already signed agreements with the following universities and research centers:

- Universidad Politécnica de Madrid (since November 2007).
- Universidad Complutense de Madrid (since November 2007).
- Universidad Rey Juan Carlos (since January 2008).
- Roskilde University, Denmark (since June 2008).
- Consejo Superior de Investigaciones Científicas (since November 2008).
- Swiss Federal Institute of Technology (ETH) Zurich (since November 2012).
- Microsoft Research (since December 2012, with Joint Research Unit established in 2014).

These agreements establish a framework for the development of collaborations and include the joint participation in and development of graduate programs; the joint use of resources, equipment, and infrastructure; exchange of staff; joint participation in research projects; the association of researchers and research groups with the Institute; or the joint commercialization of technology. In particular, research assistants at the IMDEA Software Institute can follow graduate studies at any of the cooperating Institutions, while funded by the IMDEA Software Institute and Institute faculty collaborate in those graduate programs.

To illustrate the scope and importance for the Institute of these agreements, we offer here some highlights. The agreement with the Universidad Politécnica de Madrid includes provisions for the location of the Institute building in its Montegancedo Science and Technology Park as well as a joint graduate program, instrumented currently as a separate track on *Software Development through Rigorous Methods* in an existing Masters / PhD program at UPM ("MUSS / DSS"). Under the agreement with the Consejo Superior de Investigaciones Científicas, two of its researchers —Cesar Sánchez and Pedro López— are also part of the research staff of the Institute. Under the agreement with Roskilde University, one of its full professors —John Gallagher— is also part-time senior researcher at the Institute. As mentioned before, the agreement with ETH Zurich includes the joint development and commercialization of the ActionGUI technology, from the Institute's Modeling Lab. The Institute also manages for the Regional Government REDIMadrid, the Madrid academic network which connects all the public universities and other research institutions in the Madrid region to each other and to the national and international backbones, and has signed agreements in this context with all such institutions. Finally, the Institute of course also collaborates with the other Institutes in the IMDEA network. As an example, the Institute has secured and coordinates the AMAROUT-I and AMAROUT-II COFUND programs of Marie Curie fellowships, which fund personnel in all the IMDEA Institutes, and provides other services to the IMDEA network.

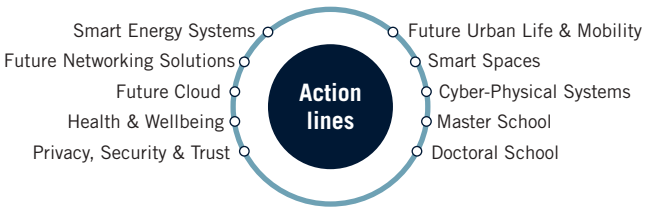
The Institute also has a strong presence in national and international bodies. It is a member of *Informatics Europe*, the organization of all deans, chairs, and directors of the leading Departments and Institutes of Computer Science in Europe, similar to the CRA in the US. In addition, the Institute is a member of ERCIM, the *European Research Consortium for Informatics and Mathematics* through SpaRCIM, the Spanish representative in ERCIM, where Manuel Hermenegildo, IMDEA Software Institute Director, is also the President of the Executive Board.

## 2.3 Association with EIT ICT Labs

In June 2013, IMDEA Software officially became an Associate Partner of EIT ICT Labs, as the first Spanish organization to enter its Pan-European network of seven full national nodes (in Helsinki, Stockholm, Berlin, London, Eindhoven, Paris, and Trento) and two associate nodes (Budapest and Madrid, located at IMDEA Software).

EIT ICT Labs is a *Knowledge and Innovation Community* (KIC) of the European Institute of Innovation and Technology (EIT), which includes some of the leading educational, research and industrial actors in the ICT innovation ecosystem in Europe. Its mission is to combine the educational, research and industrial tools and activities – known as the catalysts – to drive and foster ICT innovation on European scale in the following strategic areas: Smart Energy Systems, Future Networking Solutions, Future Cloud, Health and Wellbeing, Privacy, Security and Trust, Future Urban Life and Mobility, Smart Spaces, and Cyber-Physical Systems. These areas are complemented by an integrated and innovation-driven Master and Doctoral School and a Business Development Accelerator.

One of the key goals of IMDEA Software as the Spanish Associate Member is to promote, motivate and organize the presence of EIT ICT Labs in Spain, and to foster the activity of the Spanish Associate Partner Group (APG) – which includes some of the most prominent players in the ICT innovation arena, such as Telefónica, Indra, Atos, the Technical University of Madrid (UPM) and the Barcelona Supercomputing Center (BSC). Together with these strategic partners, the Institute is working on developing innovation-oriented projects within the framework of EIT ICT Labs, increasing its presence in Spain through interaction with regional and national governments, and boosting and creating synergy between the entrepreneurship initiatives and mechanisms led by the members of the APG and beyond.




Based on the joint work of the partners in the APG during 2013, IMDEA Software has four activities approved and included in the EIT ICT Labs Business Plan for 2014:

- Three research and innovation activities in the fields of Privacy, Security and Trust (project CADENCE), Cyber-Physical Systems (project cPAS), and FI-PPP liaison. More details are provided in Chapter 5.

- Further development of the Madrid Co-Location Center (CLC), hosted in the premises of IMDEA Software, which is the home for the EIT ICT Labs activities and the meetings of the Spanish APG. The CLC is equipped with video-conferencing equipment that allows participation in the EIT ICT Labs activities, as well as with ample office space and meeting facilities to support meetings, outreach and entrepreneurship activities.

- Development of the CLC segment which is a part of the EIT ICT Labs Business Development Accelerator network.

- Launch of the Doctoral Training Center, in cooperation with UPM, which is a part of the EIT ICT Labs educational initiative that allows doctoral and master students to obtain not only a recognized technical education, but also entrepreneurial skills and the opportunity to work with European top research facilities and leading business partners.

## 2.4 High-Speed Communication Infrastructures

The IMDEA Software Institute coordinates the academic and research Internet backbone of the Madrid Region, **REDIMadrid**, funded by the Madrid Regional Government, which currently provides high-speed connections at up to 10 Gps to the universities and research institutes located in the Madrid region.

The IMDEA Software Institute also hosts the new **EIT ICT Labs** top-level node of the Spanish High-speed Research Network Backbone, **RedIRIS-NOVA**, located at the EIT ICT Labs Madrid Co-location Center. This recent expansion of RedIRIS-NOVA has been funded by the Spanish Government in direct support of the EIT ICT Labs associate partnership in Spain. Only two other similar RedIRIS-Nova access nodes currently exist in the Madrid region.

# research



annual report

2013

This chapter describes the key lines of research currently pursued by the scientists of IMDEA Software. A common characteristic of all these lines is the attention to two tightly interrelated aspects: on one hand the development of sound and mathematically rigorous *foundations* which are at the same time oriented towards solving practical problems. On the other hand, the development of well-founded and cost-effective *tools and prototypes*, which are fundamental to both experimentation and for technology transfer towards integrated production-grade systems.


## 3.1 Towards "Greener" Software: Verifying and Controlling Computing Resource Consumption

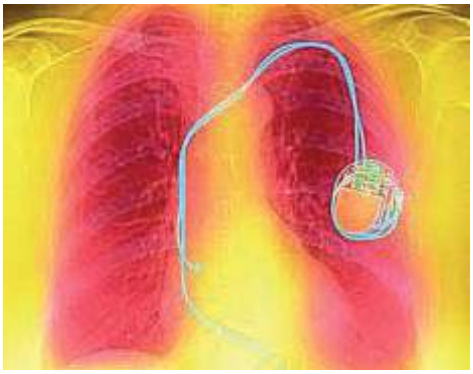
Energy consumption and the environmental impact of computing technologies have become a major worldwide concern. Energy consumption is now a major issue in high-performance computing, distributed applications, and data centers. There is also increased demand for complex computing systems which have to operate on batteries, such as implantable/portable medical devices or mobile phones. The growth of cloud computing-related energy consumption and Internet traffic is not sustainable with the energy efficiency levels of current computing technology.

In spite of the recent rapid advances in power-efficient hardware, most of the potential energy savings are wasted by software that does not exploit these hardware energy-saving features, and by poor dynamic management of tasks and resources. Facing this challenge, the IMDEA Software Institute aims to promote energy efficiency to a first-class software design goal, and, in a more general context, to develop tools that facilitate the production of "greener" devices, i.e., devices that make a certifiably more efficient use of their available *resources* (e.g., energy, execution time, memory, as well as other user-defined resources like network accesses or transactions).

IMDEA Software researchers are working towards achieving radical advances in energy-aware software design and management. These advances include the explicit exploitation of power-efficient features offered by hardware supporting conventional computation models, as well as by emerging approaches such as massively parallel systems and biologically inspired computation models. IMDEA Software has already extended conventional debugging and verification techniques to deal with resource usage properties, and developed automatic optimization techniques that reduce significantly the resource usage of programs, in particular the total execution time and power use.

All the developed techniques are implemented and integrated into IMDEA's state-of-the-art tools, which are demonstrated to industrial collaborators and tested on concrete examples extracted from their application code. The pioneering CiaoPP system provides a general framework for estimating with high precision the resources consumed by a given piece of software and for debugging/certifying such consumption with respect to specifications. The tool is highly adaptable to different languages, hardware, and resources because it is built around a customizable static analyzer with a versatile and well-defined assertion language.

A part of this research on "greener software" is being performed within the European project ENTRA (see Chapters 5 and 7).



## 3.2 Formal Verification of Cyber-Physical Systems

Modern computers are not standalone devices sitting on our desktops, but are increasingly seen embedded in everyday devices, systems and structures such as smart phones, buildings, medical devices and automobiles. The drastic reduction in the cost of sensing, actuating, computing and communication technology has enabled the proliferation of a new genre of engineered systems, referred to as Cyber-Physical Systems (CPS), in which networked embedded processors interact tightly with a physical environment to achieve global complex functionalities.

Cyber-physical systems will be a key enabling technology of the future in tackling societal and economic challenges arising in areas such as manufacturing, communication, infrastructure, energy, health-care, and transportation. Hence, governments around the world including the United States and the European Union have established several funding initiatives to exploit this potential. Cyber-physical systems invariably manifest in safety-critical domains—such as automotive, aerospace and medical devices—so ensuring reliable performance is of utmost importance. However, the state-of-the-art techniques fall short in guaranteeing correct behavior, as is evident from the recent episodes of software recalls in the automotive and medical devices industries to fix bugs. Therefore, the grand research challenge is to build techniques for the development of high-confidence cyber-physical systems.

While formal methods have been successfully applied to the analysis of stand-alone hardware and software, CPS differ from traditional software in the tight interactions with the physical system it controls, and in that CPS run on one or more embedded processors which communicate with each other. Hence, CPS are hybrid systems that encompass both discrete and continuous behaviors owing to the digital components and the physical environments, respectively. The central scientific challenge in CPS formal verification lies in dealing with this unprecedented complexity arising due to the tight coupling of computation, control, and communication.

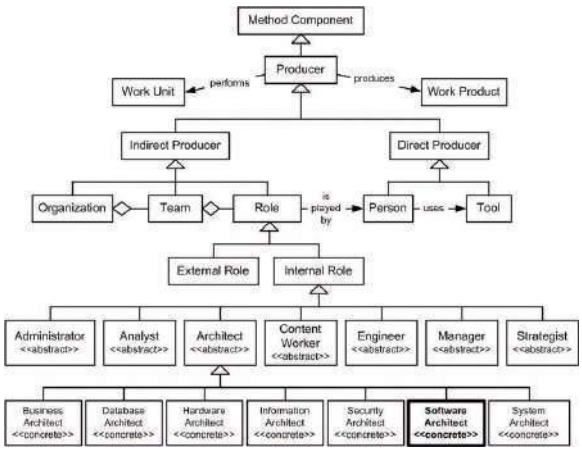
Researchers at the IMDEA Software Institute are actively involved in this exciting new area by focusing on the development of the state-of-the-art technology for verification of cyber-physical systems, particularly, in the early design phase, where reliability has a huge impact on the development cost of the products. The research carried out at IMDEA Software addresses the scalability of current verification techniques by designing novel state-space reduction algorithms and tools. Given the inter-disciplinary nature of the area, this scientific endeavor is carried out in collaboration with experts in control theory, dynamical systems, and formal methods from several institutes and universities in the US and Europe.

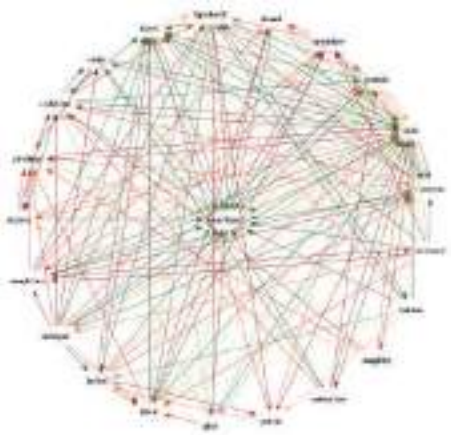
## 3.3 Architecture-Driven Verification: Tackling The Complexity Of Modern Software

The modern information society critically relies on software systems, with some of its most vital processes controlled by software. At the same time, software is notoriously unreliable. This is a consequence of a systemic problem. Recent studies have put the cost of software bugs to the economy of the US alone at $60 billion a year or about 0.6% of GDP. Given the current trends in software development, in the future the cost and dependability problems will only be exacerbated. The growing dependence of modern society on software systems makes this situation unsustainable.

Software verification is an area of computer science that has the potential to resolve this problem: its goal is to ensure the correctness of software by proving that it satisfies a given property in *all* possible situations. Formerly a purely theoretical area, since the year 2000 software verification has experienced a resurgence of interest from practitioners and is now emerging as a cutting-edge approach to improving software quality. Although there is much excitement in the verification area, there is still a huge distance to go before we will be able to verify pieces of software as complex as a modern operating system kernel. This is because the cost-benefit ratio of current verification technology is not good enough to scale it to major software systems. Software verification is currently good at dealing with programs that are either big, but simple, or complicated, but small. Unfortunately, modern software is both big and complicated. IMDEA Software Institute researchers are developing radically new verification methods aiming to overcome this problem.

The hypothesis underlying this research is that the main reason for the inadequacy of the existing verification approaches when dealing with complex software is their generality. The techniques they suggest are based on generic principles that come from properties of programming languages, which allows applying such techniques to arbitrary programs. However, since they cannot take advantage of the particular ways in which programs are



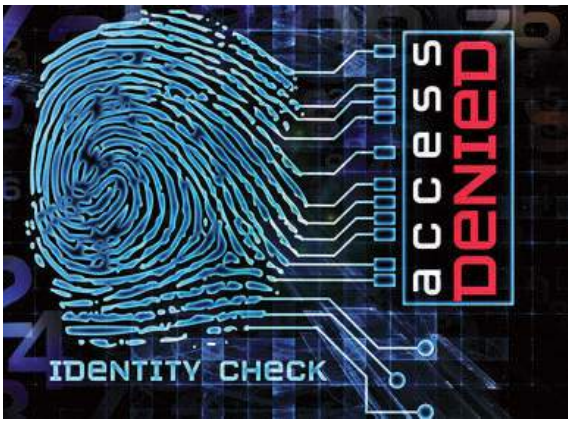
usually written in those languages, they require too much labor and do not scale to big and complicated systems. At the IMDEA Software Institute, we are developing methods and tools for cost-effective verification of real-world systems software by exploiting the way programmers write it: in practice, they stick to informally described patterns, idioms, abstractions and other forms of structure contained in their software, which are together called its *architecture*. IMDEA researchers harness this trend to develop verification methods and tools that are tailored to the architectures used in modern systems software.

### 3.4 Digital privacy

Much of our most private data is collected permanently (for instance through web browsing or networked devices that we carry with us), sent over the air to external third parties, stored in the cloud and redistributed (at best in aggregated form) to other third parties. While the availability of this data opens up tremendous opportunities for society, the economy, and individuals, it also exposes users to potential attacks against their privacy. For the information society to thrive, we need to protect ourselves against such attacks. Unfortunately, our privacy is typically in conflict with requirements on functionality, performance, usability, and cost:

- The release of sensitive information such as medical records, smart-metering data, or browsing habits severely threatens the privacy of users. However, society and the economy benefit from utilizing this data, for example, for computing health statistics, for offering competitive pricing, or for targeted advertisement.

- Mechanisms such as encryption can be used for hiding the content of messages that are exchanged between users. However, without incurring significant traffic overhead, they typically cannot hide features such as the size of the content or the mere fact that a message has been exchanged.

- Techniques such as caching greatly improve the browsing experience by increasing the responsiveness of web browsers. However, they also introduce variations into the response times of requests, which can be observed and exploited to recover private information about users.

In the presence of such conflicting requirements, perfect privacy is impossible or simply too expensive to achieve. Rather, the challenge is to identify trade-offs in which systems meet their requirements and at the same time protect the privacy of their users to a sufficient degree.

Researchers at the IMDEA Software Institute are working on the next generation of tools for ensuring the privacy of real systems. The first research thrust is to develop meaningful measures and metrics of privacy that allow users and analysts to agree on what it means for data to be "sufficiently" protected. The second research thrust is to develop tools that enable to guaranteeing that the deployed systems comply with this degree of protection. A key requirement of these approaches is that they enforce privacy preventively, that is, before the program is deployed and under attack.

Emblematic applications that have been developed at the IMDEA Software Institute are a tool that ensures the privacy of smart metering protocols, while at the same time allowing for relevant information to be extracted, and a tool that enables to quantifying the information leaked by features of web-browsing traffic.

## 3.5 Fighting Malware in Cybercrime and Targeted Attacks

The last decade has seen a radical evolution in the quantity and type of Internet threats. Gone are the days of occasional attacks, launched by highly technical individuals whose motivation was boasting their technical skills. Nowadays, Internet attacks are constantly being launched by coordinated groups such as criminal gangs, hacktivist networks (e.g., Anonymous, LulzSec), and governments, motivated by profit, political objectives, and national-level interests.

Two fundamental reasons are at the core of this transformation. First, the Internet has removed physical barriers. Attackers can easily meet and coordinate remotely. Physical access to the victims is no longer needed, e.g., bank assets can be stolen without breaking into offices, governmental websites can be taken offline as protest, and critical infrastructures can be sabotaged without entering their facilities. Second, every Internet user and Internet-connected device (such as hosts, servers, mobile and embedded devices, critical infrastructures) has become a target, with different types of attackers focusing on different target types.

Two main threats dominate this environment: *cybercrime* and *targeted attacks*. Cybercriminals compromise large numbers of Internet-connected hosts, and develop ways for monetizing those compromised hosts and their users. They focus on economies of scale; for them, any compromised host has some, even if low, value. Even if the value of each target is low, their large number makes the profit worth. Compromised hosts are valued for the user data they hold or as assets. Those assets can be used (or bought and sold) to launch malicious activities such as sending spam, launching denial-of-service (DoS) attacks, mining virtual currencies (i.e., Bitcoins), faking user clicks on online advertisements (i.e., click-fraud), or simply as stepping stones to hide the attacker's real location. Users of compromised hosts can be phished to steal their credentials and can be convinced to buy licenses of rogue software.

