VASCO

Validation de Systèmes, Composants et Objets logiciels

Head of the VASCO team: Yves LEDRU (PR UGA)

The research of the VASCO team addresses modeling, verification and validation (V&V) of systems. Models play a key role in our V&V activities. On the one hand, they may provide a reference vs which some implementation can be verified. On the other hand, an existing system can be modelled and its model can then be verified giving some clues on the correctness of the actual system. In both cases, models must be validated, i.e. it should be shown that the model corresponds to the existing reality or to the needs of the customer.

The major industrial V&V activity is testing. The researches of the VASCO team are historically dedicated to testing. In the testing context, models play two roles: executable models can be used as oracles for the test, and model-based testing can generate test cases from a model.

The researches of the VASCO team pursue the following orientations:

Models as oracles. During the last five-years period, we dedicated significant efforts to the MODMED ANR project (2015-2019), which aimed at defining a language to express properties of execution traces. These properties play the role of a partial model, and can be evaluated on the traces. These traces can be produced by the execution of test cases, but also can be collected from the usage of the system.

Inferring models for test generation. In the recently started Philae ANR project (2018-2022), we still focus on traces collected from tests or from the usage of the system. But here, we exploit these traces to infer models of the system. These models will later be used to generate tests which themselves will produce new traces. They can also be studied to identify system faults.

Building models for verification. Building the model of a complex system is not an easy task. The VASCO team has a long experience of integrating graphical models (UML diagrams) and formal models (Z and B) for system verification. Since 2008, we are building the B4MSecure system which translates a Secure UML diagram, annotated with B assertions into B machines. The resulting formal model can then be verified using proof tools, model-checkers or animation.

Lightweight formal methods. Our research aims at facilitating the work of software engineers. This can be achieved by providing automation. Therefore most of our researches end up with the development of tools (e.g. SIMPA, ParTraP-IDE, B4MSecure/Meeduse). The lightweight approach to formal methods can also be achieved by supporting well-accepted modeling languages, such as UML, or designing intuitive languages such as ParTraP, our language to express trace properties.

In order to better understand the capabilities of our research, it is systematically applied to **case studies**. In the last 5 years, we have applied our research to the field of security, but also to the modelling of railway systems, and the verification of medical systems (computer-aided surgery).

1.1 Scientific Policy

The recommandations following the previous evaluation were the following ones:

- The team should establish long term industrial partnerships to ensure a minimum level of outside financing.
  - The VASCO team participates to projects with previous partners, both from academia and industry. For example, the Philae ANR project involves Smartesting and Orange, on the industrial side, and FEMTO-ST on the academic side. These partners were

involved with us in previous projects. Currently, we are participating to a tentative European project (ITEA labelled) which involves several known partners.

  - This does not prevent us from working with new partners, as illustrated by the ANR MODMED project which involves two companies from the Grenoble area.

- The team should better integrate its tools and make them interoperable. It should optimize the diffusion of its tools to create a community of users.

  - We have made significant efforts in these directions. First of all, tools B4MSecure and RoZ share a common architecture which improves their interoperability. Also, many tools are integrated as eclipse plugins, and efforts have been made to identify suitable open-source licences to distribute them. Nevertheless, we are far from having a community of users for most of our tools.

Activity profile

- Knowledge production: 30%
- Valorization and transfer: 40%
- Support of the scientific community: 10%
- Education through research: 20%

Our major activity is "Valorization and transfer", which includes our participation in numerous projects with industrials, and the development of publicly-available tools. "Knowledge production" comes in second place, involving our research activities and publications. "Education through research" comes in third place. It includes the supervision of PhD and Master students and our teaching activities at master's level. Finally comes "Support to the scientific community", with our involvement in national and regional networks and the organisation of scientific events (e.g. journées du GDR GPL and Grehack conference).

1.2 Key Achievements

Scientific breakthrough We achieved a specific scientific breakthrough with our hW-algorithm [32, 30]. It solves a problem that had been left open since the paper of Rivest in 1993 [27]. This problem, namely to infer a system without resetting it, was felt as a handicap by the community using active inference in software validation because all active inference algorithms needed resetting. This algorithm scales up easily to large automata, with minimal assumptions, and largely outperforms all previous tentative algorithms. It has the ability to make resetting superfluous, thus impacting existing methods.

Numerous research projects Besides this scientific breakthrough, the main achievement of the VASCO team during this 5 year period is its involvement in numerous research projects, mostly national projects (ANR MODMED, ANR SACADE, ANR PHILAE, PIA ARAMIS,...). Most of these projects involve industrials or third parties, and illustrate how the research results and tools of the team can be applied to various application domains.

Collaboration with Kobe (Japan) Since 2015, we have set up a strong collaboration with the University of Kobe (Japan). In 2015, Prof. Masahide Nakamura spent 10 months in the VASCO team. From 2015 until 2017, the PICS CNRS project "Intelligent d'accord mais aussi sûr et sécurisé" focused on the validation of smart systems, i.e. systems which learn from their environment. This project supported several visits of Lydie du Bousquet in Kobe. This collaboration led to a Memorandum of Understanding signed by UGA and the Univ. of Kobe. Finally, the ongoing Kouno-Tori project, financed by Auvergne-Rhône-Alpes region and coordinated by Lydie du Bousquet supports the visit of 4 students per year at the Univ. of Kobe.

Tools In 2018, the VASCO team, as part of the ANR MODMED project, delivered the ParTraP language, which is aimed at expressing properties of parametric traces. The delivery of this language includes a formal semantics, an integrated development environment distributed under the LGPL v3 license, and tools to ease the writing and understanding of properties. Publications [41, 8] about this language assessed the unique combination of its features.

Since 2008, the VASCO team has developed the B4MSecure environment, which translates SecureUML diagrams into B specifications. In 2018, the tool has been adapted to recent versions of the Eclipse/papyrus tool, and distributed under the LGPL v3 license. It was also used for our contributions to the NeXTRegio project of IRT Railenium.

Awards In 2016, the ITEA-2 project Diamonds (October 2010 - June 2013) was awarded "EUREKA Innovation Award 2015/2016" in the category 'Added Value' during the "EUREKA Week Innovation 2016 - Smart Cities - Sustainable & Gravitational Communities" .

In 2015, Amira Radhouani, PhD Student in the VASCO team was runner-up at the Grenoble Final of "Ma thèse en 180 secondes".

In 2015, the paper "Lightweight heuristics to retrieve parameter associations from binaries" [15] won the best paper award at the 5th Program Protection and Reverse Engineering Workshop, PPREW@ACSAC, Los Angeles.

In 2019, the paper "Quelques pas vers l'Honnêteté et l'Explicabilité de moteurs de recherche sur le Web" [22] won the best paper award at the COnférence en Recherche d'Information et Applications, CORIA'19, Villeurbanne, France.

Organisation of scientific event In 2018, all members of the VASCO team were involved in the organisation of the national days of GDR GPL (Génie de la programmation et du logiciel) in Grenoble June 12-15, 2018 and co-located events: french speaking conferences AFADL, CAL and CIEL.

2.1 Team members

Permanent Members			
Name	*Institution*	*Grade*	*Date*
DU BOUSQUET Lydie	UGA	PR	01/09/2011 -
FALCONE Ylies	UGA	MCF	01/09/2011 - 11/03/2015
GROZ Roland	G-INP	PR	01/09/2007 -
IDANI Akram	G-INP	MCF	01/10/2008 -
JACQUET Paul	G-INP	PR	01/01/2007 - 31/01/2014
LEDRU Yves	UGA	PR	01/01/2007 -
ORIAT Catherine	G-INP	MCF	01/09/2007 -
OUABDESSELAM Farid	UGA	PR	01/01/2007 - 31/08/2017
RICHIER Jean-luc	CNRS	CR	01/01/2007 - 30/09/2019

Non Permanent Members		
Name	*Status*	*Date*
BEN CHEIKH Ansem	Engineer	01/09/2017 - 31/08/2018
BLEIN Yoann	PhD Student	01/10/2015 - 30/09/2018
BREMOND Nicolas	Engineer	06/11/2017 - 08/06/2018
BREMOND Nicolas	Engineer	01/10/2018 - 24/05/2019
CHEHIDA Salim	Post-Doc	01/03/2018 - 31/03/2019
COLADON Titouan	Engineer	01/10/2016 - 05/03/2017
DE GOER DE HERVE Franck	PhD Student	01/10/2014 - 20/10/2017
DUCHENE Fabien	PhD Student	17/01/2011 - 02/06/2014
GUERTE Yves	Engineer	13/06/2016 - 31/10/2016
HOSSEN Karim	PhD Student	01/12/2010 - 31/12/2014
LANGET Matthieu	Engineer	20/02/2013 - 09/01/2014
NGUYEN Manh Dung	PhD Student	27/11/2017 - 27/11/2020
PERRIER Emmanuel	PhD Student	01/10/2014 - 11/05/2017
RADHOUANI Amira	PhD Student	01/10/2013 - 23/06/2017
REY Alexis	PhD Student	20/10/2017 - 31/12/2020
WANG Lingxiao	Post-Doc	01/06/2016 - 30/04/2017

The VASCO team has seen no incoming permanent member during the last five years. Three members have left the team: Paul Jacquet and Farid Ouabdesselam retired, Ylies Falcone joined the CORSE team in 2015. The team appeared as one of the possible target teams of three positions published in 2017, 2018 and 2019, but the recruited candidates joined other teams of the laboratory.

On January 1st 2019, VASCO counted 6 permanent members (L. du Bousquet, R. Groz, A. Idani, Y. Ledru, C. Oriat, J.-L. Richier), 3 PhD students, 1 post-doctoral researcher, 1 non-permanent engineer.

Several members of VASCO have been deeply involved in teaching or local responsibilities:

- Roland Groz is deputy director of Ensimag from 2010 until 2018 and "chargé de mission Culture" for Grenoble INP since 2013.
- Lydie du Bousquet has been in charge of the Informatics School of UFR IM2AG (UGA) since 2011.
- Akram Idani has been in charge of the 1st year of Ensimag since 2013. He shares this responsibility with Catherine Oriat since 2015.

It must be noted that two current members of the team will retire within the next five years. The VASCO team is active to be a target team for the next recruitments of PR and MCF in the next years.

It must also be noted that the team benefits from the part-time support of a CNRS research engineer (German Vega). This engineer is member of the PIMLIG team which provides this support on the basis of well-defined projects for which a demand must be renewed on a annual basis.

Regarding non permanent members, most of them have been involved in research projects of the team and financed by these projects.

2.2 Team organization and scientific animation

The members of the VASCO teams have their offices grouped on the second floor of the IMAG building. This leaves plenty of opportunities to interact. Moreover, most financed research projects involve several members of the team, which gives opportunities for scientific interactions. Also, permanent members have often the opportunity to have lunch together, which favours discussions of hot scientific and administrative topics. Moreover, the team benefits from the scientific animation of the GLSI axis.

Plenary meetings of the permanent members are organized whenever necessary.

2.3 Financial resources

Project	Start date	End date
Europe		
FP7 SPACIOS	01/10/2010	30/01/2014
National		
CNRS Safe PICS	01/01/2015	31/12/2017
ANR MODMED	01/10/2015	31/03/2019
ANR SACADE	01/10/2016	30/04/2019
ANR PHILAE	01/10/2018	31/03/2022
CNRS InS3PECT PEPS	01/01/2017	31/12/2017
PIA ARAMIS	01/20/2014	30/09/2017
(IRT) NeXTRegio	01/11/2016	20/05/2019
Regional		
ARC6 Network	01/01/2014	31/12/2018
Kouno-Tori	01/01/2018	31/12/2019
Local		
UGA DIAMS	16/05/2014	31/12/2015
UGA DELISS	01/01/2015	31/12/2016
UGA TracHal	01/01/2018	31/12/2019
UGA Cyber@Alps	11/2018	2022
LIG VPSIS	01/02/2017	31/12/2017
LIG Arrosoir	01/01/2018	31/12/2018
LIG Icasate	01/01/2018	31/12/2018
LIG MOVASEC	01/01/2019	31/12/2019
LIG Equitri	01/01/2019	31/12/2019

The VASCO team has been involved in several national projects (ANR MODMED, ANR SACADE, ANR PHILAE) which provided him with significant financial resources to support salaries of non-permanent members, travel expenses of the members of the team, and renewal of machines. We have also benefited from some remaining funds from the european SPACIOS project which supported additional salaries to further develop and maintain the products of this project.

The VASCO team also participated in network projects (ARC6, CNRS InS3PECT PEPS, IDEX Cyber@Alps) where the budget is managed by one partner but redistributed in the network.

Also, the team has benefited from local funding, both through the AGIR and IDEX programmes of the Grenoble Universities (DELISS, DIAMS and TracHal projects), and through the Emergence projects managed by the LIG laboratory (MOVASEC, VPSIS, Arrosoir, Icasate and Equitri projects). Many of these projects are shared with other teams of the LIG laboratory.

Finally, the team participates to the Cyber@Alps IDEX project, dedicated to Security. This project gives us opportunities to meet partners for future projects.