Targeted attacks differ from cybercrime in that they focus on high-value targets. Targeted attacks have become a focus of the security industry, which has coined a new term for them: *Advanced Persistent Threats* (APTs) that refers to highly determined, well-funded, cyber-attackers, who persistently target an individual, a group, or an infrastructure. High-value targets include politicians, journalists, activists, enterprises, and critical infrastructures.

At the core of cybercrime and targeted attacks is the attacker's ability to install malicious programs (i.e., malware) on Internet-connected computers without the owner's informed consent. Malware includes bots, viruses, RATs, trojans, rootkits, fake software, and spyware. Malware enables attackers to establish a permanent presence in a compromised computer and to leverage that computer for their nefarious goals.

Researchers at the IMDEA Software Institute are developing novel techniques for analyzing malware and developing defenses for protecting users against malware and the cyberattacks in which malware is used. This research is being performed in part within the European MALICIA and Cadence projects (see Chapter 5).




## 3.6 Cryptography for Next Generation Cloud Computing


Cloud computing is a fast growing paradigm in which users lease computation resources from powerful service providers. Virtual machines, remote storage, email, web-content, databases are only some examples of services that are nowadays outsourced to the Cloud. This paradigm is very appealing to individuals and businesses due to its significant benefits: reduced IT costs, increased mobile productivity, convenient access to remote resources from multiple devices, different geographic locations, etc. The downside of cloud computing is that keeping a clear control over the data and the computations that are outsourced to the Cloud is becoming more difficult. This new working scenario exposes users to faults and attacks that are out of the users control and can seriously threaten privacy and integrity of data and computations delegated to the Cloud. As an example, if the cloud provider falls under an attack, this may cause the tampering or the leakage of sensitive users data (such as credit cards information or medical records) with devastating consequences.

To address these issues, researchers at the IMDEA Software Institute are working on shaping the next-generation cloud infrastructure in which users will be able to outsource their data and computations to untrusted providers in a fully reliable manner. The main goal of this research is to protect cloud users with respect to privacy and integrity. For privacy, cloud providers should be able to perform the operations delegated by the users without learning any unauthorized information about the users data. Importantly, such strong form of privacy also prevents any attacker that would penetrate into the Cloud system from learning the content of the data therein stored. For integrity, the key idea is to enable users to verify that cloud providers have indeed operated correctly (for example, to check that the original data has not been modified without the user's authorization) without, however, spending too many resources to perform this check.

To achieve these goals, our research builds on cryptography –the science of developing methods for protecting information and communication against misbehaving parties. While initially focused on encrypted communications in the military or diplomatic domain, modern cryptography has expanded considerably and already plays a central role in the Internet. To play a similar role in the Cloud, one must design new, advanced, cryptographic mechanisms that can address privacy and integrity in this new scenario. Homomorphic encryption, verifiable computation protocols and zero-knowledge proofs are some examples of cryptographic primitives useful in this context.

Researchers at the IMDEA Software Institute are therefore investigating novel cryptographic techniques that can achieve these advanced functionalities so that users will be able to outsource data and computations to the Cloud, and at the same time not to risk for their privacy and integrity.

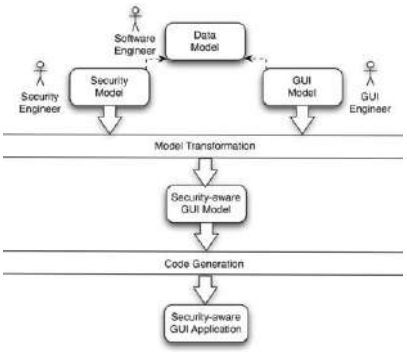
## 3.7 Secure Data Management: Model-to-Code Automation

Data-management applications are focused on the so-called CRUD actions that create, read, update, and delete data. Such applications are often implemented as multi-tier systems where the application manipulates data stored in a database and interacts with users through a graphical interface (GUI). When the data managed is sensitive, then security is a concern.

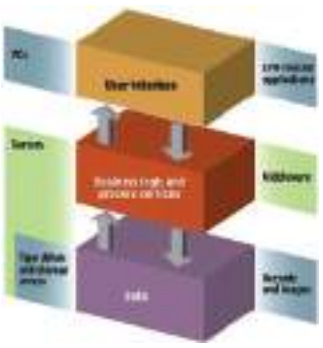
Implementing access control over data is nontrivial. Fine-grained access control policies may depend not only on the user's credentials but also on the satisfaction of constraints on the state of the persistence layer, i.e., on the values of stored data items. In such cases, authorization checks are typically implemented programmatically, by directly encoding them at appropriate places in the application. This is cumbersome, error prone, and scales poorly. Moreover, it is difficult to audit and maintain as the access checks are spread throughout the code and security policy updates require code changes.

IMDEA Software's scientists are creating a methodology for the model-driven development of secure data-management applications. It consists of formal languages for modeling multi-tier systems, and tools for generating these systems. Within the methodology, a secure data-management application is modeled using three interrelated models: a data model, a security model, and a GUI model. The heart of this methodology is a well-defined model-transformation function that automatically lifts the policy that is specified in the security model to the GUI model. The resulting GUI model is security aware.

Security-aware GUI models are platform independent and can be mapped to implementations employing different technologies, including desktop applications, web applications, and mobile applications. As a part of the Institute's research, the ActionGUI Toolkit (http://www.actiongui.org) was developed , which automatically generates Java web applications from security-aware GUI models. The ActionGUI Toolkit features model




*Model-driven development of security-aware GUIs.*



*3-tier architecture*

*ActionGUI: An example of a security model (screenshot)*

editors for constructing and manipulating data, security, and GUI models. Moreover, it implements appropriate model transformation to generate security-aware GUI models. Finally, it includes a code generator that, given a security-aware GUI model, automatically produces a Java web application, ready to be deployed in a web application container (e.g., Glassfish or Tomcat).

Overall, the contribution of this research is two-fold. First, the developed methodology offers model-driven engineering's purported benefits for data-management systems. By working with models, designers can focus on the application's data, behavior, security, and presentation, independently from the different, often complex, technologies that are used to implement them. Second, the use of model transformations leads to modularity and separation of concerns: the GUI model and the security model can be changed independently and by different developers, if desired. This avoids the problems associated with brittle, error prone, hardcoded security policies that are difficult to maintain and audit.

## 3.8 Concurrent Software Reliability

In modern economies, market competitiveness and public service quality have turned software ubiquitous. Nowadays, computer systems are present in virtually all devices and systems that influence our daily lives, from the control of critical infrastructures like airplanes or energy plants, to small devices like phones and televisions. Software not only has enabled new devices and solutions, but at the same time most devices and systems that existed before our software intensive era have been redesigned with a larger dependency on software.

At the same time, the risk of pitfalls caused by software errors has surged due to the higher complexity of software systems and its wider presence and impact in all products. Software reliability techniques are key to mitigate these risks. The predominant approach to achieve reliability is testing, in which a piece of software is run with the goal to observe whether the execution matches its intended behavior and functionality.

*Satellites have to be autonomous up to a certain degree. The programs running in their computers continuously monitor for deviations from their scheduled trajectories and take the appropriate decisions to correct them.*



Verification is an alternative approach in which the software is studied statically using mathematical techniques that intend to either find an error before the execution or guarantee the absence of such errors. Testing and formal verification are complementary techniques. Testing is readily applicable but necessarily incomplete in the sense that it cannot provide guarantees about absence of errors in programs of real-world size. Verification, on the other hand, provides higher guarantees but requires more sophisticated methods and resources (both computing and human).

At the same time, most software-based systems are becoming increasingly concurrent. One reason is the advent and popularization of multi-core and multi-processor hardware. Another reason is that many systems are intrinsically distributed, in the sense of being physically built from multiple independent components that run simultaneously, both at a small scale or even at Internet scale. Reasoning about concurrent systems requires considering a large number of interactions between the constituent components. This complexity jeopardizes the effectiveness of testing. Hence, verification is nowadays perceived as the best alternative for software reliability. New verification methods are necessary for the new challenges of modern concurrent software verification at several levels.

First, formal verification requires not only to consider the system at hand but also the description of what the intended behavior is. Specification languages need to be both humanly usable and tractable by computers. Second, automatic verification techniques are desirable because they do not require human ingenuity and intervention, and can be applied to third-party software. There is a challenge to design automatic techniques that cover useful cases of concurrent software and scale to realistic sizes. On the other hand, deductive techniques require human intervention but can potentially handle more sophisticated cases. The overall goals is to provide sufficient automation to minimize the human intervention and increase the productivity to handle industrial software of realistic size.

Researchers at the IMDEA Software Institute are actively involved in the development of novel automatic and semi-automatic software verification techniques, specifically designed to deal with the challenges of concurrent software verification.

$R_{rng}^{[x]} = R_{all}$

$\wedge\ R_{all} = R_{rng}^{[x]} \cup \bigcup_{j \in 1..3} R_j^{[x]} \quad \wedge \quad \bigcup_{j \in T_{ID} - \{x\}} R_3^{[j]}$

$\cup\ R_3^{[x]} \quad \wedge \quad R_3^{[x]} \# R_{rng}^{[x]} \quad \left( \wedge\ \text{Graph}(\text{root}, \right.$

Inv

Inv

$r) \wedge n \in r \rightarrow \text{Graph}(n, r') \wedge r' \subseteq r$ Lex (Lemma

$(x), r) \longrightarrow \bigcup_{i \in 1..3} R_i^{[x]} \subseteq r$ (Construc + HexPred)

$= R_2^{[x]} = \text{emp}$ (Teo)

Si $n \in R_3^{[x]}$, listo.

$\text{Inv}^{[x]}$ Sabemos q' $n \in r \rightarrow n \in \bigcup_{i \in 1..3} R_j^{[x]} \vee n \in$

$n \in R_1^{[x]} \cup R_2^{[x]}$. Luego $n \in stk^{[x]}$ (por 3)

Nad

e remueve de $stk^{[x]}$ solo si $n \in R_3^{[x]}$

ras, out_end $\rightarrow stk^{[x]}$ empty $\therefore$ out_end $\rightarrow R_1^{[x]} \cup R_2^{[x]}$

$[x]$ (Construc

# people



annual report 2013

The IMDEA Software Institute strives towards the level of excellence and competitiveness of the highest-ranked institutions worldwide. Success in this goal can only be achieved by recruiting highly-skilled personnel for the scientific teams and support staff. The Institute considers this one of the key critical factors and measures of its success.

Competition for talent in Computer Science is extremely high at the international level, since essentially all developed countries have identified the tremendous impact that IT has on the economy and the crucial competitive advantage that attracting truly first class researchers entails. To meet this challenge, the Institute offers a world-class working environment that is competitive with similar institutions in Europe and in the US and which combines the best aspects of a university department and a research laboratory.

Hiring at the Institute follows internationally-standard open dissemination procedures with public, international calls for applications launched periodically. These calls are advertised in the appropriate scientific journals and at conferences in the area, as well as in the Institute web page and mailing lists. Appointments at (or promotion to) the Assistant Professor, Associate Professor, and Full Professor levels (i.e., tenure-track hiring, tenure, and promotion decisions) are approved by the Scientific Advisory Board. In addition to faculty positions, the Institute also has its own programs for visiting and staff researchers, post-docs, graduate scholarships, and internships. In all aspects related to human resources, the Institute follows the recommendations of the European Charter for Researchers and a Code of Conduct for their Recruitment (http://ec.europa.eu/), which it has duly signed.

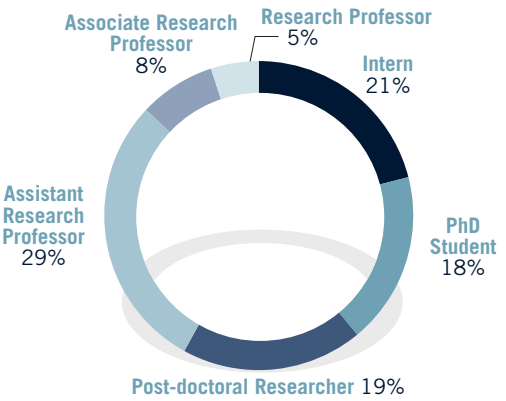



*Figure 4.1. Type of position applied for.*

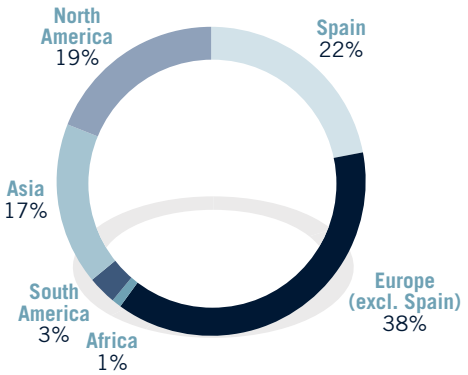



*Figure 4.2. Location of previous institution for applicants at or above the postdoc level (by continent + Spain).*

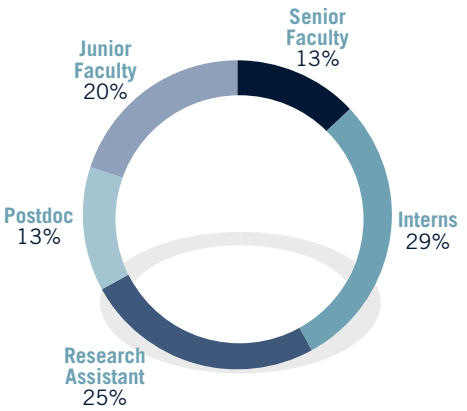



*Figure 4.3. Type of position, all researchers.*

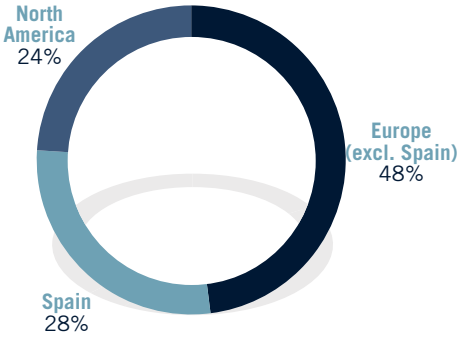



*Figure 4.4. Where PhD was obtained (by continent + Spain).*

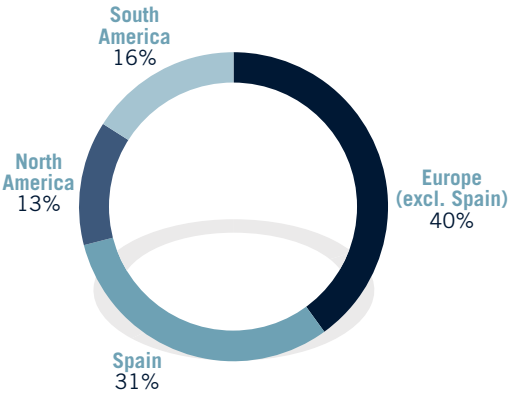



*Figure 4.5. Location of previous institution, all (by continent + Spain).*

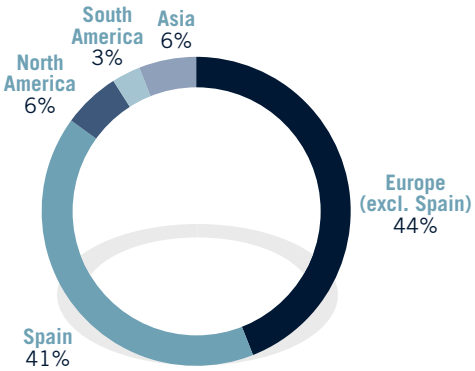



*Figure 4.6. Nationality of researchers at or above postdoc level (by continent + Spain).*

## Applications

Figure 4.1 shows the proportions of applications received for each category during 2013: associate professors (senior researchers), assistant professors (junior researchers), postdoctoral researchers, research assistants, and interns. Figure 4.2 displays the location (by continents) of the institutions in which the applicants were at the time of application (for senior, junior, and postdoctoral positions). Spain is highlighted separately from the rest of Europe to provide a finer view of the data (level of internationalization).

## Status

In 2013, the scientific staff of the Institute was composed of eight senior faculty (full or associate professors, one part-time), thirteen junior faculty (six non tenure-track), eight postdoctoral researchers, and sixteen research assistants (PhD candidates). Eighteen interns spent a variable length of time (from one month to a year) at the Institute collaborating with the faculty members. Figure 4.3 shows the proportions of each category at the end of 2013 (where 33% were faculty members vs. 67% non-faculty). Figure 4.4 summarizes where these researchers obtained their PhD (by continents plus Spain), and Figure 4.5 shows the location where the Institute researchers were working previously to joining IMDEA. Finally, Figure 4.6 presents the nationalities of researchers at or above the postdoc level.

# faculty

## Manuel Hermenegildo

Research Professor and
Scientific Director

Manuel Hermenegildo received his Ph.D. degree in Computer Science and Engineering from the University of Texas at Austin, USA, in 1986. Since January 1, 2007 he is Full Professor and Scientific Director of the IMDEA Software Institute. He is also a full Prof. of Computer Science at the Tech. U. of Madrid, UPM. Previously to joining the IMDEA Software Institute he held the P. of Asturias Endowed Chair in Information Science and Technology at the U. of New Mexico, USA. He has also been project leader at the MCC research center and Adjunct Assoc. Prof. at the CS Department of the U. of Texas, both in Austin, Texas, USA. He has received the Julio Rey Pastor Spanish National Prize in Mathematics and Information Science and Technology and the Aritmel National prize in Computer Science, and he is an elected member of the Academia Europaea. He is also one of the most cited Spanish authors in Computer Science. He has published more than 200 refereed scientific papers and monographs and has given numerous keynotes and invited talks in major conferences in these areas. He has also been coordinator and/or principal investigator of many national and international projects, area editor of several journals, and chair and PC member of a large number of conferences. He served as General Director for the research funding unit in Spain, as well as member of the European Union's high-level advisory group in information technology (ISTAG), and of the board of directors of the Spanish Scientific Research Council and the Center for Industrial and Technological Development, among other national and international duties.

### Research Interests

His main areas of interest include programming language design and implementation; abstract interpretation-based program analysis, verification, debugging, and optimization; logic and constraint programming; parallelizing compilers; parallel and distributed processing.

## Manuel Carro

Associate Research Professor and Deputy Director

Manuel Carro received his Bachelor degree in Computer Science from the Technical University of Madrid (UPM), and his PhD degree from the same University in 2003. He is currently Associate Research Professor and Deputy Director at the IMDEA Software Institute, and an Associate Professor at the Technical University of Madrid. He has previously been representative of UPM at the NESSI and INES technological platforms, and is now representative of UPM at SpaRCIM and deputy representative of IMDEA Software at ERCIM and Informatics Europe. He has published over 70 papers in international conferences and journals, some of which merited the "Best Conference Paper" award. He has been organizer and PC member of many international conferences and workshops and participated in research projects at the regional, national, and European level. He was UPM's principal investigator for the S-Cube European Network of Excellence. He has completed the supervision of three PhD thesis and is actively supervising another one.

### Research Interests

His interests span several topics, including the design and implementation of high-level (logic- and constraint-based) programming languages for improving the quality of software production, the analysis of service-based systems, and the effective usage of formal specifications in the process of teaching programming. He has long been interested in parallel programming and parallel implementations of declarative languages, and visualization of program execution.