2.4 Ethics

Parity; scientific integrity; health and safety; sustainable development and taking into account environmental impacts; intellectual property and economic intelligence

There are currently 33% of women in the permanent members of the team. Regarding non-permanent members, only two women joined our team during these years. Although we welcomed a significant number of female interns in the past years, many of them decided to go for an industrial career and did not pursue a PhD with our team.

The researches of VASCO focus on modeling, verification and validation. We present our results in five sections:

1. Model inference
2. Model integration
3. Trace analysis and test generation
4. Security validation
5. Transparency of algorithms

Roughly speaking, the first two sections refer to modeling, i.e. the construction of models for validation. The last three sections refer to verification and validation.

3.1 Model Inference

In order to get benefits of automated tasks provided by model based software engineering (such as model-checking, model-based testing, code generation etc.) it is necessary to have models of a software artefact. Traditional Model Driven Engineering assumes that development follows a top-down approach, from specifications formally defined by models. However, in many contexts models are not available or not uptodate. This is why there has been a growing interest in model inference techniques, that can reverse engineer models from software, in particular by observing the external behaviour in black box mode.

Active model inference. In connection with testing, the Vasco team has mostly investigated active inference techniques, where sequences of inputs are chosen and submitted to a system to elicit outputs, and thus refine a model until it is complete and faithfully captures the behaviour of the system [37, 12, 29]. We have also worked on an approach that combines active and passive inference, called the Z-quotient algorithm [26]. This approach computes quotient automata of a system's behavioural automaton (w.r.t. to some undistiguishability of states due to lack of evidence on a limited set of observations) that are progressively refined by getting more evidence e.g. from counterexamples provided by analyzing the system or testing it.

Inference without reset. Existing model inference algorithms assume that the system can be reset before each sequence of inputs. But this is known to be difficult (e.g. when the system is remotely tested) or costly in many contexts. Our main focus in the past 5 years has been to find algorithms that could infer a complete model of a system without resetting it. In collaboration with A. Petrenko from CRIM and A. Simao from U. Sao Paolo, we first designed an algorithm that assumes that a bound is known on the number of states of the system, as well as a characterization set, viz. a set of input sequences such that states can be differenciated by their output responses to them [33]. This was later refined for the case where the exact number of states is known [28] or when the characterization set can be organized into a tree [31]. However, it still relied on a strong assumption that some characterization is known for a black box system.

In collaboration with CRIM, we also designed a new algorithm based on constraint solving that is able to infer a minimal model of a system without resetting it, and without any assumption except for a bound on the number of states [25]. This works quite nicely, but does not scale to systems that would have more than a dozen of states, because it has a polynomial complexity with a high degree for the polynom (more than 6).

We have now found a promising approach, which we call hW-inference that scales up with an almost linear complexity [32, 30]. It combines heuristic and algorithmic features. Even for systems that can be reset at some cost, as long as they are strongly connected, hW-inference will

retrieve a model in less time and resources than classical algorithms, thus making the use of resets an unnecessary luxury.

Permanent members involved in this theme	:	R. Groz, C. Oriat
PhD students involved in this theme	:	K. Hossen
Relevant projects	:	FP7 Spacios, ANR Philae
Tools developed	:	Simpa

3.2 Model Integration

Model Integration allows to take benefits of complementary paradigms during the modeling stages of a software developement process. The Vasco team has a long experience in merging formal models (especially B and Z) with graphical modeling notations like UML. The main objectives of this topic are (1) to circumvent the ambiguities of UML notations thanks to the precision of formal languages, (2) to complement the graphical notations with formal annotations which complete the description, and (3) to prevent the lack of end-user involvement when using a formal notation by providing graphical models. For this purpose the team has continued the development of the B4MSecure platform [3, 1, 43] and technical efforts have been devoted for its structuring and its distribution under the LGPL licence. B4MSecure was a central tool in our researches about model integration for the last five years; it allowed to work on the application of UML and B integration with several perspectives: application to security in order to prevent attacks, application to business processes verification and validation, and application to DSLs (Domain Specific Languages) correctness and animation.

Model integration for security. B4MSecure allows to model functional requirements using UML class diagrams, and associated access control rules using the SecureUML profile. These models provide a readable graphical representation of the static aspects of the information system. Then, B4MSecure automatically extracts B specifications which provide a formal description of the dynamic aspects of the system. This approach makes possible the use of formal analysis techniques such as model-checking, animation, constraint solving and proof techniques in order to validate both functional and security models and also to look for insider attack scenarios. For this purpose, the thesis of Amira Radhouani [5] proposed a reachability proof based approach that identifies symbolic execution paths involving functional operations and authorization rules. Then these symbolic paths are translated into a process algebra that guides the ProB model-checker in order to identify the involved users and their roles in the attack scenarios. This approach is fully automated in the GenISIS tool [6, 7] and experiments were done on several case studies. B4MSecure also attracted a collaboration, in the railway domain, with IFSTTAR and IRT Railenium. B4MSecure was applied to the NExtRegio project. The platform contributed to model security policies of ERTMS/ETCS Railway Operating Rules [42]. The formal reasonings were done by model-checking on the B specifications produced by B4MSecure in order to exhibit unsafe scenarios where accidents may happen.

Model integration for business processes. Addressing V&V activities of business processes remains a challenging topic in information systems because existing paradigms informally address the relationships between process representation and data, and hence they don't offer efficient techniques for the corresponding V&V activities. Indeed, several errors in information systems come from inconsistencies between the encoded data and the processes that use these data. The thesis of Salim Chehida[1] [34, 35, 36] extended the B4MSecure tool in order to formally define the relationships between data (UML class diagrams), processes (UML activity diagrams) and access control rules (SecureUML). This work proposed a UML profile called BAAC@UML (Business

[1] S. Chehida defended his thesis at the University of Oran (Algeria) in March 2017. During his thesis, he spent 18 months in the VASCO team under the scientific direction of A. Idani and Y. Ledru.

Activity Access Control with UML) which integrates security concepts within business processes taking into account the static specification of the RBAC policy expressed in SecureUML and its relation with the functional UML model. B specifications can then be produced from the various models which allows to apply animation and model-checking in order to look for inconsistencies between the static models and the business processes.

Model integration for DSLs. One of the major contributions of the MDE (Model Driven Engineering) paradigm is its ability to define domain specific languages (called DSLs) thanks to frameworks dedicated to meta-modeling and code generation like EMF (Eclipse Modeling Framework). However, its major limitation is the lack of formal reasoning tools allowing to ensure the correctness of the DSL semantics. During the last years we applied our expertise in model integration, in order to bridge the gap between MDE and the rigorous world of formal methods. We developed the Meeduse tool which integrates B4MSecure and provides the possibility for MDE-based tools to define DSLs with formal semantics. Our approach translates the Ecore meta-model of a given DSL into an equivalent formal B specification using B4MSecure. The underlying dynamic semantics of the DSL can then be formally defined using B. In our approach, the AtelierB prover is used to guarantee the correctness of the DSL's behavior with respect to its invariant properties, and the ProB model-checker is used to animate execution scenarios which are translated back to the initial EMF model. Besides the use of automatic reasoning tools in MDE, proved B refinements are also investigated in order to gradually translate abstract EMF models to concrete models which can then be automatically compiled into a programming language. Meeduse successfully contributed to the NextRegio project where it was applied to define a formal railway DSL [2].

Permanent members involved in this theme	:	A. Idani, Y. Ledru
PhD students involved in this theme	:	A. Radhouani, S. Chehida (visitor)
Relevant projects	:	NeXTRegio, DELISS, VPSIS, MOVASEC
Tools developed	:	B4MSecure, Genisis, Meeduse

3.3 Trace Analysis and Test Generation

In software engineering, tracing involves a specialized use of logging to record information about the execution of a program or a system. This information is typically used for testing or debugging purposes, but also to identify the usage of a product. During the last few years, Vasco team was involved in several projects where the traces were a key artefact: ANR MODMED and ANR Philae. Our interest in traces originates from the FUI IO-32 Project (2010-2013). Its primary goal was to create easy-to-use software that facilitates the development of 32-bit microcontrollers. Beyond the intuitive graphical user interface developed by the industrial partner, VASCO team proposed approaches and tools to ease the execution trace analysis, including compression mechanisms and fault-localization [4].

Traces for passive testing. The expertise gained from *IO-32* project in trace analysis allowed us to consider traces as a key artefact for passive testing. Indeed, a trace is an abstraction of the system execution. With an appropriate formalism and an associated tool, it is possible to check that the observed behaviour satisfies a set of properties. During the ANR *ModMed* project, VASCO team developed such a formalism: a Domain Specific Language (DSL) called ParTraP that allows to specify properties on finite traces composed of *parametric events*.

The ParTraP language, defined in Y. Blein's thesis [39], is a unique combination of features that extends the specification patterns originally proposed by Dwyer et al. with parametrized constructs, nested scopes, real-time and first-order quantification [41]. In addition, an Integrated Development Environment for ParTraP has been developed [8]. A coverage measurement technique for ParTraP was also proposed to help user to get a deeper understanding of temporal properties [9].

Originally created for medical devices validation [38, 40, 44, 39], ParTraP is currently experimented within other application domains, and especially smart homes: collaborations with Kobe University through *Kouno-tori* project or and with Adele and Ctrl-A teams through internal LIG *iCasate* project [11]. Usability and ability to express relevant properties are explored, as it was done for assertions in the *Safe* CNRS PICS project [24, 21, 23].

Using traces for non-regression testing. Traces collected after the system deployment carry meaningful feedbacks on the real usage of the software. This knowledge can be exploited to enlarge the existing test set, for instance for non-regression testing. That is the purpose of the ANR *Philae* project (2018-2021).

With a similar idea, the *TracHal* idex-UGA project focuses on the validation of end-user programs for smart home. In such a context, it is not possible to produce tests automatically because there is neither a specification that describes the end-user program expectations nor the environment behaviour description (specific to each smart home). The objective of the project is to use execution traces to build a simulator of the environment that helps the users to animate their programs in their own context [10].

Permanent members involved in this theme	:	L. du Bousquet, R. Groz, Y. Ledru, C. Oriat
PhD students involved in this theme	:	Y. Blein
Relevant projects	:	ANR MODMED, Safe PICS, TracHal, Icasate, Kouno-Tori
Tools developed	:	ParTraP-IDE

3.4 Security Validation

During the last 5 years, we have investigated the use of model-based approaches for analyzing and validating the security of systems.

Model inference for security validation In the european FP7 SPaCIoS project, we have contributed to a method and a toolset to analyze the security of web-based applications and security protocols through the use of model checking and model-based testing to confirm potential vulnerabilities raised by model checkers for security [12]. In order to retrieve models in the state-machine based security language ASLAN++, during the thesis of K. Hossen [19], we developed inference techniques that were able to deal with seemingly non-deterministic values such as nonces and cookies [20]. The implementation of the inference algorithms resulted in the SIMPA tool (SIMPA Infers Models Pretty Automatically), that was later extended to implement other inference algorithms (see section 3.1).

Fuzzing To address a large set of data from models, we investigated smart fuzzing techniques. To detect XSS (Cross Site Scripting) vulnerabilites, that were the main issue in web-based applicaitons at the time, we combined control-flow inference with taint flow analysis and evolutionary fuzzing [14]. This was implemented in the KameleonFuzz tool during the thesis of F. Duchene [13].

Reverse engineering from binary code The thesis of Franck de Goër [17] was devoted to techniques for retrieving function prototypes (viz. signatures) from binary code, and relating them to identify potential weaknesses in the control flow at the level of the call graph. The approach is mostly based on heuristics, and was designed to be fast: it only requires a single execution of a program, that has been instrumented with lightweight measures [15]. It has been used to detect custom memory allocators in binary code [16]. This led to the development of the `scat` tool. A later development of similar ideas was targeted at retrieving function calls that are done through direct jumps [18].

Security of industrial systems Through the PIA ARAMIS project, and then the ASTRID SACADE project, we have been investigating the use of model-based techniques to analyze the security of SCADA systems. In particular, we consider model-checking and model-based testing to identify and qualify vulnerabilities that appear in systems run with SCADA protocols, with a particular focus on Modbus and OPC/UA protocols. However, it appears that in most cases, vulnerabilities are rather easy to spot and mostly related to the architecture, and do not require the use of formal models to be identified.

Permanent members involved in this theme	:	R. Groz, C. Oriat, J.-L. Richier
PhD students involved in this theme	:	K. Hossen, F. De Goër, F. Duchene, A. Rey, Nguyen Manh Dung
Relevant projects	:	ANR ARAMIS, ANR SACADE, FP7 Spacios
Tools developed	:	KameleonFuzz, scat

3.5 Transparency of algorithms

Companies and governments increasingly rely upon algorithms to make decisions that affect people's lives and livelihoods. While the impact in their life become more important, users need to understand the algorithms behaviours. This is called "transparency" of the algorithms. The internal LIG project *Arrosoir* (2018), MRIM and VASCO teams evaluate the transparency of web search engines. We applied an approach that is very close to testing. The description of the search engine behaviour (its policy) is considered as an informal specification. Tests (here web queries in a controlled environment) are then carried out to check whether the specification is satisfied. This appears to be a promising research direction : our first results were published in [22] which received the best paper award at the CORIA'19 conference.