## Gilles Barthe

Research Professor

Gilles Barthe received a Ph.D. in Mathematics from the University of Manchester, UK, in 1993, and an *Habilitation à diriger les recherches* in Computer Science from the University of Nice, France, in 2004. He joined the IMDEA Software Institute in April 2008. Previously, he was head of the Everest team on formal methods and security at INRIA Sophia-Antipolis Méditerranée, France, and a member of the Microsoft Research-INRIA Joint Centre. He also held positions at the University of Minho, Portugal; Chalmers University, Sweden; CWI, Netherlands; University of Nijmegen, Netherlands. He has published more than 100 refereed scientific papers. He has been coordinator/principal investigator of many national and European projects, and served as the scientific coordinator of the FP6 FET integrated project "MOBIUS: Mobility, Ubiquity and Security" for enabling proof-carrying code for Java on mobile devices (2005-2009). In 2012, he was a PC member of several conferences (POST, MFCS, ASE-Tools, Tools Europe, and STM), and served as PC chair of ESSoS.

### Research Interests

Gilles' research interests include program verification, programming languages, software and system security, cryptography, privacy, and foundations of mathematics and computer science. His recent work focuses on computer-aided cryptographic proofs.

## Anindya Banerjee

### Research Professor

Anindya Banerjee received his PhD from Kansas State University, USA, in 1995. After his PhD, Anindya was a postdoctoral researcher, first in the Laboratoire d'Informatique (LIX) of École Polytechnique, Paris and subsequently at the University of Aarhus. He joined the IMDEA Software Institute Institute in February 2009 as Full Professor. Immediately prior to this position, Anindya was Full Professor of Computing and Information Sciences at Kansas State University, USA. He was an Academic Visitor in the Advanced Programming Tools group, IBM T. J. Watson Research Center in 2007 and a Visiting Researcher in the Programming Languages and Methodology group at Microsoft Research in 2007–2008. He was a recipient of the Career Award of the US National Science Foundation in 2001. He is an associate editor of the journal Higher-Order and Symbolic Computation.

#### Research Interests

Anindya's research interests lie in language-based computer security, program analysis and verification, program logics, concurrency, programming language semantics, abstract interpretation and type systems. His primary research activities over the past couple of years have centered around automatic and interactive verification of properties of pointer-based programs and in verification of security properties of such programs.

## Juan José Moreno-Navarro

### Research Professor and Director for International and Industrial Relations

Juan José Moreno-Navarro received his Ph.D. degree in Computer Science from the Technical U. of Madrid (UPM), Spain in 1989. He developed a large part of his Ph.D. at RWTH Aachen (Germany). He has been Full Professor at the UPM Computer Science Department since 1996 and joined the IMDEA Software Institute upon its foundation. He served as Deputy Director up to 2008. Currently he is Director of International and Industrial Relations. He has published more than 100 papers in international conferences, books, and journals. He has organized, served in program committees, and given invited talks and tutorials in many conferences in the IST field.

He has been actively involved in research and university policy, serving as General Director for University Policies (Ministry of Education, 2009-2012), General Director for Technology Transfer and Enterprise Development (Ministry of Science and Innovation, 2009) and General Director for Planning and Coordination (Ministry of Science and Innovation, 2008-2009). During this period he has been chairman of CNEAI (Spain's Researcher Activity Evaluation Agency), has been involved in the setting up of several research infrastructures, secretary of the Spanish University Council and of the Spanish Science and Technology Council, and member of the steering board of several foundations (ANECA, UIMP, CENER-Ciemat, Universidad.es, CSIC, ISCIII, IDAE, etc.)

He has been the founding director of SpaRCIM. He has been responsible for the Spanish ICT research program, in charge on International Relations for IST, FP6 IST Committee member, and Spanish National Contact Point for the Spanish Ministry of Education and Science. Currently he is chair of the Spanish Society of Software Engineering, general chair of the Spanish Conference of Informatics 2013, and coordinator of the Spanish Turing Year.

#### Research Interests

His research interests include all aspects related to declarative and rigorous software development technologies. This includes software development techniques, specially specification languages, automatic generation of code (programming from specifications), and software services description. His interests also include the integration of functional and logic programming. He has led the design and implementation of the language BABEL and took part in the activities of the international committee involved in the design of the language Curry. He is also currently involved in scientific policy analysis, bibliometry, and research impact evaluation and analysis.

## John Gallagher

### Research Professor (part-time)

John Gallagher received the B.A. (Mathematics with Philosophy) and Ph.D. (Computer Science) degrees from Trinity College Dublin in 1976 and 1983 respectively. He held a research assistantship in Trinity College (1983-4), and post-doc appointments at the Weizmann Institute of Science, Israel (1987-1989) and Katholieke Universiteit Leuven, Belgium (1989). From 1984-1987 he was employed in research and development in a software company in Hamburg, Germany. Between 1990 and 2002 he was a lecturer and later senior lecturer at the University of Bristol, UK. Since 2002 he has been a professor at the University of Roskilde, Denmark, where he is leader of the research group Programming, Logic and Intelligent Systems and the Experience Lab as well as (part-time) Professor and holds a dual appointment at the IMDEA Software Institute since February 2007. He is a member of the executive committee of the Association of Logic Programming (2008-2011) and of the steering committee of the ACM SIGPLAN workshop series on Partial Evaluation and Program Manipulation (PEPM). He is an area editor for the journal Theory and Practice of Logic Programming. He has published approximately 50 peer-reviewed papers which have over 1200 citations.

#### Research Interests

His research interests focus on program transformation and generation, constraint logic programming, rewrite systems, temporal logics, semantics-based emulation of languages and systems, analysis and verification of energy consumption of programs and other properties, and has participated in and led a number of national and European research projects on these topics.

## Manuel Clavel

### Associate Research Professor

Manuel Clavel received his Bachelor's degree in Philosophy from the Universidad de Navarra in 1992, and his Ph.D. from the same university in 1998. Currently, he is an Associate Research Professor at the IMDEA Software Institute, as well as an Associate Professor at the Universidad Complutense de Madrid. He was Deputy Director from 2008 until April 2011. During his doctoral studies, he was an International Fellow at the Computer Science Laboratory of SRI International (1994 - 1997) and a Visiting Scholar at the Computer Science Department of Stanford University (1995 - 1997). His Ph.D. dissertation was published by the Center for the Study of Language and Information at Stanford University. Since then, he has published over 30 refereed scientific papers. He has also been involved in the supervision of 3 Ph.D. students (1 completed).

#### Research Interests

His research focuses on rigorous, tool-supported model-driven software development, including: modeling languages, model transformation, model quality assurance, and code-generation. Related interests include specification languages, automated deduction, and theorem proving.

## César Sánchez

Associate Research Professor

César Sánchez received his Ph.D. degree in Computer Science from Stanford University, USA, in 2007, studying applications of formal methods for guaranteeing deadlock-freedom in distributed algorithms. After a post-doc at the University of California at Santa Cruz, USA, César joined the IMDEA Software Institute in 2008, becoming also a Scientific Researcher at the Spanish Council for Scientific Research (CSIC) in 2009. In 2013 he was promoted to Associate Professor at the IMDEA Software Institute. César holds a degree in Ingeniería de Telecomunicación (MSEE) from the Technical University of Madrid (UPM), Spain, in 1998. Funded by a Fellowship from La Caixa, he moved to Stanford University, USA, receiving a M.Sc. in Computer Science in 2001, specializing in Software Theory and Theoretical Computer Science. César is a recipient of the 2006 ACM Frank Anger Memorial Award. He keeps active collaborations with research groups in the USA and Europe.

### Research Interests

César's general research interest are based on applications of logic for the development, understanding and verification of computational devices. In particular, formal methods for reactive systems with emphasis on the development and verification of concurrent, embedded and distributed systems. His foundational research includes the temporal verification of concurrent datatypes, runtime verification, and rich specification languages extending temporal logics.

## Pierre Ganty

Assistant Research Professor

Pierre joined the IMDEA Software Institute in the Fall 2009 after completing a nearly two year postdoc at the University of California, Los Angeles (UCLA). He holds a joint PhD degree in Computer Science from the University of Brussels (ULB), Belgium and from the University of Genova (Unige), Italy that he obtained late 2007. He is the author of over 30 publications including 7 journal and 17 conference papers accumulating more than 320 citations. He is the principal investigator of the Spanish national project Paran'10 (2011-2013) on the verification of parameterized systems. He has supervised 7 internships at the IMDEA Software Institute. In 2013, he served on the program committee of the international venues VMCAI (Verification, Model-Checking and Abstract Interpretation) and RP (Reachability Problems).

### Research Interests

Pierre's research is focused on the design, complexity study and implementations of fully automated analysis techniques for systems with infinitely many states. Examples of such infinite state systems include sequential programs over unbounded data type, Internet of Things systems, communication protocols or event-based programs. In each of the previous example, there is an unbounded dimension: the data domain, the number of processes or the number of events; which is best modeled using an infinite state system.

## Aleks Nanevski

Assistant Research Professor

Aleks received his Ph.D. degree in Computer Science from Carnegie Mellon University, USA in 2004. After holding postdoctoral positions at Harvard University (USA), and Microsoft Research, Cambridge (UK), Aleks joined the IMDEA Software Institute in September 2009. Prior to the PhD, Aleks finished his undergraduate studies in Computer Science at the University of Skopje, Macedonia in 1995.

### Research Interests

Aleks' research is in the design and implementation of programming languages that facilitate verification of various program properties, ranging from type and memory safety, lack of memory leaks or information leaks, all the way to full functional correctness. His languages and systems unify programming and specification with automated and interactive theorem proving, via a common foundational framework of type theory. He is particularly interested in verifying programs that combine modern higher-order linguistic features such as higher-order functions, polymorphism, abstract types, objects and modules, with imperative ingredients such as pointer arithmetic, pointer aliasing, unstructured control flow, and concurrency.

## Alexey Gotsman

Assistant Research Professor

Alexey Gotsman received his Ph.D. degree in Computer Science from University of Cambridge, UK in 2009. During his Ph.D. studies, Alexey interned at Microsoft Research Cambridge, UK and Cadence Berkeley Labs, USA. He was a postdoctoral fellow at Cambridge before joining IMDEA in September 2010. Prior to his Ph.D., Alexey did his undergraduate and master studies in Applied Mathematics at Dnepropetrovsk National University, Ukraine, interning at the University of Trento, Italy in the process. He has received the prestigious Microsoft Research SEIF award to work on specifying and validating components on memory models of mobile platforms.

### Research Interests

Alexey's research interests are in software verification, with particular focus on concurrent systems software. He is interested in developing both logics for reasoning about programs and automatic tools for verifying them.

## Boris Köpf

Assistant Research Professor

Boris joined the IMDEA Software Institute in September 2011 after completing a post-doc at the Max Planck Institute for Software Systems (MPI-SWS). He received a Ph.D. degree from ETH Zurich in 2007, investigating formal methods for countering side-channel attacks. Before that, he studied mathematics at the Universidad de Chile, the Universidade Federal de Campinas, and the University of Konstanz, from which he received a M.Sc. degree. He is an alumnus of the German National Academic Foundation.

### Research Interests

Boris' research focuses on the foundations of computer security. In particular, he is interested in quantitative notions of security, and in techniques for computing corresponding guarantees for real systems. He applies his research to the analysis of side-channel attacks (and countermeasures) and to privacy-preserving data publishing.

## Juan Caballero

Assistant Research Professor

Juan Caballero joined the IMDEA Software Institute as an Assistant Research Professor in November 2011, after receiving his Ph.D degree in Electrical and Computer Engineering from Carnegie Mellon University, USA. Prior to joining the IMDEA Software Institute, Juan was a visiting graduate student researcher at University of California, Berkeley for two years. He was awarded the La Caixa fellowship for graduate studies in 2003. Juan also holds a M.Sc. in Electrical Engineering from the Royal Institute of Technology (KTH), Sweden, and a Telecommunications Engineer degree from the Technical University of Madrid (UPM), Spain.

### Research Interests

Juan's research focuses on computer security, including security issues in systems, software, and networks. He enjoys designing program analysis techniques, specially techniques that work directly on program binaries. He applies those techniques for analyzing security properties of benign programs, as well as for malware analysis. In addition, he is interested in network security, the economic aspects of cybercrime, applying machine learning for security, and software engineering.

## Pavithra Prabhakar

Assistant Research Professor

Pavithra Prabhakar obtained her doctorate in Computer Science from the University of Illinois at Urbana-Champaign in 2011, from where she also obtained a masters in Applied Mathematics. She has a masters degree in Computer Science from the Indian Institute of Science, Bangalore and a bachelors degree from the National Institute of Technology, Warangal, in India. She has been on the faculty of IMDEA Software since 2011, and spent the year between 2011-2012 at the California Institute of Technology as a CMI (Center for Mathematics of Information) fellow on leave of absence from IMDEA. She is the recipient of the Sohaib and Sara Abbasi fellowship from the University of Illinois and M.N.S Swamy medal from the Indian Institute of Science for the best master's thesis. Her paper at the ACM Hybrid Systems: Computation and Control Conference 2012 received a honorable mentions award.

### Research Interests

Pavithra's main research interest is the formal analysis of cyber-physical systems. Her research is at the intersection of formal methods, hybrid systems and control theory with applications in robotics and aeronautics. Her research aims at building scalable analysis methods for systems consisting of mixed discrete continuous behaviors. To this end, she investigates foundational aspects such as decidability of verification problems and pre-orders for approximation; and develops algorithmic verification techniques and tools based on state-space reduction methods such as predicate abstraction and counter-example guided abstraction refinement. She has published widely in formal methods and hybrid systems conferences.

## Pedro López-García

Researcher

Pedro López-García received a MS degree and a Ph.D. in Computer Science from the Technical University of Madrid (UPM), Spain in 1994 and 2000, respectively. In May 28, 2008 he obtained a Scientific Researcher position at the Spanish Council for Scientific Research (CSIC) and joined the IMDEA Software Institute. Immediately prior to this position, he held associate and assistant professor positions at UPM and was deputy director of the Artificial Intelligence unit at the Computer Science Department. He has published about 40 refereed scientific papers, many of them at conferences and journals of high or very high impact. He served as the scientific local coordinator of the european project ES_PASS "Embedded Software Product-based ASSurance," and is currently the principal investigator at the institute of the european FP7 FET project ENTRA "Whole-Systems Energy Transparency." He has also participated as a researcher in many other regional, national, and international projects.

### Research Interests

His main areas of interest include energy-aware software engineering; automatic analysis and verification of non-functional program properties such as resource usage (user defined, energy, execution time, memory, etc.), non-failure and determinism; performance debugging; abstract interpretation; (automatic) granularity analysis/control for parallel and distributed computing; profiling; combined static/dynamic verification and unit-testing; type systems; tree automata; constraint and logic programming.

## Dario Fiore

Assistant Research Professor

Dario joined the IMDEA Software Institute as an Assistant Research Professor in November 2013, after holding postdoctoral positions at Max Planck Institute for Software Systems (Germany), New York University (USA), and Ecole Normale Supérieure (France). Dario obtained a Ph.D. in Computer Science from University of Catania (Italy) in 2010 under the supervision of Dario Catalano. During his PhD, he was also a visiting student at IBM T.J. Watson research center and New York University (USA).

### Research Interests

Dario's research interests focus mainly on Cryptography and Security. More specifically, he works on the design of provably-secure cryptographic primitives and protocols. Some of the topics he works on include: secure delegation of data and computation to the Cloud, homomorphic authentication, zero-knowledge proof systems, functional encryption, protocols for anonymous communication, and foundations of cryptography.

## Mark Marron

Researcher

He joined the IMDEA Software Institute as a postdoctoral researcher in June 2008. Following four months as a Visiting Researcher at Microsoft Research in Redmond he returned to IMDEA as a Researcher. Recent research highlights include the release of a robust and scalable heap analysis toolkit (Jackalope analysis tools) for public use and the award of a prestigious Microsoft Innovation Award for work on heap analysis and memory use.

### Research Interests

His research interests are on developing practical techniques for modeling program behavior and using this information to support error detection and optimization applications. His work to date has focused on the development of static analysis for the program heap which infers region, sharing, footprint and heap based data dependence information. More recent work has focused on using the information extracted by the analysis to support program parallelization, memory management, error detection, and software engineering applications.

## Laurent Mauborgne

Researcher

Laurent Mauborgne received his Ph.D. in Computer Science from École Polytechnique, France, in 1999, and an Habilitation a diriger les recherches from University Paris-Dauphine (France) in 2007. He has been assistant professor at the École Normale Supérieure, Paris, since 2000, and associate director of computer science studies there since 2006. He was also part-time professor at École Polytechnique. He was invited to spend a year at the IMDEA Software Institute in August 2009.

He published 16 refereed papers in international conferences and 3 papers in journals. He gave courses in research summer schools and participated in the European projects DAEDALUS and ES_PASS. He was program committee member of the Static Analysis Symposium for 4 years. He is one of the authors of the Astrée analyzer, a tool that proved the absence of runtime errors in critical avionic codes.

### Research Interests

The research of Laurent Mauborgne is focused on static analysis of programs and abstract interpretation. The goal is to develop theoretical as well as practical tools to analyze the behaviors of programs. This includes proving safety or temporal properties, optimizing compilation and computing resource usage. Among the recent subjects, he studied the cooperative combination of analyzers in different frameworks.

## Michael Emmi

Researcher

Michael received his Ph.D. in Computer Science from the University of California, Los Angeles (UCLA) in 2010. Michael joined the IMDEA Software Institute in September 2013, following a post-doc at the Université Paris Diderot, on a fellowship awarded La Fondation Sciences Mathématiques de Paris. Prior to receiving his doctorate, Michael completed his undergraduate studies at the University of Binghamton, of the State University of New York (SUNY).

### Research Interests

Michael is primarily interested in verifying parallel and distributed software systems. His recent work has developed formal models of such systems to facilitate automated reasoning, and techniques to detect, or prove the absence of, programming errors.

## Pierre-Yves Strub

Researcher

Pierre-Yves Strub received his Ph.D. in Computer Science from École Polytechnique, France, in 2008. He joined the IMDEA Software Institute in 2013, after a postdoctoral position at the Microsoft-INRIA Joint Lab in Paris, France and at the LIAMA institute in Beijing, China.

### Research Interests

Pierre-Yves research interests include formal proofs, proof assistants and their related type theory, certification of cryptographic algorithms and mathematical proofs, program verification via typing, and secure web programming. He is currently focused on EasyCrypt, a toolset for reasoning about relational properties of probabilistic computations with adversarial code, of which he is one of the main authors. He is also the main author of CoqMT, an extension of the Coq proof assistant.

## José Francisco Morales

Researcher

Jose F. Morales joined the IMDEA Software Institute as a postdoctoral researcher in November 2011, after receiving his Ph.D degree in Computer Science from the Technical University of Madrid (UPM), Spain. Previously, he held a teaching assistant position at the Universidad Complutense de Madrid, starting in 2005.

Jose's work to date has focused on mechanisms for the efficient execution of logic programs: inference of program properties by abstract interpretation, highly-optimizing translation to low-level code using those properties, and the development of abstractions for the specification and automated construction of abstract machines.

### Research Interests

His current research interests include the design of multiparadigm languages (combining imperative, logic, functional, and object-oriented programming), assertion languages and type systems, abstract interpretation, abstract machines, compiler optimizations, and native code generation.