Permanent members involved in this theme	:	L. du Bousquet
Relevant projects	:	LIG Arrosoir, LIG Equitri

3.6 Conclusion

We have reviewed the results of the researches of the VASCO team along five major themes. These themes cover the major research orientations of the team mentioned at the beginning of this report.

The theme "Trace analysis and test generation" is at the heart of our current research and covers the "Models as oracles" orientation. This theme combined with theme "Model inference" corresponds to the direction "Inferring models for test generation". The theme "Model integration" covers the research orientation "Building models for verification".

Our research orientation towards "lightweight formal methods" is common to all our themes. We try to produce tools based on our research results which automate and facilitate the use of our approaches.

The fourth and fifth themes, "Security validation" and "Transparency of algorithms" mainly correspond to case studies where our results can be applied. They are also relevant to the testing and validation activities which are central to the researches of the VASCO team.

Strengths

- The team is regularly involved in national projects.
- At short term: the team takes part in the ANR Philae project, and participates to the ITEA-labelled IVVES proposal. Both projects are in our domains of interest.
- The team has a strong visibility in the national community (involvement in the GDR GPL network).

Weaknesses

- The number of PhD students is small with respect to the number of habilitated professors.
- Two permanent members (J.-L. Richier and R. Groz) will retire in the next five years.
- The number of publications is decreasing with respect to the previous period.

Opportunities

- The MIAI institute gives opportunities to address the challenge of confidence (including correctness and transparency) of artificial intelligence applications.
- The Cyber Alps IDEX project structures the local community dedicated to security, which is a significant application domain for VASCO.

Threats

- Recruitment of new permanent members is difficult, as shown by our recent attempts (2017, 2018, 2019), and we have no guarantee that the retirements of permanent members will be compensated.
- Software Engineering and Formal Methods are not popular topics for our students, decision makers and the general public. This makes it difficult to attract PhD Students and funding.
- The VASCO members are often involved, or solicited for significant responsibilities in our universities, which significantly reduce the amount of time dedicated to research.

Our research perspectives are aligned with the themes of the previous five years. This is due to the fact that several projects are on-going (e.g. ANR Philae) but also that our recent results opened new perspectives.

The "Security Validation" theme is no longer identified as a major theme, but remains present in our model inference activities and in our support of RBAC in model integration. The fourth theme "Validation of applications with AI features" is less developed because it corresponds to a recent activity. But it must be noted that this fourth theme, together with theme 1 "Model inference" show the upcoming use of AI techniques in our research. We expect that these research works will benefit from the creation of the MIAI institute and give opportunities for joint research projects.

5.1 Model inference

Up to now, VASCO has mostly developed methods for active inference of behavioural models of systems. This stemmed from our previous activities in model-based testing (MBT). MBT is meant to test a system by sending inputs and observing its outputs. Therefore, we have considered algorithms that can learn a model of a system by testing it, and elicit a model that is exact, with a controlled level of approximation, because algorithms converge towards exact models. This is a form of machine learning that is deterministic and not based on statistics, well suited for the verification and validation of systems.

We are now moving towards extending our research in two directions:

- incorporating passive learning, e.g. from software logs; actually, the Z-Quotient approach that we developed previously already encompassed the use of existing software traces, so it combined passive and active learning; however, it was mostly aimed at generating tests to refine a model.
- using classical "statistical" ML approaches to extract partial models from software traces, and use them for software validation, test generation, fault analysis etc.

Working from software traces will capitalize on the expertise acquired by VASCO both in inference methods and in trace verification methods. In both cases, we extend classical methods used for finite models (e.g. finite automata) so that they can be used on parametric traces where event structures contain many parameters with large domains (such as values, strings and more general structures).

In particular, the starting ANR project PHILAE will investigate the use of ML techniques combined with inference algorithms to derive models from the information that can be collected during regression testing and from DevOps activities. The goal is to solve the bottleneck faced by software developers with continuous integration: regression testing becomes too large and time consuming, so it is both important to select and prioritize regression tests, and at the same time to enhance tests to cope with the new features that are continuously integrated into the software.

A similar idea will be explored in collaboration with IIHM team. The problem is to propose an approach to help end-users to test their own programs for home. Such programs look like rules that fire depending on the state of the environment. They are hard to test because they require to put the environment in special state, which is usually impossible (e.g. to check if the heater starts correctly, home temperature should be decreased). Our objective is to learn the environment behaviour, i.e. infer a model of the environment, as program behaviour can be learned, in order to propose a realistic simulator for testing.

In parallel, we will continue to improve the current algorithms and our SIMPA tool for inference. In particular, we will extend hW-inference to deal with parametric models and explore approaches to infer models of systems with a minimal or at least reduced number of resets for models that are not strongly connected.

5.2 Model Integration

From models to secure architectures Evolutions of the B4MSecure platform was one of our main researches dedicated to the model integration topic during the last five years. The tool has been the subject of several theses developed outside our team and made it possible to attract interesting collaborations like the NExTRegio project supported by the IRT Railenium. The platform was successful for security modeling and verification at a platform independent level. However, the missing link is the relationship with target secure architectures. This may lead to a significant gap between models and their implementations in a given technology (web, databases, etc). One interesting perspective that we plan for the future is to propose solutions to reconcile modeling and implementation in B4MSecure. This perspective will be built on two research directions:

- define semantic links between B4MSecure models and platform specific models using abstraction and refinement techniques, and
- develop a tool-set for conformance testing where the validation activities done at the modeling level can be replayed on the implementation level.

These perspectives led to the proposal of a research project submitted to the ANR 2019 call for international collaborative projects (PRCI), with the University of Düsseldorf; especially in collaboration with M. Leuschel, leader of the ProB tool for constraint solving and model-checking.