# postdoctoral researchers

## César Kunz

Postdoctoral Researcher

César Kunz received a Computer Science degree from the National University of Córdoba (UNC), Argentina in 2004. He continued his studies at INRIA, France, funded by the FP6 FET integrated project "MOBIUS: Mobility, Ubiquity and Security", and received a Ph.D. from the École des Mines de Paris (ENSMP), France in February, 2009. He joined the IMDEA Software Institute as a postdoctoral researcher in February 2009.

### Research Interests

His research interests lie around formal program analysis and verification, abstract interpretation, and program transformation. His primary research activities are centered on the certification of program correctness, the verification of compiler optimizations, and the transformation of verification results in the presence of program transformations.

## Zorana Banković

Postdoctoral researcher

Zorana Banković obtained her Electrical Engineer degree from the Faculty of Electrical Engineering at the University of Belgrade (Serbia) in 2005 and her Ph.D. degree from the Universidad Politécnica de Madrid (UPM) in 2011. Her dissertation was given the UPM special award as one of the four best theses of Telecommunications School that year. Before joining IMDEA Software, she was a researcher at the Department of Electronic Engineering at UPM. She has participated in 11 research and development projects, and authored 10 journal publications. During that time her main research interests included energy-efficient security solutions for wireless sensor networks, anomaly detection and thermal–aware optimizations in data centers, such as floorplanning, dynamic resource scheduling and allocation, as well as the design of a reputation system, that allows applying optimization techniques to each state of a data center.

After joining IMDEA Software in October 2012, her research has mainly been related to ENTRA research project, funded by the EU 7th Framework Program Future and Emerging Technologies (FET).

### Research Interests

Her current research interests are in "energy-aware" software development using advanced program analysis and modeling of energy consumption in computer systems, aimed at making predictions of energy consumption early in the software design phase, and therefore enabling the development of greener IT through energy-efficient usage of hardware resources. Zorana's work includes research and development of energy optimization techniques at all software levels (compiler, OS, algorithms), as well as identification of static analyses that provide necessary input to the optimization stages which aim at improving resource consumption.

## François Dupressoir

Postdoctoral researcher

François Dupressoir joined the IMDEA Software Institute as a postdoctoral researcher in February 2013. He successfully defended his Ph.D. in Computer Science at the Open University (U.K.) under the supervision of Andy Gordon, Jan Jürjens, and Bashar Nuseibeh. His Ph.D. studies were partially funded by a Microsoft Research Ph.D. scholarship, and led him to internships at the European Microsoft Innovation Center, and at Microsoft Research in Redmond and Cambridge.

### Research Interests

François is broadly interested in program verification, theorem proving and cryptography. He is currently working with Gilles Barthe on methods for formally reasoning about cryptographic security properties of real-world systems, especially focusing on obtaining strong correctness and security results on low-level implementations of schemes and protocols, and studying how such properties can be preserved through compilation.

## Benedikt Schmidt

Postdoctoral researcher

Benedikt Schmidt joined the IMDEA Software Institute as a postdoctoral researcher in February 2013. He received his Ph.D. degree in Computer Science from ETH Zurich, under the supervision of David Basin.

### Research Interests

Benedikt is broadly interested in the areas of theorem proving, program verification, and rewriting and in their application to analyzing the security of systems. So far, his work has focused on the symbolic analysis of security protocols including interactive machine-checked approaches and fully automated approaches. Currently, he is also interested in the verification of cryptographic primitives and protocols against the computational model of attacks.

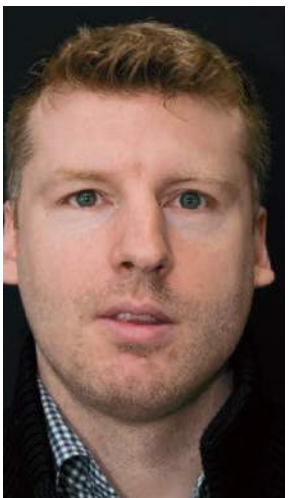
## Ilya Sergey

Postdoctoral researcher

Ilya Sergey joined the IMDEA Software Institute as a postdoctoral researcher in December 2012. He received his Ph.D. degree in Computer Science from KU Leuven (Belgium) under the supervision of Dave Clarke in November 2012. During his doctoral studies he was a visiting Ph.D. fellow at the Department of Computer Science of Aarhus University, hosted by Olivier Danvy, and a research intern in the Programming Principles and Tools group at Microsoft Research Cambridge, supervised by Simon Peyton Jones.

### Research Interests

Ilya's research interests dwell in the area of the design and implementation of programming languages, including but not limited to program semantics, certified programming, program transformations and refactoring techniques. He is particularly interested in developing methods of systematic derivation of correct-by-construction static analyses for higher-order languages by means of abstract interpretation, as well as their efficient implementations. Since joining IMDEA and working with Aleks Nanevski and Anindya Banerjee, he also became passionate about verification of multithreaded programs. He is currently working on a type-theoretic approach to specification and checking of properties of higher-order concurrent programs.



## Dragan Ivanović

Postdoctoral researcher

Before joining IMDEA Software, Dragan Ivanović received his B.Sc. and M.Sc. degrees in Computer Science and Electrical Engineering from University of Sarajevo, Bosnia and Hercegovina, and PhD in Computer Science from the Technical University of Madrid (UPM). His doctoral studies mainly concentrated on employing logic and constraint modeling and programming, as well as the corresponding program analysis methods, to study properties of complex and adaptive service oriented computing systems. He received the best paper award at ICSOC 2011.

### Research Interests

His main research interests are currently related to using computational logic and constraint programming techniques to model and analyze properties of complex adaptive software systems, such as service compositions provided via cloud. His other interests include dynamic modeling of cloud provision systems, and study of probabilistic behavior of service compositions, in terms of their performance and other non-functional properties.

## Andrea Cerone

Postdoctoral researcher

Andrea Cerone obtained his Ph.D. in November 2012, from Trinity College Dublin. During his Ph.D. his work focused on the definition of process calculi for representing wireless networks at different levels of abstraction. One of such process calculi was presented at the federated conference DiScoTec 2013, where he won the best paper award. From August 2012 to May 2013, he was a post-doc in the same university, where he started to grow an interest in probabilistic process algebras. In June 2013 he joined the IMDEA Software Institute, as a post-doc in the ADVENT Project. To date, his research topic in the project focuses on extending the notion of linearisability to higher order, concurrent programs.

### Research Interests

Andrea is mainly interested in the understanding of behavioural theories in different concurrent models of computation. These range over a wide spectrum, including linearisability for multithreaded programs, testing preorders for wireless networks and non-deterministic, probabilistic systems. Another of his main research interests are the development and the study of temporal and modal logics for verifying properties of concurrent systems, especially when seen in connection with the aforementioned behavioural theories.

## Guillermo Vigueras

Postdoctoral researcher

Guillermo Vigueras joined IMDEA Software Institute as a postdoctoral researcher in November 2013. He received his PhD degree in Computer Science from University of Valencia (Spain). His PhD studies were funded by a PhD scholarship granted by University of Valencia. This scholarship also granted him funds to do a research internship at the Computer Graphics Lab of University of Cyprus, under the supervision of Yiorgos Chrysanthou and another research stay at the Distributed Systems and Middlewares Group of INRIA-Rennes, under the supervision of Thierry Priol. Before joining IMDEA he worked as a postdoctoral researcher at the Biomedical Engineering Department of King's College London (KCL) and IMDEA Materials Institute where he worked with multidisciplinary teams for computer simulation of different scientific and engineering problems. During his stay at KCL he proposed the first GPU implementation of a cardiac electro-mechanical model showing the impact that HPC computing can have in patient specific diagnosis and surgery plan.

### Research Interests

In the past his research interests were focussed on addressing the problems of code parallelization for the exploitation of heterogeneous computer architectures like HPC and embedded platforms. Now at IMDEA Software Institute he plan to apply his previous experience and work to the automatic transformation of programs for heterogeneous platforms. This research line involve different topics like compilation techniques for automatic parallelization, mathematical program specification, program transformation based on functional and non-functional properties like resource usage, energy consumption, execution time,... The aim of this research is to drastically reduce the difficulties and cost of programming heterogeneous platforms, which are ubiquitous nowadays in society, and produce efficient software for these type of platforms.

# research assistants

Research Assistants hold full scholarships or contracts at the Institute, performing research within one of the Institute's research lines under the supervision of a junior or senior researcher, and they undertake their Ph.D. at one of the Universities that the Institute has agreements with. Many of our Research Assistants obtain their degrees from the Technical University of Madrid (UPM), with whom the Institute collaborates in the development of graduate programs, and also at Universidad Complutense de Madrid (UCM).

## Álvaro García

Research Assistant

Degree: Technical University of Madrid (UPM), Spain

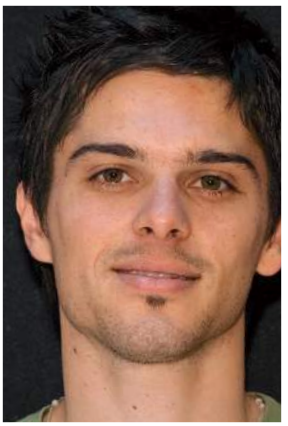
Research: Efficient implementations of functional programming languages: theories and models for higher-order languages and lambda calculus, inter-derivation of program semantics, and abstract machines.

## Miguel Angel García de Dios

Research Assistant

Degree: Universidad Complutense de Madrid (UCM), Spain

Research: Formal specification and verification; rigorous tool supported modeling and validation of software systems.



## Julian Samborski-Forlese

Research Assistant

Degree: Universidad Nacional de Rosario (UNR), Argentina

Research: Formal verification of reactive systems and asynchronous programs, with particular emphasis on the model checking of rich temporal logics.

## Juan Manuel Crespo

Research Assistant

Degree: Universidad Nacional de Rosario (UNR), Argentina

Research: Relational logics; formal verification of cryptographic primitives and protocols; programming languages.

### Federico Olmedo
Research Assistant

Degree: Universidad Nacional de Rosario (UNR), Argentina

Research: Verification of cryptographic systems and semantics of programming languages.

### Alejandro Sánchez
Research Assistant

Degree: Universidad Nacional de Córdoba (UNC), Argentina

Research: Concurrent systems; decision procedures; dynamic memory analysis; program verification.

### Carolina Inés Dania
Research Assistant

Degree: Universidad Nacional de Córdoba (UNC), Argentina

Research: Software engineering, formal methods and security. Particularly, I am working in tools and techniques for modeling, building and validating secure and reliable software systems.

### Javier Valdazo Parnisari
Research Assistant

Degree: Universidad Nacional de Córdoba (UNC), Argentina

Research: Formal specification and verification; rigorous tool supported modeling and validation of software systems; model driven software engineering; model transformations; security models, transformation and enforcement.

### Germán Andrés Delbianco
Research Assistant

Degree: Universidad Nacional de Rosario (UNR), Argentina

Research: Program verification with dependent types; development of new logics for reasoning about higher-order programs with imperative features, e.g., dynamic mutable state, continuations and concurrency, from a computational effects perspective.

### Umer Liqat
Research Assistant

Degree: Technical University of Madrid (UPM) and Dresden University of Technology (TUD), Germany

Research: Energy-aware software engineering, static analysis of energy consumption and optimization in embedded systems. Optimizations trading-off precision/performance/energy. Multi-language analysis and verification. He is working on the FP7 project Whole-Systems ENergy TRAnsparency (ENTRA).

### Gonzalo Ortiz
Research Assistant

Degree: Universidad Complutense de Madrid (UCM), Spain

Research: Languages and libraries to develop secure data-centric applications; model driven security; model-view-controller architecture; GUI development and libraries.

### Antonio Nappa
Research Assistant

Degree: Università degli Studi di Milano, Italy

Research: Computer security; malware analysis and cybercrime

### Artem Khyzha
Research Assistant

Degree: Dnipropetrovsk National University, Ukraine

Research: Developing compositional reasoning techniques for concurrent software; application of separation logic to software verification.

### Alejandro Serrano
Research Assistant

Degree: Autonomous University of Madrid (UAM), Spain

Research: Static resource analysis based on abstract interpretation; applications to energy transparency and optimization in embedded systems.

### Miriam García
Research Assistant

Degree: MSc in Mathematical Modelling in Engineering, University of L'Aquila and University of Hamburg

Research: Stability analysis based on model-checking techniques; hybrid systems; applied mathematics (PDEs, dynamical systems).

### Goran Doychev
Research Assistant

Degree: M.Sc. from Saarland University, Germany

Research: Obtaining quantitative security guarantees for computer systems, and using them to develop economically justified defenses. Favorite application: Side-channel attacks.

# interns

| Intern | Period | Nationality |
|---|---|---|
| Damir Valput | Oct. 2013 – Apr. 2014 | Croatia |
| Davide Ramaglietta | Feb. – Dec. 2013 | Italy |
| Elena Gutierrez | Jun. – Sep. 2013 | Spain |
| Guillaume Davy | Apr. – Aug. 2013 | France |
| Guillermo Guridi | May – Sep. 2013 | Spain |
| Guillermo Ramos | Jul. 2013 – Jul. 2014 | Spain |
| Iván López | Jun. – Aug. 2013 | Spain |
| Joaquín Arías | Jul. 2013 – Aug. 2014 | Spain |
| Lavinia Damian | Oct. 2013 – Apr. 2014 | Romania |
| Martin Cereza | Apr. – Oct. 2013 | Argentina |
| Nataliia Stulova | Jan. – Dec. 2013 | Ukraine |
| Önder Babur | Nov. 2012 – Jul. 2013 | Turkey |
| Peerachai Kaowichakorn | Aug. 2012 – Jan. 2013 | Thailand |
| Scott Livingston | May – Jun. 2013 | United States |
| Sergio del Olmo | Feb. – May. 2013 | Spain |
| Shiva Shabaninejad | Feb. 2012 – Jul. 2013 | Iran |
| Zhoulai Fu | Apr. – Aug. 2013 | China |
| M. Zubair Rafique | Apr. 2012 – Apr. 2013 | Pakistan |

# project staff
## joint research units

Project Staff provide additional support for the development of projects and contracts being carried out at the Institute. They are typically co-funded by such projects.

**Guillermo Jiménez**
Technical Project Staff,
Telefónica Joint Research Unit

Degree: B.Sc., European University Miguel de Cervantes, Valladolid, Spain

**Beatriz Muñoz**
Technical Project Staff,
Telefónica Joint Research Unit

Degree: B.Sc., University Rey Juan Carlos, Madrid, Spain

# project
## management unit

**Jesús Contreras**
Project Strategy Manager
& Business Developer

Degree: MBA - CEREM and PhD in CS - Technical University of Madrid (UPM), Spain

**Juan José Collazo**
Project Manager

Degree: B.Sc. in Economic Scienc-es-Complutense University, Madrid, Spain

# technical support
## infrastructures unit

Research Support Technical Staff provide support for the research infrastructures provided to the researchers at the Institute. These include virtualization environments, version control systems, research collaboration tools, continuous integration platforms, experimentation harnesses, computing farms, communications, etc. They are currently co-funded by different projects and agreements.

**Roberto Lumbreras**
Communication
Infrastructures

Degree: MSc. Elec. & Computer Eng. Technical University of Madrid (UPM), Spain

**Juan Céspedes**
Network and Systems
Engineer (part-time)

Degree: MSc. Elec. & Computer Eng. Technical University of Madrid (UPM), Spain

# management
## & administration

**María Alcaraz**
General Manager

Degree: MBA - Escuela Internacional de Negocios – CEREM Madrid, Spain

**Paola Huerta**
Human Resources Assistant

Degree: M.A. in Art History - Universidad Complutense, Madrid, Spain

**Tania Rodríguez**
Administrative Assistant (part-time)

Degree: M.Sc. in Business Administration - Universidad Centroamericana José Simeón Cañas, El Salvador

**Laura Bellmont**
Infrastructures Manager (part-time)

Degree: M.Sc. in Architecture, Technical University of Madrid (UPM), Spain

**Andrea Iannetta**
Administrative Assistant

Degree: B.Sc. in Economics - Godspell College, Argentina

**Carlota Gil**
Accounting Assistant

Degree: M.Sc. in Business Administration - Universidad Rey Juan Carlos, Madrid, Spain

# research projects and contracts

An important source of funding and technology transfer opportunities for the Institute are cooperative projects, awarded through competitive calls for proposals by national and international funding agencies, and contracts with industry. In 2013, the Institute participated in 27 funded research projects and contracts, 15 of which (68% of the total) involve collaboration with industry. Of the 27 projects, 13 are international (11 funded by the European Union, 1 by the US ONR and Stanford University, and 1 by the Danish Research Council), 9 of them are direct industrial funding, and the rest are funded by national (4) and regional (1) agencies. Figure 5.1 shows the origin of project funding. In the same year, the Institute benefited from 13 fellowships.

Figure 5.2 shows the trend in external funding for the period 2008-2013, with the forecast for 2014. The external funding for 2014 is expected to increase by 22% with respect to 2013. The percentage of external funding with respect to the total budget of the Institute was already around 30% in 2013, and also shows an increasing trend for 2014. Direct contracts with industry play an increasingly important role in the Institute's external funding. The number of such contracts has almost doubled in 2013 compared to the year before.

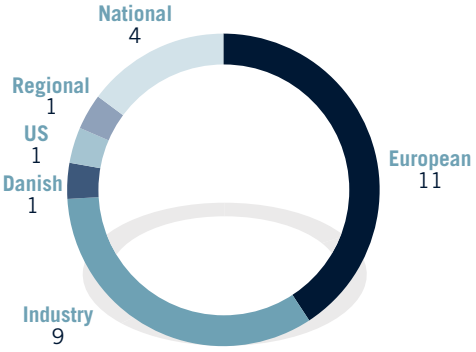



*Figure 5.1: Projects by origin of funding.*

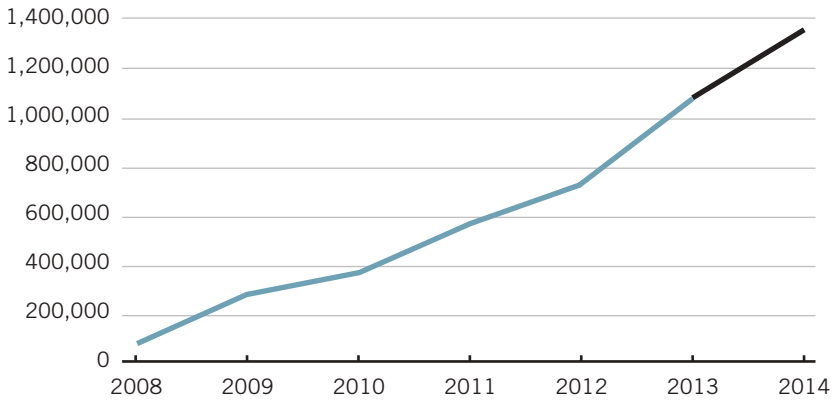



*Figure 5.2: Evolution in external funding since 2008.*

The rest of the chapter summarizes the main projects, contracts, grants, and fellowships awarded to the Institute in 2013, and briefly describes some interesting recently granted projects.

## 5.1 Ongoing Projects in 2013

### ADVENT

#### Architecture-Driven Verification of Systems Software

Funding: European Union – 7th Framework Programme – FET Young Explorers
Duration: 2013–2016
Project Coordinator: Alexey Gotsman

IMDEA Software is the main partner and coordinator of the ADVENT research project. The project was awarded during the year 2012 and will run from April 2013 to 2016. It is funded by the very competitive EU 7th Framework Programme, Future and Emerging Technologies (FET) *Young Explorers Initiative*, and has an overall budget of 1 million Euro. In addition to IMDEA Software, the consortium includes as partners Tel Aviv Univesity (Israel), The Max Planck Institute (Germany), and Katholieke Universiteit Leuven (Belgium).

The ADVENT project (http://advent-project.eu) will develop innovative methods and tools for cost-effective verification of real-world systems software, making it possible to guarantee an unprecedented level of reliability. ADVENT will achieve this by exploiting a trend among programmers to use informally described patterns, idioms, abstractions, and other forms of structure contained in their software, which are together called its architecture.

Building on the emerging technology of separation logic, ADVENT will formalize such software engineering concepts used by systems programmers to reason about their software informally, and will use the results to drive the design of verification techniques. This is a radically novel approach to the problem of verifying complex software: it departs from the common practice of building generic verification tools that, not being able to take advantage of programmers' knowledge and intuition, do not scale to big and complicated systems.

The architecture-driven verification techniques resulting from the project have the potential to yield a dramatic leap in the cost-benefit ratio of the verification technology. This will allow verification to scale to systems of real-world size and complexity that so far have been beyond the reach of quality assurance methods guaranteeing correctness.

# 4CaaSt

## Building the PaaS Cloud Platform of the Future

Funding: European Union – 7th Framework Program
Duration: 2010-2013
Principal Investigator: Prof. Manuel Carro

IMDEA Software joined the EU 7th FP project *4CaaSt* as a partner in January 2013. The goal of the project was to create an advanced PaaS Cloud platform which supports the optimized and elastic hosting of Internet-scale multi-tier applications. 4CaaSt embeds all the necessary features, easing programming of rich applications and enabling the creation of a true business ecosystem where applications coming from different providers can be tailored to different users, mashed up and traded together.

IMDEA's participation focused on the cloud application lifecycle engineering, management and experimentation, with a special focus on the process of resolution of application and component specifications (*blueprints*) to produce deployable configurations of cloud components that can be packaged into products that can be commercialized and marketed, thus promoting fast value uptake for small and medium enterprises using the cloud technologies.

# POLCA

## Programming Large Scale Heterogeneous Infrastructures

Funding: European Union – 7th Framework Program
Duration: 2013–2016
Principal Investigator: Prof. Manuel Carro

The POLCA project explicitly addresses the programmability concerns of both embedded and high performance computing. Both domains have generated strongly focused approaches for solving their specific problems that are now confronted with the increasing need for parallelism even in Embedded Systems and the need for addressing non-functional criteria in High Performance Computing. Rather than improving both domains separately, POLCA takes a bold step forward by proposing a hybrid programming model that decisively increases programming efficiency in both areas and enables realisation of multi-domain use cases.

This model thereby allows efficient parallelisation and distribution of the application code across a highly heterogeneous infrastructure, not through automatic methods, but through exploitation of fundamental mathematical axioms behind the execution logic. The model is strongly oriented towards mathematical application cases of both domains, ranging from sensor evaluation, over monitoring-control-loops to complex simulation and modelling. POLCA is thereby explicitly geared towards exploitation of reconfigurable hardware to make use of their high efficiency under the right usage criteria. In principal it even allows for exploitation of run-time reconfigurations, given an application with a suitable profile.

The project builds up on existing collaboration between experts from embedded computing and high performance computing, to combine complementary expertise from the two domains into an accessible and productive programming model of the future.

# ENTRA

## Whole-systems energy transparency

Funding: European Union - 7th Framework Program - FET proactive MINECC call
Duration: 2012-2015
Project Coordinator: Prof. John Gallagher

ENTRA is an FP7 “Future and Emerging Technologies” project under the proactive “MINECC” objective - “Minimizing Energy Consumption of Computing to the Limit”. The ENTRA project proposes radical advances in energy-aware software design and

management with the objective of providing an important key to the pervasive realization of energy-aware computing. Though huge advances have been made in power-efficient hardware, most of the potential energy savings are wasted by software that does not exploit energy-saving features of hardware, and by poor dynamic management of tasks and resources. The budget of the project is approximately 2.7M Euros.

The project is built around the central concept of *energy transparency* at every stage of the software lifecycle. The project will develop novel *program analysis* and *energy modeling* techniques, making energy usage transparent through the system layers. This will enable *energy optimizations* both during code development and at run-time, and promote energy efficiency to a first-class software design objective.

## AutoCrypt

Funding: US Office of Naval Research (ONR), through Stanford University
Duration: 2012-2015
Project Coordinator: Prof. Gilles Barthe

AutoCrypt is a joint project with Stanford University, University of Pennsylvania, and SRI, funded by ONR and which will run from July 2012 until July 2015. It has an overall budget of 2 Million Euros. AutoCrypt aims to use computer technology to provide mathematical guarantees that a cryptographic algorithm is secure, and that it is adequate for a given product, process, or service.

Within the project, the IMDEA Software team will use their EasyCrypt tool (http://www.easycrypt.info) to develop a systematic classification of cryptographic algorithms and to create a cryptographic atlas that will be used by researchers and companies to choose the most suitable algorithm for their needs.

## HATS

### Highly Adaptable and Trustworthy Software using Formal Models.

Funding: European Union – 7th Framework Program – FET proactive *Forever Yours* call
Duration: 2009-2013
Principal Investigator: Prof. Gilles Barthe

HATS is an Integrated Project funded by the European Union within the 7th Framework Program, "Future and Emerging Technologies" under the proactive "Forever Yours" objective. The main outcome envisaged by this project is an integrated architectural frame-

work and a methodology for rigorous development of highly adaptable and trustworthy software. The IMDEA Software Institute is one of the research centers in a consortium of 8 academic partners, 2 industrial research centers, and 1 SML, from 7 countries. The budget for the project is approximately 6M Euros.

Specifically, HATS strives to turn software product family (SWPF) development into a rigorous approach. The technical core of the project is an Abstract Behavioral Specification language which allows precise description of SWPF features and components and their instances. The main project outcome is a methodological and tool framework achieving not merely far-reaching automation in maintaining dynamically evolving software, but an unprecedented level of trust while informal processes are replaced with rigorous analysis based on formal semantics.

The IMDEA Software Institute is responsible for the development of a highly adaptable architecture that allows cost-effective verification of the executable programs that will be automatically generated from Abstract Behavioral Specifications. The security architecture is specifically directed towards security policies expressed using information flow and functional correctness policies.

## NESSoS

### Network of Excellence on Engineering Secure Future Internet Software Services and Systems

Funding: European Union, Cooperation Program (NoE) – 7th Framework Program
Duration: 2011-2013
Principal Investigator: Prof. Manuel Clavel

The Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS) aims at constituting and integrating a long lasting research community on engineering secure software-based services and systems. The NESSoS consortium involves 12 partners, including 2 companies (namely, Siemens and ATOS), from 7 countries. The budget for the project is approximately 3.5 M Euros.

The domain of Engineering Secure Software Services covers a collection of engineering activities that aim at the creation of software services —i.e. ICT services delivered through the deployment of software systems— that are both behaviorally correct (typically guided by software engineering principles) as well as secure (typically guided by security engineering principles). The approach of engineering secure software services is based on the principle of addressing security issues from the very beginning in system design and analysis, thus contributing to reducing system and service vulnerabilities, improving the

necessary assurance level, thereby considering risk and cost issues during development in order to prioritize investments.

IMDEA Software plays a prominent role in three research workpackages: secure service architectures and design; programming environments for secure and composable services; and security assurance for services. Also, IMDEA Software leads the researcher mobility program within the consortium. This program is a mechanism that supports the integration of activities across the various sites: it brings together researchers working on related topics; it drives knowledge exchange and knowledge generation through union and diversity; and, finally, it increases the capability of joint cooperation among researchers.

## VARIES

### Variability in safety critical embedded systems

Funding: ARTEMIS- European Union - 7th Framework Program
Duration: 2012-2015
Principal Investigator: Laurent Mauborgne

VARIES is an ARTEMIS Joint Undertaking project granted under the FP7 ARTEMIS-2011-1 Call. The 26 partners-strong international consortium includes the participation of national partners Hi-Iberia, Integrasys, and Tecnalia. The main goal of the VARIES project is to help Embedded Systems (ES) developers to maximize the full potential of variability in safety-critical ES. The objectives of this project will be therefore (i) to enable companies to make informed decisions on variability use in safety-critical ES; (ii) to provide effective variability architectures and approaches for safety-critical ES; and (iii) to offer consistent, integrated and, continuous variability management over the entire product life cycle.

The VARIES project will deliver the VARIES Platform: a complete, cross-domain, multi-concern, state-of-the-art reference platform for managing variability in safety-critical ES. Special attention will be given to aspects specific to safety-critical ES, in particular the impact of reuse and composition on certification.

In addition to this ambitious goal, the VARIES project will create a Center of Innovation Excellence (CoIE) for managing variability in ES. The VARIES CoIE will support the European ES industry on the 3 aforementioned objectives.

# DESAFIOS-10

## High-Quality, Reliable, Distributed, and Secure Software Development

Funding: Spanish Ministry of Science and Innovation
Duration: 2011-2013
Principal Investigator: Prof. Gilles Barthe

The overall goal of the DESAFIOS-10 project is to contribute both foundations and technologies for the development of software systems with certified quality and reliability, based on formal methods and declarative programming. The consortium involves groups from three different Institutions (Universidad Complutense de Madrid, Universidad Politécnica de Madrid, and IMDEA Software) and a number of industrial users.

This project arises as a natural evolution of the previous coordinated project DESAFIOS, which involved only the research groups from Universidad Complutense de Madrid and Universidad Politécnica de Madrid. In contrast, DESAFIOS-10 emphasizes the security and reliability aspects of this research, which is precisely the workpackage led by IMDEA Software.

# PROMETIDOS

## Methods for Rigorous Software Development

Funding: Regional Government of Madrid
Duration: 2011-2013
Principal Investigator: Prof. Gilles Barthe

The PROMETIDOS-CM research program is focused on four main areas: specification and validation, to provide a solid foundation for the description and analysis of services; reliability and security, to guarantee robust solutions from start to end; declarative programming, to develop the next generation of languages for services; and efficiency, to optimize quality of service with respect to performance. A common goal for all these research lines is the development of tools that will rigorously support their scientific results and that can be eventually transferred to industry.

PROMETIDOS-CM is a consortium involving groups from Universidad Complutense de Madrid, Universidad Politécnica de Madrid, and the IMDEA Software Institute, which is the project coordinator.

# PARAN-10

## Parametrized Verification of Computing Systems

Funding: Spanish Ministry of Science and Innovation
Duration: 2011-2013
Investigator: Prof. Pierre Ganty

This project aims at developing novel techniques for production, verification and certification of computing systems where *parameters* play an essential role. Parameters either at the level of the system specification or at the level of the verification technique make it possible to address scalability and undecidability issues. However, specification and verification in the presence of parameters are highly non-trivial, and pose problems for automated verification methods (such as model checking) as well as interactive approaches to computing systems verification (such as theorem-proving), both of which are relevant in practice.

The project is organized along three research lines: model-checking of parametrized systems, parametric model-checking, and programming languages and logics for parametrization. In these three lines the project aims at making fundamental contributions to advance the state of the art as well as develop prototype implementations in order to explore and demonstrate the practical relevance of the proposed approaches.

# StrongSoft

## Sound Technologies for Reliable, Open, New Generation Software

Funding: Spanish Ministry of Economy and Competitiveness
Duration: 2013–2015
Principal Investigator: Prof. Gilles Barthe

The goal of the StrongSoft project is to define, implement, evaluate, and disseminate disruptive technologies that are able to keep pace with the rapid evolution of software systems and address the challenges it implies. The project will provide solutions for supporting the cost-effective development of a new generation of software systems that are reliable, efficient, and secure while connected to an open, untrusted world, across different application domains. The workplan is organized in a number of coordinated lines that cover security and cryptography, verification, debugging and testing, language technology, and tools. To achieve its objectives the StrongSoft consortium coordinates some of Spain's leading research groups in reliable software technologies together with a number of key foreign researchers and highly interested industrial end users.

# RMT

## Rich-Model Toolkit – An Infrastructure for Reliable Computer Systems (COST Action IC0901)

Funding: European Union, Cost action
Duration: 2009 - 2013
Investigator: Prof. César Sánchez

This initiative explores directions and techniques for making automated reasoning (including analysis and synthesis) applicable to a wider range of problems, as well as making them easier to use by researchers, software developers, hardware designers, and information system users and developers. It includes participants from over 20 countries. A selection of the topics of interest is:

**Standardization of expressive languages:** Definitions of formats to represent systems, formulas, proofs, counterexamples. A framework to specify translations between specification languages, as well as benchmarks and competitions for automated reasoning, verification, analysis, and synthesis.

**Decision procedures:** Creation of decision procedures for new classes of constraints, including implementation of SAT and SMT and their certification. This requires the encoding of synthesis and analysis problems into SMT. The encoding of description logics (widely used in the Semantic Web) and the problem of scalable reasoning about knowledge bases are also addressed.

**Transition system analysis:** One key topic of study is abstraction-based approaches and refinement for verification of infinite-state systems. The application of constraint-based program analysis is also being analyzed, as well as data-flow analysis for complex domains. The application of TSA to programming languages and bytecode is being explored by extracting transition systems from them.

**High-level synthesis:** The project is devising new algorithms for synthesis from high-level specifications, and decision procedures are being extended to perform synthesis tasks. A relevant point being explored is the connection between invariant generation and code synthesis.

# NUSA

## Numeric and Symbolic Abstractions for Software Model Checking

Funding: The Danish Council for Independent Research - Natural Sciences
Duration: 2011-2013
Principal Investigator: Prof. John Gallagher

Abstract interpretation and model checking are two approaches to verifying or deriving properties of software and hardware systems. While model checking is applied to finite-state systems (typically hardware), abstract interpretation is usually aimed at infinite-state software

systems. Indeed, the very notion of verification by abstraction starts from the assumption that the system under consideration is infinite or very large. Both abstract interpretation and model checking are the subject of major research efforts, both in academic and industrial laboratories, since they hold out the promise of an automatic, push-button approach to obtaining guarantees of system behavior. This proposal lies in the intersection of abstract interpretation and model checking. The main question for investigation in this project is how the framework and accumulated experience of abstract interpretation can be applied to model checking infinite state systems - in short, to define abstract model checking methods that exploit the generality and power of the framework of abstract interpretation.

## AMAROUT Europe

Funding: European Union, Marie Curie Action (PEOPLE-COFUND) - 7th Framework Program
Duration: 2009-2013
General Coordinator: Prof. Manuel Hermenegildo

AMAROUT Europe was a Marie Curie Action (PEOPLE-COFUND) to foster and consolidate the European Research Area by attracting to Europe and, in particular, to the region of Madrid, top research talent. AMAROUT helps the IMDEA network contribute to the goal of turning Madrid into one of the top knowledge generation regions in Europe. To accomplish this, the AMAROUT program finances up to 132 researchers to join the IMDEA network of research institutes for one year (renewable up to twice). The total budget for the program was around 11 M Euros of which the European Union cofinances 40%.

Both “experienced” and “very experienced” researchers from any country worldwide could apply for AMAROUT fellowships at any of the seven IMDEA Institutes participating in the program (Energy, Food, Materials, Nanoscience, Networks, Software, and Water). The AMAROUT Selection Committee consisted of seven Evaluation Panels, one for each of the participating IMDEA Institutes. Each Evaluation Panel was formed from the Director of the Institute, three members of its Scientific Advisory Board, and two external, independent peer reviewers. The main AMAROUT selection criteria was the candidate’s demonstrated ability and commitment to research, as well as the match of experience and interests with the research theme and lines of the IMDEA Institute chosen by the candidate.

The AMAROUT Program was a joint initiative from the seven IMDEA research institutes. The IMDEA Software Institute was in charge of writing and submitting the proposal and is the beneficiary, acting as the administrator of the program for the other institutes. As such, it was in charge of the project management and its structure: Scientific Committee (SC); Fellowships Management Unit (FMU); Secretary; and Local Board of Prospective (BP).

# AMAROUT II Europe

Funding: European Union, Marie Curie Action (PEOPLE-COFUND) - 7th Framework Program
Duration: 2012-2016
General Coordinator: Prof. Manuel Hermenegildo

AMAROUT-II Europe is a Marie Curie Action (PEOPLE-COFUND) which continues the AMAROUT action sharing with it the objectives of fostering and consolidating the European Research Area by attracting to Europe and, in particular, to the region of Madrid top research talent. As in the previous AMAROUT program "experienced" and "very experienced" researchers from any country (worldwide) can apply for AMAROUT II fellowships at any of the seven IMDEA Institutes participating in the program (Energy, Food, Materials, Nanoscience, Networks, Software, and Water). The program is seeking to attract, over 4 years, 152 experienced researchers to carry out research projects within the IMDEA network. The program keeps a call open permanently until months 36. Applications are evaluated by batches, according to quarterly cut-off dates. To promote the program and its calls, both nationally and abroad, best practices developed during the previous AMAROUT program are being applied. IMDEA Software is the mono-beneficiary of the AMAROUT-II programme, the same role that it is currently performing for the previous AMAROUT programme.

As in AMAROUT, the AMAROUT-II Program is a joint initiative from the seven IMDEA research institutes. The IMDEA Software Institute was in charge of writing and submitting the proposal and is the beneficiary, acting as the administrator of the program for the other institutes.

# Microsoft Research Software Engineering Innovation Foundation Awards

The *SEIF (Software Engineering Innovation Foundation)* awards are given by Microsoft to support research in software engineering technologies, tools, practices, and teaching methods. These awards are given to project proposals which can be related to any of the core areas of interest in software engineering and have been given in 2012 for the third time. More than 100 project proposals were received this year, among which 10 projects were selected to receive the prize and the associated grant. Out of these 10 selected projects, two were granted to the IMDEA Software Institute for the following projects:

- **Alexey Gotsman** with the project *Specifying and Validating Components on Memory Models of Mobile Platforms*.
- **Mark Marron** with the project *MemAlyzer: Finding and Fixing Memory Usage Problems*.

The rest of the selected applications were from centers in the US (6), Canada (1 – U. of Calgary) and Switzerland (1 – ETH Zurich).

## AbsInt GmbH

This project is a contract with AbsInt Angewandte Informatik GmbH to collaborate in the development of static analyzers by abstract interpretation. It is coordinated by Laurent Mauborgne. The goal of this contract is to develop advanced abstract interpretation techniques allowing fine tuning and increasing the precision and efficiency of the Astrée static analyzer sold and maintained by AbsInt. IMDEA Software brings its expertise and advice on sound abstractions of the memory model of the C language and on adaptive relational abstract domain tuning.

## EIT ICT Labs CLC

### Co-Location Center

IMDEA Software headquarters hosts the **Madrid Co-Location Center (CLC)** of EIT ICT Labs. The CLC is the central place for organizing and implementing EIT ICT Labs activities in Spain, and the principal meeting point for the Spanish Associate Partner Group (APG), lead by IMDEA Software, which includes some of the most prominent actors in the ICT innovation arena, such as Telefónica, Indra, Atos, the Technical University of Madrid (UPM) and the Barcelona Supercomputing Center (BSC).