Models@Runtime One emerging research that we addressed during the last year is about executing and debugging models expressed in domain specific languages (DSLs). The challenge of debugging a model is not new and was widely addressed in the literature at several abstraction levels. However, when an executable DSL is not carefully checked by underlying V&V activities, it may lead to a succession of conceptual failures: failures of modeling operations may result in failures of execution operations, which in turn may result in failures of the coordination operations... While building models is well mastered by MDE tools, the definition and the execution of operational semantics using classical approaches suffer from the lack of formal reasonings and then many failures may happen with their DSLs. Meeduse was developed in order to circumvent this shortcoming and then favour the execution and the debugging of DSLs that address safety critical systems. It mixes the formal B method with MDE-based DSLs and was experimented on several case studies (parking-lot controller, automatic car light regulator, lift automatism) which showed its viability to define DSLs with proved executional semantics. In the future we plan to evolve this technique in order to define proved semantics of runtime DSL models which are views on a running software system and which can be used for monitoring, analyzing or adapting a system at runtime. Several new challenges will be approached such as:

- How to allow runtime DSL animation in Meeduse and extract monitors and/or controllers given a DSL animation trace?
- How to deal with multiple DSL collaboration and dynamically resolve their trade-offs or overlaps at runtime using constraint solving techniques?

5.3 Traces

The design of the ParTraP language and its associated toolset was a major activity of the past five years. In next five years, we intend to build on these assets, and widen our research interests to other exploitations of traces.

The design of ParTraP aimed at providing an intuitive and expressive language. Although it was initially targeted to the verification of medical devices, the language is general-purpose and we expect that it can be applied to other application domains. Our goal for the next years is to

experiment with the language on several domains, and improve the language based on lessons learned. Improvements can be of three kinds:

- increase the ease of use of the language by providing new constructs which allow for a more intuitive expression of several properties;
- improve the performances of the generated monitors, and consider an evolution of these monitors to evaluate properties at run-time instead of a posteriori;
- better structure the explanation of evaluation results to make them easier to understand, and allow for the design of tools which will support this explanation.

Our current research projects provide us with a diversity of traces. The ANR Philae project gives us access to traces of regression tests of web applications and endurance tests of Liveboxes. We expect that the ParTraP language can help us retrieve traces satisfying given properties from the large amount of raw data. In this project, we will also experiment with AI classification techniques to cluster traces of regression tests and perform reduction of the regression test suite. Our collaboration with the University of Kobe gives us access to traces of home automation. Here again, we intend to use the ParTraP language to retrieve traces, or portions of traces featuring interesting properties.

Also, one may expect that some properties of test traces are robust to evolutions of systems and can be exploited in regression testing. The evolution of a software or system can lead to evolution of its test traces, but still conform to initial trace properties.

5.4 Validation of applications wih AI features

Nowadays, Artificial Intelligence (AI) is becoming a leading paradigm for the development of software systems. But systems built using AI must also be safe and secure. However, learned features make software system much more difficult to validate, especially because specification becomes tricky, and sometimes impossible, to express. This impacts the validation procedures. To be able to carry out a suitable validation phase, VASCO will look for relevant monitoring strategies.

5.5 Conclusion

In this section, we have presented the main research perspectives of the VASCO team. They are closely aligned with our previous research themes, and will benefit from on-going research projects such as the ANR Philae project. These perspectives define the domains where we intend to be active. But we are open to new collaborations, in particular in the case of recruitment of new team members.

Compatibility with the LIG project

The LIG has identified several objectives regarding Publications, Habilitations, Scientific integrity and Data security. Here is the positioning of the VASCO team with respect to these objectives

Publications The VASCO team will target more conferences and journals ranked at the highest level. Nevertheless, we also intend to participate to more focussed conferences as was done in the last five years with ICGI, RV or RssRail, because these smaller communities lead to fruitful interactions.

Habilitations Due to the size of the team (6 permanents) and the current number of Habilitated permanents (3) we foresee 1 HDR defense in the coming years.

Scientific integrity We will encourage the members of the team to participate to the tutorials organized by the LIG.

Data security Currently, Vasco is not storing personal data. We only store data of some of our partners in projects. In the Philae Project, we got a huge amount of technical confidential data. Adequate measures were taken, in order to store these on a machine which is only accessible inside the laboratory, by identified members of the project. Our previous projects in security and access control have led us to be aware that data security matters.

[1] Akram Idani and Yves Ledru. B for Modeling Secure Information Systems - The B4MSecure Platform (démo). In *Formal Methods and Software Engineering - 17th International Conference on Formal Engineering Methods (ICFEM 2015)*, volume 9407 of *Formal Methods and Software Engineering - 17th International Conference on Formal Engineering Methods (ICFEM 2015)*, pages 312–328, Paris, France, 2015. Springer.

[2] Akram Idani, Yves Ledru, Abderrahim Ait Wakrime, Rahma Ben Ayed, and Philippe Bon. Towards a tool-based domain specific approach for railway systems modeling and validation. In *International Conference on Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification - RssRail 2019*, Lille, France, June 2019. Springer.

[3] Akram Idani, Yves Ledru, and Amira Radhouani. Modélisation graphique et validation formelle de politiques RBAC en systèmes d'information. Plateforme B4MSecure. *Revue des Sciences et Technologies de l'Information - Série ISI : Ingénierie des Systèmes d'Information*, 19(6):33–61, 2014.

[4] Azzeddine Amiar. *Aide à l'Analyse de Traces d'Exécution dans le Contexte des Microcontrôleurs*. Thesis, Université de Grenoble, November 2013.

[5] Amira Radhouani. *Formal methods for extracting insider attacks from Information Systems*. Thesis, Université Grenoble Alpes, June 2017.

[6] Amira Radhouani, Akram Idani, Yves Ledru, and Narjes Ben Rajeb. Extraction of Insider Attack Scenarios from a Formal Information System Modeling. In Véronique Cortier and Riadh Robbana, editors, *Formal Methods for Security*, volume 1158, pages 5–19, Tunis, Tunisia, June 2014. CEUR-Wrokshops.

[7] Amira Radhouani, Akram Idani, Yves Ledru, and Narjes Ben Rajeb. Symbolic Search of Insider Attack Scenarios from a Formal Information System Modeling. *LNCS Transactions on Petri Nets and Other Models of Concurrency*, 10:131–152, 2015.

[8] Ansem Ben Cheikh, Yoann Blein, Salim Chehida, German Vega, Yves Ledru, and Lydie Du Bousquet. An Environment for the ParTraP Trace Property Language (Tool Demonstration). In *Runtime Verification - 18th International Conference, RV 2018*, pages 437–446, Limassol, Cyprus, November 2018.

[9] Yoann Blein, Mohammad Ali Tabikh, and Yves Ledru. Wp4/d1: Test assessment - preliminary study and tool prototype, March 2018.

[10] Baptiste Bleuze. Exploitation de traces pour produire des tests, rapport de stage, June 2018.

[11] Mathieu Bochaton. Testing pervasive service resilience in icasate, June 2018.