## Telefónica Digital

Since 2012, IMDEA has cooperated with *Telefónica Digital*, Spain on research and development in components for automatic management of cloud scalability towards their integration into *Claudia*, a product developed within the European FI-WARE initiative. *Claudia* facilitates the definition and automatic deployment and management of virtual machines, storage, and connectivity resources that comprise the virtual infrastructure on which cloud applications are run.

The Institute is in charge of providing advice on the software architecture and high-level design of the software components, within the FI-WARE requirements, and participates in their development and testing. The component integration is based on the OpenStack cloud architecture.

As mentioned before, Telefonica Digital and the Institute also established during 2013 a *Joint Research Unit* (JRU) within their more global strategic partnership.

## Boeing Research & Technology Europe

IMDEA has also been contracted since 2012 by *Boeing Research & Technology Europe* (which is located in Spain), to work jointly in research and development in the fields of Big Data and Social Network Analytics. In particular, the Institute and Boeing are jointly designing and implementing a framework for data mining in social media. The framework includes a declarative embedded language designed by IMDEA Software. This language supports the description of workflows that integrate map-reduce jobs and native applications. The implementation avoids costly recomputations increasing the efficiency of social media processing, with applications in rich Web interfaces that rely on live collection of social network information from Twitter streams and other sources.

## Logicblox

In 2013, the IMDEA Software Institute started cooperation with LogicBlox, located in Georgia, USA, applying IMDEA's expertise in logic engines within the LogicBlox commercial deductive (smart) database system. The smart database and its high-level declarative query language (LogiQL) enable users used to build applications that combine transactional, analytical, graph, probabilistic, and mathematical programming. This makes possible new classes of hybrid applications that are hard or impossible to build on a traditional technological stacks that involve a cocktail of multiple programming languages and databases. This system includes sophisticated logic for optimizing database query execution, and is able to take advantage of multi-core and cloud programming, while abstracting away much of their intrinsic complexity.

## 5.2 Projects with Associated Groups

Part of the research of the Institute is performed in collaboration with research groups at associated institutions. This is exemplified by the existence of research projects led by these institutions but in which IMDEA personnel take part (and the resulting joint publications and results). We provide a summary list of the most relevant such projects which were active during 2013.

| Project | Duration | Description | Funding Agency |
|---|---|---|---|
| DOVES | 2009-2014 | Development of verifiable and efficient software | MINECO |
| SpaRCIM | 2003-2014 | Spanish Research Consortium for Informatics and Mathematics | European Union / MINECO |

## 5.3 Some Recently Granted Projects (not started in 2013)

### CADENCE

#### Cyber Attack Detector Engineering for Commercial Exploitation

The CADENCE project is a year-long action and a part of the EIT ICT Labs activities in 2014 in its Action Line on Privacy, Security, and Trust. The project concentrates on development of a sensor able to detect advanced cyber attacks in network traffic by applying innovative anomaly detection technology, with the goal of advancing cyber-defense expertise and creating more secure ICT environments in both governments and businesses. CADENCE aims at addressing the needs of a segment of a market whose size is estimated at 250 billion EUR in Europe with specific innovative product and service prototypes. The project will be developed together with TNO in Netherlands, and the Reply Spa. group in Italy. The principal investigator on this project for IMDEA Software will be Juan Caballero.

### I3H

#### Incubating Internet Innovation Hubs

The objective of the I3H project is to contribute to the sustainability of FI PPP by creating a European network of Internet Innovation Hubs (IIH), regional or thematic clusters that bring together web entrepreneurs, mentors, investors, students, academia, industry, and public sector innovators to speed up the transformation of FI PPP results to services and applications addressing the needs of European citizens, companies, and society. The starting point is the initial network of EIT ICT Labs hubs in Budapest, Eindhoven, Helsinki, Madrid, Paris and Trento coinciding with the Nodes of EIT ICT Labs. The seed network will grow organically with a robust life-cycle incubation stage gate process for identifying candidate hubs and guiding them through tangible milestones towards full-fledged IIH's with hands-on coaching, resources and support, including knowledge and best practice transfer.

## VerisTab

### Formal Verification of Stability of Embedded Control Systems

The VerisTab project addresses the challenge of building high confidence embedded control systems, by means of verifying their stability (resistance to perturbation in the initial state or inputs) using automated formal verification techniques that will be developed within the project. The objective is to facilitate the development of fully automated and scalable methods for stability verification, thereby addressing the shortcomings of the state-of-the-art deductive techniques. An algorithmic approach to stability verification is a challenging task, since, even fundamental notions for abstraction and composition, which form the backbone of scalable algorithmic verification, have not been well explored. VerisTab proposes a three-phase plan from developing theoretical foundations to algorithm design and software tool development. The principal investigator on this project for IMDEA Software will be Pavithra Prabhakar.

## 5.4 Fellowships

1. *Microsoft Research PhD Scholarship funds*, awarded in 2011, active in 2012-2015 (**Alexey Gotsman**).
2. *Juan de la Cierva Postdoc grant*, Spanish Ministry of Science and Innovation, awarded in 2010 and ending in 2014 (**César Kunz**, through UPM).
3. *Juan de la Cierva Postdoc grant*, Spanish Ministry of Science and Innovation, awarded in 2011 and ending in 2015 (**Juan Caballero**).
4. *Ramón y Cajal grant*, Spanish Ministry of Science and Innovation, awarded in 2010 and ending in 2015 (**Aleksandar Nanevski**).
5. *Marie Curie AMAROUT II Incoming Fellowships (6)*, European Union – 7 Framework Program, awarded in 2012 and active in 2013 (**Dario Fiore**, **Michael Emmi**, **François Dupressoir**, **Benedikt Schmidt**, **Pierre-Yves Strub** and **Ilya Serrgey**).
6. *Predoctoral Grants*, Madrid Regional Government, awarded in 2009 and continuing in 2013 (**Álvaro García**).
7. *FPI Doctoral Grant*, Spanish Ministry of Science and Innovation, awarded in 2010 and continuing until 2014 (**Juan Manuel Crespo**).
8. *FPU Doctoral Grant*, Spanish Ministry of Education, Culture and Sports, awarded in 2012 (**Julián Samborski-Forlese**).

# dissemination of Results

## 6.1 Publications

### 6.1.1 Refereed Publications

Journals

1. *Anindya Banerjee*, David A. Naumann, Stan Rosenberg. Local Reasoning for Global Invariants, Part I: Region Logic. Journal of the ACM, Vol. 60, Num. 3, pages 1–56, ACM, 2013.

2. *Anindya Banerjee*, David A. Naumann. Local Reasoning for Global Invariants, Part II: Dynamic Boundaries. Journal of the ACM, Vol. 60, Num. 3, pages 1–73, ACM, 2013.

3. Alexander Malkis, *Anindya Banerjee*. On Automation in the Verification of Software Barriers: Experience Report. Journal of Automated Reasoning, Vol. 52 Num. 3, Springer-Verlag New York, Inc., 2013.

4. *Gilles Barthe*, *Boris Köpf*, *Federico Olmedo*, Santiago Zanella Béguelin. Automatically Deriving Information-theoretic Bounds for Adaptive Side-channel Attacks. ACM Transactions on Programming Languages and Systems (TOPLAS), Vol. 35, Num. 3, ACM, November 2013.

5. *Juan Caballero*, Dawn Song. Automatic Protocol Reverse-Engineering: Message Format Extraction and Field Semantics. Computer Networks, Vol. 57, Num. 2, pages 451–474, 2013.

6. *Manuel Carro*, Ángel Herranz, Julio Mariño. A Model-Driven Approach to Teaching Concurrency. ACM Transactions on Computer Education, Vol. 13, Num. 1, 2013.

7. Kyriakos Kritikos, Barbara Pernici, Pierluigi Plebani, Cinzia Cappiello, Marco Comuzzi, Salima Benbernou, Ivona Brandic, Attila Kertesz, Michael Parkin, *Manuel Carro*. A Survey on Service Quality Description. ACM Computing Surveys, Vol. 46, Num. 1, 2013.

8. *Andrea Cerone*, Matthew Hennessy. Modelling Probabilistic Wireless Networks. Logical Methods in Computer Science, Vol. 9, Num. 3, 2013.

9. *Alexey Gotsman*, Hongseok Yang. Modular Verification of Preemptive OS Kernels. Journal of Functional Programming, Vol. 23, Num. 4., pp. 452-514. Cambridge University Press, 2013.

10. *Alexey Gotsman*, Hongseok Yang. Linearizability With Ownership Transfer. Logical Methods in Computer Science, Vol. 9, 2013.

11. *Dragan Ivanović*, *Manuel Carro*, *Manuel V. Hermenegildo*. A Sharing-Based Approach to Supporting Adaptation in Service Compositions. Computing, Vol. 95, Num. 6, pages 1–40, Springer Wien, June 2013. 10.1007/s00607-012-0230-z.

12. *Mark Marron*, *César Sáncheze*, Zhendong Su, and Manuel Fähndrich. Abstracting Runtime Heaps for Program Understanding, In IEEE Transactions in Software Engineering 39(6): 774-786, 2013.

13. Georges Gonthier, Beta Ziliani, *Aleksandar Nanevski*, Derek Dreyer. How To Make Ad Hoc Proof Automation Less Ad Hoc. Journal of Functional Programming (JFP), Vol. 23, Num. 4, pages 357–401, July 2013.

14. Murdoch J. Gabbay, *Aleksandar Nanevski*. Denotation of Syntax And Metaprogramming in Contextual Modal Type Theory (CMTT). Journal of Applied Logic (JAL), Vol. 11, Num. 1, pages 1–29, March 2013.

15. *Aleksandar Nanevski*, *Anindya Banerjee*, Deepak Garg. Dependent Type Theory for Verification of Information Flow and Access Control Policies. ACM Trans. Program. Lang. Syst., Vol. 35, Num. 2, pages 1–41, ACM, 2013.

16. Maria-Cristina Marinescu, *César Sánchez*. Fusing Statecharts and Java, In ACM Transactions in Embedded Computing Systems, vol 12, number 1s, pages 45:1-45:21, ACM, 2013.

17. Nikhil Swamy, Juan Chen, Cédric Fournet, *Pierre-Yves Strub*, Karthikeyan Bhargavan, Jean Yang. Secure distributed programming with value-dependent types. Journal of Functional Programming, Vol. 23, Num. 4, pages 402-451, Cambridge University Press, 2013.

publications

## Conferences

1. Gordon Stewart, *Anindya Banerjee*, *Aleksandar Nanevski*. Dependent Types for Enforcement of Information Flow and Erasure Policies in Heterogeneous Data Structures. 15th International Symposium on Principles and Practice of Declarative Programming (PPDP 2013), pages 145–156, ACM, 2013.

2. Shachar Itzhaky, *Anindya Banerjee*, Neil Immerman, *Aleksandar Nanevski*, Mooly Sagiv. Effectively-Propositional Reasoning about Reachability in Linked Data Structures. Computer Aided Verification (CAV 2013), Lecture Notes in Computer Science, Vol. 8044, pages 756–772, Springer, 2013.

3. *Z. Banković*, *P. Lopez-Garcia*. Genetic Algorithm-based Allocation and Scheduling for Voltage and Frequency Scalable XMOS Chips. Hybrid Artificial Intelligent Systems, Lecture Notes in Computer Science, Vol. 8073, pages 401–410, Springer, 2013.

4. *Gilles Barthe*, George Danezis, Benjamin Grégoire, *César Kunz*, Santiago Zanella Béguelin. Verified Computational Differential Privacy with Applications to Smart Metering. CSF, pages 287–301, IEEE, 2013.

5. José Bacelar Almeida, Manuel Barbosa, *Gilles Barthe*, *Francois Dupressoir*. Certified Computer-Aided Cryptography: Efficient Provably Secure Machine Code From High-Level Implementations. ACM Conference on Computer and Communications Security, pages 1217–1230, 2013.

6. *Gilles Barthe*, *Juan Manuel Crespo*, *César Kunz*. Beyond 2-Safety: Asymmetric Product Programs for Relational Program Verification. Logical Foundations of Computer Science, International Symposium, LFCS 2013, Lecture Notes in Computer Science, Vol. 7734, pages 29–43, Springer, 2013.

7. *Gilles Barthe*, *Juan Manuel Crespo*, Sumit Gulwani, *César Kunz*, *Mark Marron*. From Relational Verification to SIMD Loop Synthesis. ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming, PPoPP '13, pages 123–134, ACM, 2013. **Best paper award.**

8. *Gilles Barthe*, *Juan Manuel Crespo*, Benjamin Grégoire, *César Kunz*, Yassine Lakhnech, *Benedikt Schmidt*, Santiago Zanella Béguelin. Fully Automated Analysis of Padding-Based Encryption in the Computational Model. ACM Conference on Computer and Communications Security, pages 1247–1260, 2013.

9. Martina Lindorfer, Matthias Neumayr, *Juan Caballero*, Christian Platzer. POSTER: Cross-Platform Malware: Write Once, Infect Everywhere. Proceedings of the 20th ACM Conference on Computer and Communications Security, November 2013.

10. M. Zubair Rafique, *Juan Caballero*. FIRMA: Malware Clustering and Network Signature Generation with Mixed Network Behaviors. Proceedings of the 16th International Symposium on Research in Attacks, Intrusions and Defenses, October 2013.

11. P. Chico de Guzmán, *M. Carro*, *M. Hermenegildo*. Supporting Pruning in Tabled LP. Practical Aspects of Declarative Languages (PADL'13), LNCS, Springer Verlag, January 2013.

12. *Andrea Cerone*, Matthew Hennessy, Massimo Merro. Modelling MAC-Layer Communications in Wireless Systems. In Coordination Models and Languages, volume 7890 of Lecture Notes in Computer Science, pages 16-30. Springer, 2013. **Best paper award.**

13. *Carolina Dania*, *Manuel Clavel*. OCL2FOL+: Coping with Undefinedness. Proceedings of the MODELS 2013 OCL Workshop co-located with the 16th International ACM/IEEE Conference on Model Driven Engineering Languages and Systems (MODELS 2013), Miami, USA, September 30, 2013, CEUR Workshop Proceedings, Vol. 1092, pages 53–62, CEUR-WS.org, 2013.

14. *Germán Andrés Delbianco*, *Aleksandar Nanevski*. Hoare-Style Reasoning With (Algebraic) Continuations. Proceedings of the 18th ACM SIGPLAN international conference on Functional programming, ICFP '13, pages 363–376, ACM, 2013.

15. *Goran Doychev*, Dominik Feld, *Boris Köpf*, *Laurent Mauborgne*, Jan Reineke. CacheAudit: A Tool for the Static Analysis of Cache Side Channels. 22nd USENIX Security Symposium, USENIX, 2013.

16. Michael Backes, *Goran Doychev*, *Boris Köpf*. Preventing Side-Channel Leaks in Web Traffic: A Formal Approach. Proc. 20th Network and Distributed Systems Security Symposium (NDSS), Internet Society, 2013.

17. Javier Esparza, *Pierre Ganty*, Rupak Majumdar. Parameterized Verification of Asynchronous Shared-Memory Systems. CAV'13: Proc. 23rd Int. Conf. on Computer Aided Verification, LNCS, Vol. 8044, pages 124–140, Springer, 2013.

18. *Pierre Ganty*, Samir Genaim. Proving Termination Starting from the End. CAV'13: Proc. 23rd Int. Conf. on Computer Aided Verification, LNCS, Vol. 8044, pages 397–412, Springer, 2013.

19. *Pierre Ganty*, Radu Iosif, Filip Konecný. Underapproximation of Procedure Summaries for Integer Programs. TACAS'13: Proc. 19th Int. Conf. on Tools and Algorithms for the Construction and Analysis of Systems, LNCS, Vol. 7795, pages 247–261, Springer, 2013.

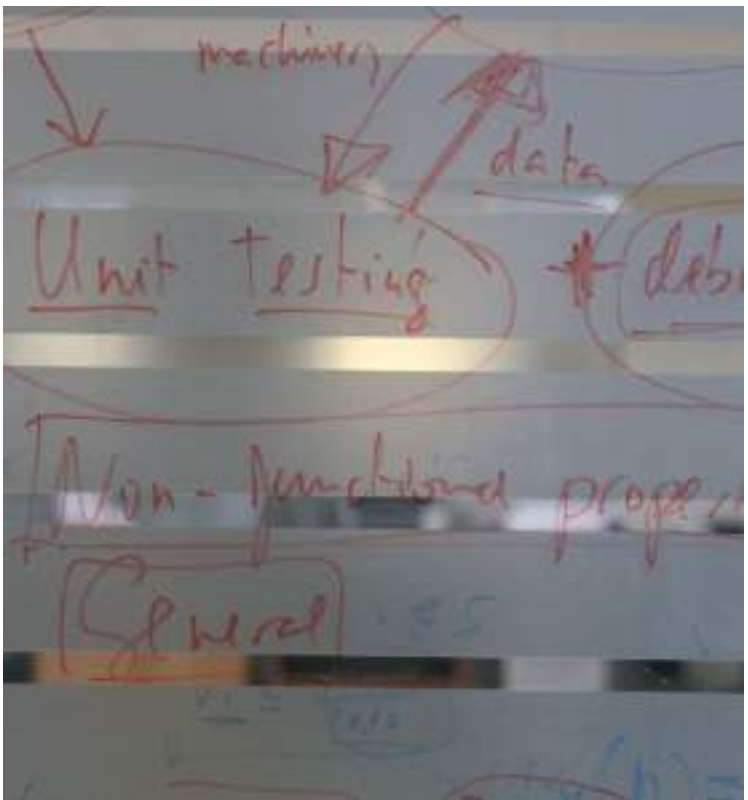
20. *Álvaro García-Pérez*, Pablo Nogueira, *Ilya Sergey*. Deriving Interpretations of the Gradually-Typed Lambda Calculus. Proceedings of the ACM SIGPLAN 2014 workshop on Partial evaluation and program manipulation, PEPM 2014, pages 157–168, ACM, 2014.

21. *Álvaro García Pérez*, Pablo Nogueira, *Juan José Moreno Navarro*. Deriving the Full-reducing Krivine Machine from the Small-step Operational Semantics of Normal Order. Proceedings of the 15th Symposium on Principles and Practice of Declarative Programming, PPDP '13, pages 85–96, ACM, 2013.

22. *Álvaro García Pérez*, Pablo Nogueira. A Syntactic and Functional Correspondence Between Reduction Semantics and Reduction-free Full Normalisers. Proceedings of the ACM SIGPLAN 2013 Workshop on Partial Evaluation and Program Manipulation, PEPM '13, pages 107–116, ACM, 2013.

23. Hagit Attiya, *Alexey Gotsman*, Sandeep Hans, Noam Rinetzky. A Programming Language Perspective on Transactional Memory Consistency. Proceedings of the 32nd ACM Symposium on Principles of Distributed Computing (PODC'13), Montreal, Canada, pages 309–318, ACM Press, 2013.

24. *Alexey Gotsman*, Noam Rinetzky, Hongseok Yang. Verifying Concurrent Memory Reclamation Algorithms With Grace. Proceedings of the 22nd European Symposium on Programming (ESOP'13), Rome, Italy, LNCS, Vol. 7792, pages 249–269, Springer, 2013.



25. Mark Batty, Mike Dodds, *Alexey Gotsman*. Library Abstraction for C/C++ Concurrency. Proceedings of the 40th ACM Symposium on Principles of Programming Languages (POPL'13), Rome, Italy, pages 235–248, ACM Press, 2013.

26. *Boris Köpf*, Andrey Rybalchenko. Automation of Quantitative Information-Flow Analysis. 13th International School on Formal Methods for the Design of Computer, Communication, and Software Systems (SFM), LNCS 7938, Springer, 2013.

27. Z. Drey, *J. F. Morales*, *M. V. Hermenegildo*, *M. Carro*. Reversible Language Extensions and their Application in Debugging. Practical Aspects of Declarative Languages (PADL'13), LNCS, Vol. 7752, Springer, January 2013.

28. Beta Ziliani, Derek Dreyer, Neelakantan R. Krishnaswami, *Aleksandar Nanevski*, Viktor Vafeiadis. Mtac: A Monad for Typed Tactic Programming in Coq. International Conference on Functional Programming (ICFP), pages 87–100, 2013.

29. Ruy Ley-Wild, *Aleksandar Nanevski*. Subjective Auxiliary State for Coarse-Grained Concurrency. Principles of Programming Languages (POPL), pages 561–574, 2013.

30. *Antonio Nappa*, M. Zubair Rafique, *Juan Caballero*. Driving in the Cloud: An Analysis of Drive-by Download Operations and Abuse Reporting. Proceedings of the 10th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, July 2013.

31. *Pavithra Prabhakar*, *Boris Köpf*. Verifying Information Flow Properties of Hybrid Systems. Proc. 2nd ACM International Conference on High Confidence Networked Systems (HiCoNS), ACM, 2013.

32. *Pavithra Prabhakar*, Parasara Sridhar Duggirala, Sayan Mitra, Mahesh Viswanathan. Hybrid Automata based CEGAR for Rectangular Hybrid Automata. VMCAI, 2013.

33. *Pavithra Prabhakar*, Jun Liu, and Richard M. Murray. Pre-Orders for Reasoning About Stability Properties With Respect to Input of Hybrid Systems. In Proceedings of the International Conference on Embedded Software, EMSOFT 2013, Montreal, QC, Canada, September 29 - Oct. 4, 2013. IEEE, 2013.

34. *Pavithra Prabhakar*, *Miriam Garcia Soto*. Abstraction-based Model-Checking of Stability of Hybrid Systems. In Natasha Sharygina and Helmut Veith, editors. Computer Aided Verification - 25th International Conference, CAV 2013, Saint Petersburg, Russia, July 13-19, 2013. Proceedings, volume 8044 of Lecture Notes in Computer Science. Springer, 2013.

35. *Pavithra Prabhakar*, Mahesh Viswanathan. On the Decidability of Stability of Hybrid Systems. In Calin Belta and Franjo Ivancic, editors. Proceedings of the 16th international conference on Hybrid systems: computation and control, HSCC 2013, April 8-11, 2013, Philadelphia, PA, USA. ACM, 2013.

36. Scott C. Livingston, *Pavithra Prabhakar*, Alex B. Jose, and Richard M. Murray. Patching Task-Level Robot Controllers Based on a Local-Calculus Formula. In 2013 IEEE International Conference on Robotics and Automation, Karlsruhe, Germany, May 6-10, 2013. IEEE, 2013.

37. Necmiye Ozay, Jun Liu, *Pavithra Prabhakar*, and Richard M Murray. Computing Augmented Finite Transition Systems to Synthesize Switching Protocols for Polynomial Switched Systems. In American Control Conference (ACC), 2013, pages 6237-6244. IEEE, 2013.

38. Dominique Devriese, *Ilya Sergey*, Dave Clarke, Frank Piessens. Fixing Idioms: a Recursion Primitive for Applicative DSLs. Proceedings of the ACM SIGPLAN 2013 Workshop on Partial Evaluation and Program Manipulation, PEPM 2013, pages 97–106, ACM, 2013.

39. *Ilya Sergey*, Dominique Devriese, Matthew Might, Jan Midtgaard, David Darais, Dave Clarke, Frank Piessens. Monadic Abstract Interpreters. Proceedings of the 34th ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI '13, pages 399–410, ACM, 2013.

40. *A. Serrano*, *P. Lopez-Garcia*, F. Bueno, *M. Hermenegildo*. Sized Type Analysis for Logic Programs (Technical Communication). Theory and Practice of Logic Programming, 29th Int'l. Conference on Logic Programming (ICLP'13) Special Issue, On-line Supplement, Vol. 13, Num. 4-5, pages 1–14, Cambridge U. Press, August 2013.

41. Simon Meier, *Benedikt Schmidt*, Cas Cremers, David Basin. The tamarin prover for the symbolic analysis of security protocols. Computer Aided Verification - 25th International Conference, CAV 2013, Saint Petersburg, Russia, July 13-19, 2013. Proceedings, volume 8044 of Lecture Notes in Computer Science, pages 696–701. Springer, 2013.

42. Cédric Fournet, Nikhil Swamy, Juan Chen, Pierre-Évariste Dagand, *Pierre-Yves Strub*, Benjamin Livshits. Fully abstract compilation to JavaScript. Proceedings of the 40th ACM Symposium on Principles of Programming Languages (POPL'13), Rome, Italy, pages 371–384, ACM Press, 2013.

43. Karthikeyan Bhargavan, Markulf Kohlweiss, Alfredo Pironti, *Pierre-Yves Strub*. Implementing TLS with Verified Cryptographic Security. Proceedings of the 2013 IEEE Symposium on Security and Privacy, (SP'13), Berkeley, CA, USA, pages 445-459, IEEE Press, 2013.

### Workshops

1. *Álvaro García Pérez*, Pablo Nogueira, *Ilya Sergey*. Derivación de intérpretes del cálculo lambda con tipos graduales. V Taller de Programación Funcional TPF 2013, September 17 2013. Charla impartida en el V Taller de Programación Funcional TPF 2013.

2. *Dragan Ivanović*, Peerachai Kaowichakorn, and *Manuel Carro*. Towards QoS Prediction Based on Composition Structure Analysis and Probabilistic Environment Models. In D. Bianculli, P. Lago, G.A. Lewis, and H-Y. Paik, editors, 5th international workshop on principles of engineering service-oriented systems (PESOS 2013), May 2013.

3. *Dragan Ivanović*. Implementing Constraint Handling Rules as a Domain-Specific Language Embedded in Java. In Rémy Haemmerlé and José Francisco Morales, editors, Proceedings of the 23rd Workshop on Logic-based methods in Programming Environments (WLPE 2013), August 2013.

4. *U. Liqat*, S. Kerrison, *A. Serrano*, K. Georgiou, *P. Lopez-Garcia*, N. Grech, *M.V. Hermenegildo*, K. Eder. Energy Consumption Analysis of Programs based on XMOS ISA-Level Models. Pre-proceedings of the 23rd International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR'13), September 2013.

5. *A. Serrano*, *P. Lopez-Garcia*, *M. Hermenegildo*. Towards an Abstract Domain for Resource Analysis of Logic Programs Using Sized Types. 23rd Workshop on Logic-based Methods in Programming Environments (WLPE 2013), 15 pages, August 2013.

### 6.1.2 Articles in Books and other Collections

1. *Anindya Banerjee*, David A. Naumann. State Based Encapsulation for Modular Reasoning about Behavior-Preserving Refactorings. Aliasing in Object-Oriented Programming, Lecture Notes in Computer Science, Vol. 7850, pages 319–365, Springer, 2013.

2. Dave Clarke, Johan Östlund, *Ilya Sergey*, Tobias Wrigstad. Ownership Types: A Survey. Aliasing in Object-Oriented Programming. Lecture Notes in Computer Science, Vol. 7850, pages 18-64, Springer, 2013.

### 6.1.3 Edited Volumes

1. Rémy Haemmerlé, *José F. Morales*. Proceedings of the 23rd Workshop on Logic-based methods in Programming Environments (WLPE 2013). Vol. abs/1308.2055, 2013.

### 6.1.4 Doctoral and Master Theses

1. Dragan Ivanović. Analysis of Service-Oriented Computing Systems. PhD Thesis. Technical University of Madrid (UPM). January 2013. Advisor: Manuel Carro (IMDEA Software Institute and UPM).

2. Nataliia Stulova. Dynamic Checking of Assertions for Higher-order Predicates. MSc. Thesis. Technical University of Madrid (UPM). July, 203. Advisors: Manuel Hermenegildo (IMDEA Software Institute and UPM) and Jose Morales (IMDEA Softtware Institute).

## invited talks

## 6.2 Invited Talks

### 6.2.1 Invited and Plenary Talks by IMDEA Scientists

1. *Gilles Barthe*. Invited talk at the European Joint Conferences on Theory and Practice of Software (ETAPS 2013).

2. *Gilles Barthe*. Invited talk at the 10th International Conference on Quantitative Evaluation of SysTems (QEST 2013).

3. *Gilles Barthe*. Invited talk at the 18th Nordic Conference on Secure IT Systems (NordSec 2013).

4. *Juan Caballero*. Specialization in the Malware Distribution Ecosystem. Invited talk at GreHack 2013 in Grenoble, France, November 2013.

5. *Juan Caballero*. Measuring Pay-per-Install: The Commoditization of Malware Distribution. Invited talk at the Second System Security Workshop, in Bochum, Germany, July 2013.

6. *Juan Caballero*. MALICIA Project. 38th Annual meeting of the Messaging, Malware, and Mobile Anti-Abuse Working Group in Vienna, Austria, July 2013.

7. *John Gallagher*. Verification by Abstraction and Specialisation of Constraint Logic Programs. Invited talk at Rich Model Toolkit COST Action Meeting, Malta, June 2013.

8. *Alexey Gotsman*. Abstraction for Weakly Consistent Systems. Invited talk at 3rd Workshop on Formal Methods in the Development of Software (WF-FMDS 2013).

9. *Alexey Gotsman*. Understanding Eventual Consistency. Invited talk at REORDER/EC2 2013.

10. *Manuel Hermenegildo*. Analysis and Verification 'of and with' CLP. Keynote speech at COST action "rich model toolkit" meeting, Malta, 2013.

11. *Boris Köpf*. Invited talk at the 13th International School on Formal Methods for the Design of Computer, Communication and Software Systems (SFM 2013).

12. *Boris Köpf*. Invited talk at the Workshop on Foundations of Computer Security (FCS 2013).

13. *Pedro López García*. The CiaoPP Resource Usage Analysis and Verification Framework. Invited talk at Sixth Energy Aware Computing Workshop (EACO), Bristol, UK, March 2013.

14. *José Morales*. The Ciao Language. Invited talk at LogicBlox User Days 2013, Atlanta, USA.

15. *Ilya Sergey*. Monadic Abstract Interpreters. Invited talk at the 15th International Symposium on Principles and Practice of Declarative Programming (PPDP 2013). Madrid, Spain. September 2013.

16. *Ilya Sergey*. Communicating State Transition Systems for Fine-Grained Concurrent Resources. Invited talk at 2nd ACM SIGPLAN Workshop on Higher-Order Programming with Effects (HOPE 2013). Boston, MA, USA. September 2013.


## 6.2.2 Invited Seminars and Lectures by IMDEA Scientists

1. *Juan Caballero*. Attack Drivers and Attack Mechanisms. 2nd Building Trust in the Information Age Summer School in Cagliary, Italy, September 2013.

2. *Manuel Carro*. Invited speaker at the "Digital cities of the Future" meeting, Trento, September 2013.

3. *Manuel Carro*. Enseñando concurrencia con modelos formales. Joint work with Ángel Herranz and Julio Mariño. Seminario de Investigación en Tecnologías de la Información Aplicadas a la Educación (SITIAE 2013), Madrid, April 2013.

4. *Dario Fiore*. Invited speaker at the 2nd PROMETIDOS Winter School. Madrid, December 2013.

5. *Pierre Ganty*. Parametrized Verification of Asynchronous Shared-Memory Systems. Laboratoire d'Informatique Algorithmique: Fondements et Applications, Université Paris 7, April 2013.

6. *Pierre Ganty*. Proving Termination Starting From the End. École Polytechnique Fédérale de Lausanne, March 2013; at Laboratoire d'Informatique Algorithmique: Fondements et Applications, Université Paris 7, April 2013.

7. *Alexey Gotsman*. Consistency in Concurrent and Distributed Systems. Invited tutorial at 40th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2013).

8. *Boris Köpf*. Invited talk at the 20th Escuela de Verano de Ciencias Informáticas (RIO 2013).

9. *Juan José Moreno*. Does More Data and ICT Make Cities Smarter? IEEE SmartMile 2013.

10. *Juan José Moreno*. ¿Qué hay de nuevo en la universidad digital? , Seminario La Universidad Digital, Catedra Unesco de Gestión y Política Universitaria Madrid, Noviembre 2013.

11. *Juan José Moreno*. Algunos desafíos de las TIC en las Universidades, Sociedad de la Información: TIC en las Universidades, Revista SOCINFO, Madrid, Marzo 2013.

12. *Pavithra Prabhakar*. Invited speaker at the Automatic Control Laboratory, KTH Royal Institute of Technology, Stockholm, Sweden. November, 2013:

13. *Pavithra Prabhakar*. Invited talk in the Department of Automatic Control and Systems Engineering, University of Sheffield. November, 2013.

14. *Pavithra Prabhakar*. Invited speaker in the Department of Computer Science, University of Oxford. November, 2013.

15. *Pavithra Prabhakar*. Invited speaker at the Toyota Technical Center. October, 2013.

16. *Pavithra Prabhakar*. Invited speaker at the Centre Federe en Verification, University Libre de Bruxelles, Belgium. February, 2013.

17. *Pavithra Prabhakar*. Invited speaker at Verimag, Grenoble, France. January, 2013.

18. *Pavithra Prabhakar*. Invited lecturer at the CPS Summer School. Organized by EIT-ICT Labs and PERSYVAL Labs. June, 2013.

19. Benedikt Schmidt. Invited talk at the 2nd PROMETIDOS Winter School. Madrid, December 2013.

20. Benedikt Schmidt. Invited talk at the 1st CERIST Autumn School on Cyber-Physical Systems. Algiers, Algeria, October 2013.

### 6.2.3 Invited Speaker Series

During 2013, 16 external speakers were invited to give talks at IMDEA Software. The following list gives the speakers and the titles of their talks.

1. *Aleksandar Dimovski*. PhD Student, FON University, Macedonia: Program Verification by Game Semantics: From Abstraction-Refinement to Symbolic Approach.

2. *Andrea Cerone*. PhD Student, Trinity College, Dublin, Ireland: Testing Wireless Networks.

3. *Dario Fiore*. Post-doctoral Researcher, Max Planck Institute for Software Systems, Germany: Provably-Secure Cryptography: theory and practice meet up to tackle modern challenges.

4. *Anthony W. Lin*. Post-doctoral Researcher, U. of Oxford: Reversal-bounded Acceleration of Counter Systems

5. *Radu Iosif*. Researcher, VERIMAG/CNRS, Grenoble, France: The Tree Width of Separation Logic with Recursive Definitions.

6. *Ivan Beschastnikh*. PhD Student, University of Washington, USA: Modeling Systems from Logs of their Behavior.

7. *Johannes Kinder*. Post-doctoral Researcher, EPFL, Switzerland: Basing Trust in Applications on More Than Pure Faith.

8. *Jorge A. Navas*. Post-doctoral Researcher, The University of Melbourne, Australia: Unbounded Model-Checking with Interpolation for Regular Language Constraints.

9. *Philipp Leitner*. Post-doctoral Researcher, Vienna University of Technology, Austria: Building Applications for the Infrastructure-as-a-Service Cloud with CloudScale.

10. *Tudor Dumitras*. Symantec Research Labs (SRL): Improving System Security with Big Data Techniques.

11. *Michael Emmi*. Post-doctoral Researcher, LIAFA, Université Paris Diderot: Concurrent Software Modeling and Analysis: Recursively Parallel Programs.

12. *Neng-Fa Zhou*. Professor, The City University of New York: The Picat Language and System.

13. *Gopal Gupta*. Professor, The University of Texas at Dallas, USA: Logic, Coinduction and Infinite Computation.

14. *Cesare Tinelli*. Professor, The University of Iowa, USA: SMT-based Model Checking.

15. *Roberto Di Cosmo*. Professor, Universite Paris Diderot, Director IRILL: The Aeolus approach to Cloud automation.

16. *Alessandro Orso*. Professor, Georgia Institute of Technology, USA: Automated Debugging: Are We There Yet?

### 6.2.4 Software Seminar Series

The Institute also holds an internal seminar series to foster communication and collaboration. A total of 30 seminars were given in 2013.

## 6.3 Scientific Service and Other Activities

### 6.3.1 Participation in Program Committees

Gilles Barthe:

1. IEEE 26th Computer Security Foundations Symposium (CSF 2013).

2. 2nd Conference on Principles of Security and Trust (POST 2013).

3. 9th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC-FSE) Tools 2013.

Juan Caballero:

4. 20th ACM Conference on Computer and Communications Security (CCS 2013) – Poster track.

5. 16th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2013).

6. 10th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2013).

7. 22nd Intenational World Wide Web Conference (WWW 2013).

8. 34th IEEE Symposium on Security & Privacy (IEEE S&P 2013).

9. 2nd ACM SIGPLAN Program Protection and Reverse Engineering Workshop (PPREW 2013).