[12] Matthias Büchler, Karim Hossen, Petru Florin Mihancea, Marius Minea, Roland Groz, and Catherine Oriat. Model Inference and Security Testing in the SPaCIoS Project. In *IEEE Working Conference on Reverse Engineering, CSMR-WCRE 2014*, pages 411–414, Antwerp, Belgium, 2014.

[13] Fabien Duchene. *Detection of web vulnerabilities via model inference assisted evolutionary fuzzing*. Thesis, Université de Grenoble, June 2014.

[14] Fabien Duchene, Sanjay Rawat, Jean-Luc Richier, and Roland Groz. KameleonFuzz: Evolutionary Fuzzing for Black-Box XSS Detection. In *Fourth ACM Conference on Data and Application Security and Privacy (CODASPY 2014)*, pages 37–48, Unknown, 2014. ACM.

[15] Franck de Goër, Roland Groz, and Laurent Mounier. Lightweight heuristics to retrieve parameter associations from binaries. In *Proceedings of the 5th Program Protection and Reverse Engineering Workshop, PPREW@ACSAC*, Los Angeles, CA, United States, December 2015.

[16] Franck de Goër, Roland Groz, and Laurent Mounier. Metrics for runtime detection of allocators in binaries. In *10th USENIX Workshop on Cyber Security Experimentation and Test, CSET 2017*, Vancouver, BC, Canada, August 2017.

[17] Franck de Goër de Herve. *Reverse-engineering of binaries in a single execution : a lightweight function-grained dynamic analysis*. Thesis, Université Grenoble Alpes, October 2017.

[18] Franck de Goër de Herve, Sanjay Rawat, Dennis Andriesse, Herbert Bos, and Roland Groz. Now You See Me: Real-time Dynamic Function Call Detection. In *ACSAC 2018: Annual Computer Security Applications Conference*, San Juan, Puerto Rico, December 2018.

[19] Karim Hossen. *Automatic model inference of Web applications and protocols for vulnerability detection*. Thesis, Université de Grenoble, December 2014.

[20] Karim Hossen, Catherine Oriat, Roland Groz, and Jean-Luc Richier. Automatic Model Inference of Web Applications for Security Testing. In *Position Statement at SecTest2014, co-located with ICST2014*, Cleveland, Ohio, United States, 2014.

[21] Lydie du Bousquet and Masahide Nakamura. Improving Testability of Software Systems that Include a Learning Feature. In *The Tenth International Conference on Advances in System Testing and Validation (VALID)*, Nice, France, October 2018.

[22] Philippe Mulhem, Lydie Du Bousquet, and Sara Lakah. Quelques pas vers l'Honnêteté et l'Explicabilité de moteurs de recherche sur le Web. In *COnférence en Recherche d'Information et Applications*, Villeurbanne, France, March 2019.

[23] Masahide Nakamura and Lydie du Bousquet. Constructing Execution and Life-Cycle Models for Smart City Services with Self-Aware IoT. In *2015 IEEE International Conference on Autonomic Computing (ICAC) and Workshop*, Grenoble, France, July 2015.

[24] Long Niu, Sachio Saiki, Lydie Du Bousquet, and Masahide Nakamura. Recognizing ADLs Based on Non-Intrusive Environmental Sensing and BLE Beacons. In *Eighth International Conference on Indoor Positionning and Indoor Navigation (IPIN2017)*, Sapporo, Japan, September 2017.

[25] Alexandre Petrenko, Florent Avellaneda, Roland Groz, and Catherine Oriat. From Passive to Active FSM Inference via Checking Sequence Construction. In Nina Yevtushenko, Ana Rosa Cavalli, and Hüsnü Yenigü, editors, *29th IFIP International Conference on Testing Software and Systems (ICTSS)*, volume LNCS-10533 of *Testing Software and Systems*, pages 126–141, St. Petersburg, Russia, October 2017. Springer International Publishing. Part 2: Test Derivation Methods.

[26] Alexandre Petrenko, Keqin Li, Roland Groz, Karim Hossen, and Catherine Oriat. Inferring Approximated Models for Systems Engineering. In *15th IEEE International Symposium on High Assurance Systems Engineering (HASE 2014)*, pages 249–253, Miami, Florida, United States, 2014.

[27] R. L. Rivest and R. E. Schapire. Inference of finite automata using homing sequences. In *Machine Learning: From Theory to Applications*, pages 51–73, 1993.

[28] Roland Groz, Catherine Oriat, and Nicolas Bremond. Inferring Non-resettable Mealy Machines with n States. In *International Conference on Grammatical Inference 2016 (ICGI'16)*, Delft, Netherlands, October 2016.

[29] Roland Groz, Keqin Li, and Alexandre Petrenko. Integration testing of communicating systems with unknown components. *Annales des Télécommunications*, 70(3-4):107–125, 2015.

[30] Roland Groz, Nicolas Bremond, and Adenilso Simao. Using Adaptive Sequences for Learning Non-Resettable FSMs. In *ICGI: International Conference on Grammatical Inference*, Wroclaw, Poland, September 2018.

[31] Roland Groz, Adenilso Simao, and Catherine Oriat. Adaptive Localizer Based on Splitting Trees. In Nina Yevtushenko, Ana Rosa Cavalli, and Hüsnü Yenigü, editors, *29th IFIP International Conference on Testing Software and Systems (ICTSS)*, volume LNCS-10533 of *Testing Software and Systems*, pages 326–332, St. Petersburg, Russia, October 2017. Springer International Publishing. Part 6: Short Contributions.

[32] Roland Groz, Adenilso Simao, Nicolas Bremond, and Catherine Oriat. Revisiting AI and testing methods to infer FSM models of black-box systems. In *Proceedings of the 13th International Workshop on Automation of Software Test, AST@ICSE 2018, Gothenburg, Sweden, May 28-29, 2018*, pages 16–19. ACM Press, May 2018.

[33] Roland Groz, Adenilso Simao, Alexandre Petrenko, and Catherine Oriat. Inferring Finite State Machines Without Reset Using State Identification Sequences. In Khaled El-Fakih, Gerassimos Barlas, and Nina Yevtushenko, editors, *27th IFIP International Conference on Testing Software and Systems (ICTSS)*, volume LNCS-9447 of *Testing Software and Systems*, pages 161–177, Sharjah and Dubai, United Arab Emirates, November 2015. Part 4: Model and System Testing.

[34] Salim Chehida, Akram Idani, Yves Ledru, and Mustapha Kamel Rahmouni. Extensions du diagramme d'activité pour contrôler l'accès au SI. In *INFORSID 2015*, pages 151–165, Biarritz, France, 2015.