Manuel Carro:

**10.** 35th International Conference on Software Engineering (ICSE 2013).

**11.** 29th International Conference on Logic Programming (ICLP 2013).

**12.** European Conference on Service-Oriented and Cloud Computing (ESOCC 2013).

**13.** 15th International Symposium on Principles and Practice of Declarative Programming (PPDP 2013).

**14.** XIII Jornadas sobre Programación y Lenguajes (PROLE 2013).

**15.** 11th International Conference on Service Oriented Computing (ICSOC 2013).

Manuel Clavel:

**16.** 13th International Workshop on OCL, Model Constraint and Query Languages (OCL 2013).

John Gallagher:

**17.** 29th International Conference on Logic Programming (ICLP 2013).

**18.** 12th Scandinavian AI conference (SCAI 2013).

**19.** 23rd Workshop on Logic-based methods in Programming Environments (WLPE'2013).

Pierre Ganty:

**20.** 7th International workshop on Reachability Problems (RP 2013).

**21.** 14th International Symposium on Verification, Model Checking and Abstract Interpretation (VMCAI 2013).

Alexey Gotsman:

**22.** 30th International Colloquium on Automata, Languages and Programming (ICALP 2013).

Manuel Hermenegildo:

**23.** 40th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2013).

**24.** 29th International Conference on Logic Programming (ICLP 2013).

**25.** 23rd International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR 2013).

**26.** Logic for Programming Artificial Intelligence and Reasoning (LPAR 2013).

**27.** Spanish Conference on Computer Science (CEDI 2013).

Dragan Ivanović:

**28.** 5th International Workshop on Principles of Engineering Service-Oriented Systems (PESOS 2013).

Boris Köpf:

**29.** IEEE Workshop on Privacy and Anonymity for the Digital Economy (PADE 2013).

**30.** 26th IEEE Computer Security Foundations Symposium (CSF 2013).

**31.** 10th International Conference on Quantitative Evaluation of Systems (QEST 2013).

**32.** 9th International Conference in Information Security Practice and Experience (ISPEC 2013).

**33.** 2nd Conference on Principles of Security and Trust (POST 2013).

José Morales:

**34.** 13th International Colloquium on Implementation of Constraint and Logic Programming Systems (CICLOPS 2013).

**35.** 23rd Workshop on Logic-based methods in Programming Environments (WLPE'2013).

**36.** International Conference on Logic Programming (ICLP) Doctoral Consortium 2013.

Juan José Moreno:

**37.** XIII Jornadas sobre Programación y Lenguajes (PROLE 2013).

**38.** XVIII edición de las Jornadas de Ingeniería del Software y Bases de Datos (JISBD 2013).

**39.** IX Jornadas de Ciencia e Ingeniería de Servicios (JCIS 2013).

Aleksandar Nanevski:

**40.** 22nd European Symposium on Programming (ESOP 2013).

Pavithra Prabhakar:

**41.** Hybrid Systems: Computation and Control (HSCC 2013).

César Sanchez:

**42.** Formal Methods in Computer-Aided Design (FMCAD 2013).

**43.** 5th IPM International Conference on Fundamentals of Software Engineering (FSEN 2013).

### 6.3.2 Conference and Program Committee Chairmanship

Juan Caballero:

**1.** TPC vice-chair for the 13th Annual Digital Forensics Research Conference (DFRWS 2013).

Boris Köpf:

**2.** Workshop on Quantitative Aspects in Security Assurance (QASA 2013).

Juan José Moreno:

**3.** Spanish Conference on Computer Science (CEDI 2013).

César Sanchez:

**4.** 20th International Symposium on Temporal Representation and Reasoning (TIME 2013).

### 6.3.3 Editorial Boards and Conference Steering Committees

Gilles Barthe:

**1.** Editorial board of the Journal of Automated Reasoning.

**2.** Editorial board of the Journal of Computer Security.

**3.** Steering committee of Principles of Security and Trust (POST).

**4.** Steering committee of the European Joint Conferences on Theory and Practice of Software (ETAPS).

**5.** Steering committee of Trustworthy Global Computing (TGC).



Manuel Carro:

**6.** Conference Coordinator of the Association for Logic Programming (ALP).

John Gallagher:

**7.** Editorial board of Theory and Practice of Logic Programming (Cambridge Univ. Press). Area Editor for Technical Notes and Rapid Publications.

Manuel Hermenegildo:

**8.** Steering Committee of the Static Analysis Symposium (SAS).

**9.** Steering Committee of the International Symposium on Functional and Logic Programming (FLOPS).

**10.** Steering Committee of the International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI).

**11.** Editorial Advisor and former Area Editor (architecture and implementation) of "Theory and Practice of Logic Programming" (Cambridge U. Press)

**12.** Associate Editor of the "Journal of New Generation Computing" (Springer-Verlag)

**13.** Area Editor of "Journal of Applied Logic" (Elsevier North-Holland).

**14.** Board of the Logic Journal of the IGPL

### 6.3.4 Association and Organization Committees

Juan Caballero:

**1.** Working Group 3 "Secure ICT Research and Innovation" of the European Commission Public-Private Platform on Network and Information Security (NIS).

Manuel Carro:

**1.** Representative of the Technical University of Madrid (UPM) at the SpaRCIM steering board.

**2.** SpaRCIM deputy representative at ERCIM.

Dario Fiore:

**3.** Management Committee member (representing Spain) of COST Action IC1306 "Cryptography for Secure Digital Interaction."

Manuel Hermenegildo:

**4.** Elected member Informatics Europe steering board.

**5.** Elected President of SpaRCIM.

**6.** Member *Academia Europaea*.

**7.** Member Dagstuhl scientific advisory board.

**8.** Member IRILL (French Free Software Institute) scientific board.

**9.** Member Informatics Europe department evaluation board.

**10.** Member IFCoLog advisory board.

José Morales:

**11.** 13th International Colloquium on Implementation of Constraint and Logic Programming Systems (CICLOPS 2013).

Juan José Moreno:

**12.** Jury member of the Innovative Companies Forum 2013.

Pavithra Prabhakar:

**13.** European Control Conference (ECC 2013): Invited session on Formal Verification and Design of Hybrid Systems.

César Sánchez:

**14.** Workshop on Synthesis, Verification and Analysis of Rich Models: Rome, 20-21 January 2013 (collocated with POPL'13 and VMCAI'13).

## 6.4 Awards

Conference Paper Awards:

**1.** *Gilles Barthe*, *Juan Manuel Crespo*, Sumit Gulwani, *César Kunz*, *Mark Marron*. From Relational Verification to SIMD Loop Synthesis. ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming, PPoPP '13, pages 123–134, ACM, 2013. **Best paper award.**

**2.** *Andrea Cerone*, Matthew Hennessy, Massimo Merro. Modelling MAC-layer communications in wireless systems. In Coordination Models and Languages, volume 7890 of Lecture Notes in Computer Science, pages 16-30. Springer, 2013. **Best paper award.**

Thesis Awards:

**3.** *Benedikt Schmidt*: **ETH Medal for Outstanding PhD Thesis.**

Other Awards:

**4.** *Juan José Moreno*: **Technical University of Madrid (UPM) Medal.**

awards

# scientific highlights



annual report 2013

# computer-aided cr

## Computer-Aided Cryptographic Proofs

To deal with the rising complexity of cryptographic proofs, researchers from IMDEA Software Institute and INRIA have been developing EasyCrypt, an SMT-based tool for writing and checking complex cryptographic security proofs. Although development is still ongoing, the tool has had some early successes in identifying and filling gaps in proofs of widely deployed cryptographic specifications. The team is now considering two main directions for applications of the tool: proof automation and applications to real-world cryptographic systems.

Proof automation, embodied in the ZooCrypt tool, has already led to an exhaustive classification of encryption schemes based on RSA [1], and the discovery of a new and efficient scheme, called ZAEP [2]. Work is ongoing to provide automation for a wider class of cryptographic schemes, including pairing-based cryptography.

The second direction aims at making use of the proven efficiency of SMT solvers in program verification to carry formal security proofs over to concrete implementations of cryptography. In addition to bridging the gap between specifications and implementations, the resulting security proofs also consider stronger adversaries that may obtain or influence information about secret data via leakage. This has already led to an application where a verifiably secure x86 implementation of the PKCS#1 standard was obtained, combining EasyCrypt with the CompCert verified compiler [3]. Work is ongoing to consider even stronger adversaries that may obtain information through the sequence of memory accesses (*cache attacks*) or by interfering with the execution of the program (*fault injection*).

Externally, EasyCrypt is used at the Microsoft Research-INRIA joint centre in a formal proof of the TLS protocol, and at the MIT Lincoln Laboratory, as part of AutoCrypt, a joint project of the IMDEA Software Institute and Stanford University, University of Pennsylvania and SRI. The project funded by the US Office of Naval Research (ONR), with a total budget of EUR 2 million and runs from 2012 to 2015. As a part of the

# yptographic proofs

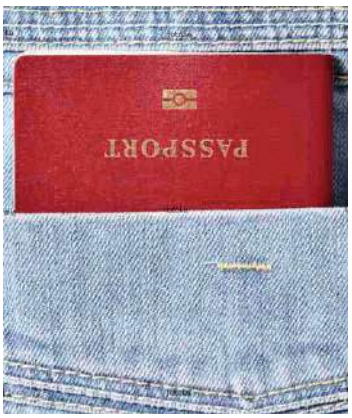
AutoCrypt project, a summer school and workshop dedicated to EasyCrypt took place at the University of Pennsylvania in July 2013, gathering more than 30 participants.

## Related publications

[1] G. Barthe, J. Crespo, B. Grégoire, C. Kunz, Y. Lakhnech, B. Schmidt and S. Zanella-Béguelin, "Fully automated analysis of padding-based encryption in the computational model," in 20th ACM conference on computer and communications security, CCS 2013. 2013, pp. 1247–1260.

[2] G. Barthe, D. Pointcheval and S. Zanella-Béguelin, "Verified security of redundancy-free encryption from Rabin and RSA," in 19th ACM conference on computer and communications security, CCS 2012. 2012, pp. 724–735.

[3] J.B. Almeida, M. Barbosa, G. Barthe and F. Dupressoir, "Certified computer-aided cryptography: efficient provably secure machine code from high-level implementations," in 20th acm conference on computer and communications security, CCS 2013. 2013, pp. 1217–1230.




energy tran

for developing energy-efficient software

# Energy Transparency for Developing Energy-Efficient Software

An important part of the IMDEA Software Institute's research on energy-efficient software development is performed in the context of the EU FP7 FET project "ENTRA: Whole-Systems Energy Transparency," in collaboration with Roskilde University (Denmark), the University of Bristol (UK) and XMOS Ltd (UK) (described in Chapter 5).

Achieving energy transparency through the system layers, from machine code to source code, implies that energy consumption at the hardware layer should be immediately visible at the layer at which software is designed or used. This requires an important effort on developing novel analyses and combined hardware-software energy modeling. Energy transparency enables program verification and optimization, which are also important topics to be investigated in the project. Based on the energy transparency concept, ENTRA proposes a novel, holistic, energy-aware system development approach that covers hardware, software, and the run-time environment, making information on energy usage available throughout the system layers and promoting optimizations both during code development and at run time.

The ENTRA project successfully passed its first year evaluation in November 2013. Among the results from the first year is a novel analysis framework for statically estimating the energy consumption of programs using low level energy models [2,3,4]. The definition of an assertion language allowing energy models to be integrated with static analysis tools, and initial energy optimization techniques [1]. The project's second year focuses on developing prototype tools for analyzing energy usage as well as program energy optimization techniques.

# sparency

ENTRA
Whole-Systems Energy Transparency

University of BRISTOL

XMOS®

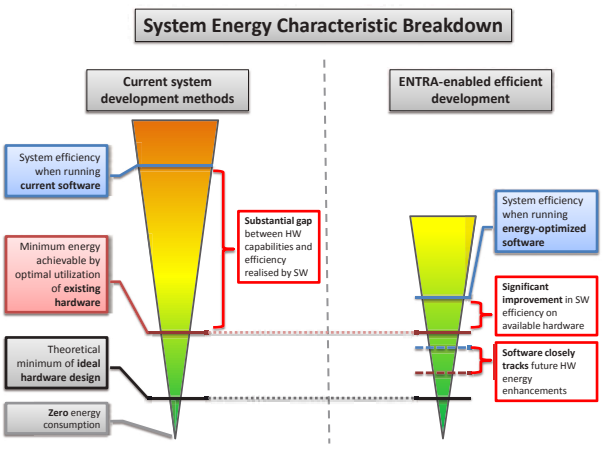
## Related publications

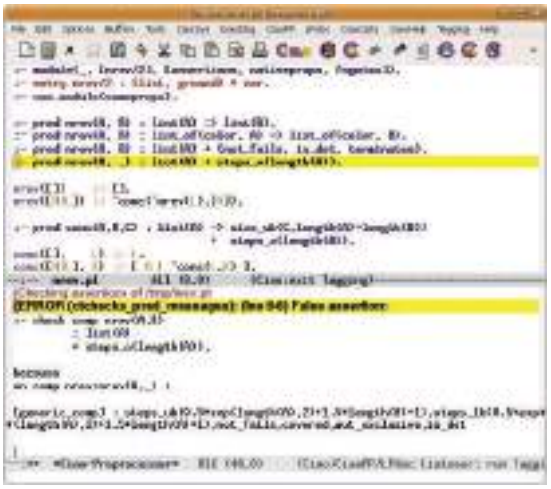
[1] Z. Banković and P. Lopez-Garcia. Genetic Algorithm-based Allocation and Scheduling for Voltage and Frequency Scalable XMOS Chips. In *Hybrid Artificial Intelligent Systems*, volume 8073 of *Lecture Notes in Computer Science*, pages 401–410. Springer, 2013.

[2] U. Liqat, S. Kerrison, A. Serrano, K. Georgiou, P. Lopez-Garcia, N. Grech, M.V. Hermenegildo, and K. Eder. Energy Consumption Analysis of Programs based on XMOS ISA-level Models. In *Pre-proceedings of the 23rd International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR'13)*, September 2013.

[3] A. Serrano, P. Lopez-Garcia, F. Bueno, and M. Hermenegildo. Sized Type Analysis for Logic Programs (technical communication). In T. Swift and E. Lamma, editors, *Theory and Practice of Logic Programming, 29th Int'l. Conference on Logic Programming (ICLP'13) Special Issue, On-line Supplement*, volume 13, pages 1–14. Cambridge U. Press, August 2013.

[4] A. Serrano, P. Lopez-Garcia, and M. Hermenegildo. Towards an Abstract Domain for Resource Analysis of Logic Programs Using Sized Types. In R. Haemmerlé and J. F. Morales, editors, *23rd Workshop on Logic-based Methods in Programming Environments (WLPE 2013)*, August 2013.



architecture-dri

# Architecture-Driven Verification of Systems Software

of systems software

The research in architecture-driven verification of system software at the IMDEA Software Institute is performed in part within the scope of the EU project ADVENT, an FP7 FET Young Explorers project started in 2013 and coordinated by IMDEA Software in cooperation with Katholieke Universiteit Leuven (Belgium), Max Planck Institute for Software Systems (Germany) and Tel-Aviv University (Israel). The research is also supported by a Microsoft Software Engineering Innovation Foundation Award and a Microsoft European PhD Scholarship.

The key element of the ADVENT approach is to base the design of advanced verification techniques on formalization of software engineering concepts already used by systems programmers to reason about their software informally. By taking advantage of programmers' knowledge and intuition, this approach improves on the common practice of building generic verification tools that fail to scale to big and complicated systems.

The architecture-driven techniques have the potential to result in verification tools that require a minimal and intuitive user input — essentially equivalent to a formal version of the high-level informal specifications programmers already have in mind when developing software. In time, this can yield a dramatic leap in the cost-benefit ratio of the verification technology, allowing it to scale to systems of real-world size and complexity that have so far been beyond the reach of quality assurance methods for guaranteeing correctness.

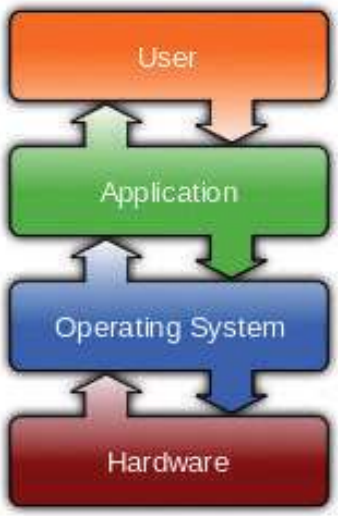
# ven verification



## Related publications

[1] Hagit Attiya, *Alexey Gotsman*, Sandeep Hans, Noam Rinetzky. A Programming Language Perspective on Transactional Memory Consistency. Proceedings of the 32nd ACM Symposium on Principles of Distributed Computing (PODC'13), Montreal, Canada, pages 309–318, ACM Press, 2013.

[2] Sebastian Burckhardt, *Alexey Gotsman*, Hongseok Yang, Marek Zawirski: Replicated data types: specification, verification, optimality. Proceedings of POPL 2014. ACM Press, 2014.




automatic gene

application configurations

# Automatic Generation of Cloud Application Configurations

The IMDEA Software Institute has just completed its participation in the EU FP7 project 4CaaSt, involving a number of key industrial and research organizations in Europe that are active in the cloud computing arena. The project concentrated on developing an advanced Platform-as-a-Service (PaaS) Cloud supporting optimized and elastic hosting of Internet-scale multi-tier applications.

The main contribution by IMDEA Software to 4CaaSt has been in designing and developing an Advanced Blueprint Resolution Engine, a key component of the 4CaaSt architecture. This engine is responsible for efficiently generating cloud application configurations from abstract specifications (blueprints) of components, such as functional units of business logic, Web-based user interface modules, RESTful and WSDL-based Web services for interoperability with other systems, back end databases, application servers, virtual networks, and virtual machines.

The IMDEA Software Institute used its extensive experience in software engineering, language design, and constraint logic programming to ensure the efficiency and completeness of the resolution engine, whose results, based on the functional and elasticity requirements and dependencies between components, can be further refined by applying Quality-of-Service (QoS) constraints. The related research concentrated on a technique for probabilistic modeling of service composition QoS and a tighter integration of the constraint logic programming tools with the mainstream cloud programming platforms.

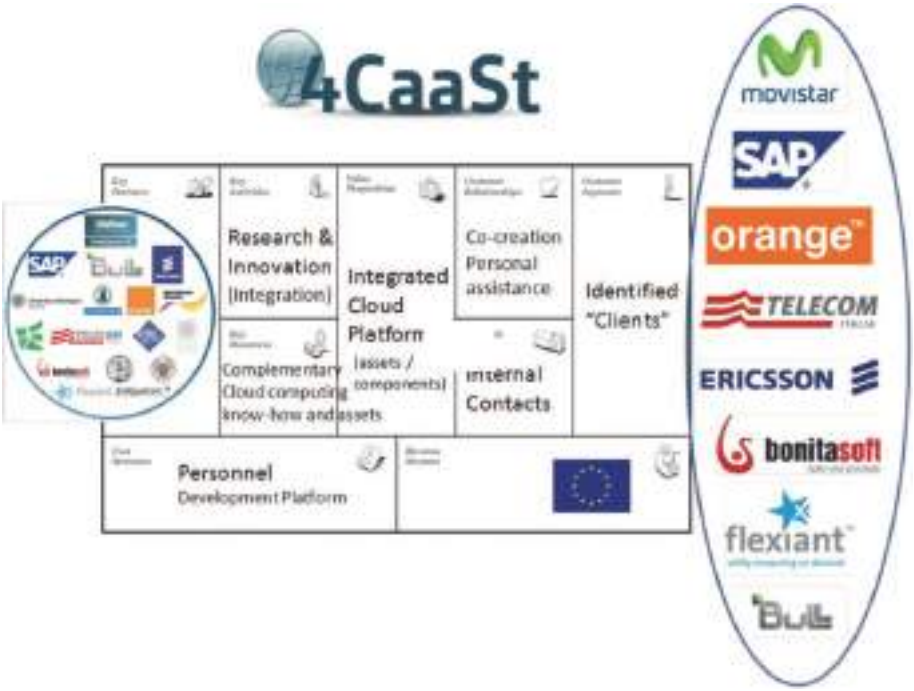
# ration of cloud



## Related publications

[1] Dragan Ivanović, Peerachai Kaowichakorn, and Manuel Carro. Towards QoS Prediction Based on Composition Structure Analysis and Probabilistic Environment Models. In D. Bianculli, P. Lago, G.A. Lewis, and H-Y. Paik, editors, 5th international workshop on principles of engineering service- oriented systems (PESOS 2013), May 2013.

[2] Dragan Ivanović, Implementing Constraint Handling Rules as a Domain-Specific Language Embedded in Java. In Rémy Haemmerlé and José Francisco Morales, editors, Proceedings of the 23rd Workshop on Logic-based methods in Programming Environments (WLPE 2013), August 2013.



editor
imdea software institute

graphic design
base 12 diseño y comunicación

photos on pages 12, 59, 63 y 86
Daniel Schäfer

legal deposit number
M-8.319-2014