[35] Salim Chehida, Akram Idani, Yves Ledru, and Mustapha Kamel Rahmouni. Combining UML and B for the specification and validation of RBAC policies in business process activities. In *Tenth IEEE International Conference on Research Challenges in Information Science, RCIS 2016*, Grenoble, France, June 2016.

[36] Salim Chehida, Akram Idani, Yves Ledru, and Mustapha Kamel Rahmouni. Extensions du diagramme d'activité pour la spécification de politiques RBAC. *Revue des Sciences et Technologies de l'Information - Série ISI : Ingénierie des Systèmes d'Information*, 21(2):11–37, 2016.

[37] Muzammil Shahbaz and Roland Groz. Analysis and testing of black-box component based systems by inferring partial models. *Software Testing, Verification and Reliability*, 24(4), 2014.

[38] Yoann Blein. Identification de propriétés pour la validation d'un système cyber-physique médical. In *Approches Formelles dans l'Assistance au Développement de Logiciels (AFADL'16)*, Besançon, France, June 2016.

[39] Yoann Blein. *ParTraP: a language for the specification and runtime verification of parametric properties (to appear)*. Thesis, Université Grenoble Alpes, April 2019.

[40] Yoann Blein, Arnaud Clere, Fabrice Bertrand, Yves Ledru, Roland Groz, and Lydie Du Bousquet. Improving Trace Generation and Analysis for Medical Devices. In *IEEE International Conference on Software Quality, Reliability and Security Companion, QRS-C 2017*, pages 599–600, Prague, Czech Republic, July 2017.

[41] Yoann Blein, Yves Ledru, Lydie du-Bousquet, and Roland Groz. Extending specification patterns for verification of parametric traces. In *the 6th Conference on Formal Methods in Software Engineering (FormaliSE'18)*, pages 10–19, Gothenburg, Sweden, June 2018. ACM Press.

[42] Yves Ledru, Akram Idani, Rahma Ben Ayed, Abderrahim Ait Wakrime, and Philippe Bon. A separation of concerns approach for the verified modelling of railway signalling rules. In *International Conference on Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification - RssRail 2019*, Lille, France, June 2019.

[43] Yves Ledru, Akram Idani, Jérémy Milhau, Muhammad Nafees Qamar, Régine Laleau, Jean-Luc Richier, and Mohamed-Amine Labiadh. Validation of IS Security Policies featuring Authorisation Constraints. *International Journal of Information System Modeling and Design*, 6(1):24–46, 2015.

[44] Yves Ledru, Yoann Blein, Lydie Du Bousquet, Roland Groz, Arnaud Clere, and Fabrice Bertrand. Requirements for a Trace Property Language for Medical Devices. In *the International Workshop on Software Engineering in Healthcare Systems, SEHS@ICSE 2018*, Gothenburg, Sweden, May 2018. ACM Press.

EVALUATION CAMPAIGN 2019-2020
VAGUE A

Name of the team : VASCO
Acronym : VASCO

Head of the team for the current contract : Yves LEDRU
Head of the team for the next contract : Yves LEDRU

1.1 Production of knowledge and activities contributing to the influence and scientific attractiveness of the unit

1.1.1 Journal Articles

Scientific articles in English

Top 20%

[J1] Mickaël Delahaye and Lydie Du Bousquet. Selecting a software engineering tool: lessons learnt from mutation analysis. *Software: Practice and Experience*, 45(7):875–891, July 2015.

[J2] Alexandre Petrenko, Florent Avellaneda, Roland Groz, and Catherine Oriat. FSM inference and checking sequence construction are two sides of the same coin. *Software Quality Journal*, 2018.

[J3] Muzammil Shahbaz and Roland Groz. Analysis and testing of black-box component based systems by inferring partial models. *Software Testing, Verification and Reliability*, 24(4), 2014.

[J4] Amira Radhouani, Akram Idani, Yves Ledru, and Narjes Ben Rajeb. Symbolic Search of Insider Attack Scenarios from a Formal Information System Modeling. *LNCS Transactions on Petri Nets and Other Models of Concurrency*, 10:131–152, 2015.

[J5] Roland Groz, Keqin Li, and Alexandre Petrenko. Integration testing of communicating systems with unknown components. *Annales des Télécommunications*, 70(3-4):107–125, 2015.

[J6] Yves Ledru, Akram Idani, Jérémy Milhau, Muhammad Nafees Qamar, Régine Laleau, Jean-Luc Richier, and Mohamed-Amine Labiadh. Validation of IS Security Policies featuring Authorisation Constraints. *International Journal of Information System Modeling and Design*, 6(1):24–46, 2015.

Review articles

Top 20%

Other articles (professional journals, etc.)

Top 20%

[OA1] Akram Idani, Yves Ledru, and Amira Radhouani. Modélisation graphique et validation formelle de politiques RBAC en systèmes d'information. Plateforme B4MSecure. *Revue des Sciences et Technologies de l'Information - Série ISI : Ingénierie des Systèmes d'Information*, 19(6):33–61, 2014.

[OA2] Rahma Ben-Ayed, Simon Collart-Dutilleul, Philippe Bon, Yves Ledru, and Akram Idani. Formalismes basés sur les rôles pour la modélisation et la validation des règles d'exploitation ferroviaires. *Technique et Science Informatiques*, 34(5):p495–521, January 2015.

[OA3] Philippe Collet, Lydie Du Bousquet, Laurence Duchien, and Pierre-Etienne Moreau. Défis 2025. *Techniques et sciences informatique (TSI)*, 34(3):311–324, 2015.

[OA4] Salim Chehida, Akram Idani, Yves Ledru, and Mustapha Kamel Rahmouni. Extensions du diagramme d'activité pour la spécification de politiques RBAC. *Revue des Sciences et Technologies de l'Information - Série ISI : Ingénierie des Systèmes d'Information*, 21(2):11–37, 2016.

1.1.2 Books

Monographs, critical editions, translations (total numbers)

Management and coordination of scientific books / Scientific book edition Management and coordination of scientific books / Scientific book edition in English or another foreign language

Top 20%

[B1] Nicolas Halbwachs, Laurent Mounier, and Jean-Luc Richier, editors. *Actes des Dixièmes journées nationales du GDR Génie de la Programmation et du Logiciel*, Grenoble, France, June 2018. LIG - Université Grenoble Alpes.

Book chapters in English or another foreign language

Top 20%

[Ch1] Roland Groz, Adenilso Simao, Alexandre Petrenko, and Catherine Oriat. Inferring FSM Models of Systems Without Reset. In *Machine Learning for Dynamic Software Analysis*, pages 178–201. July 2018.

Edited theses

Top 20%

[PhD1] Amira Radhouani. *Formal methods for extracting insider attacks from Information Systems*. Thesis, Université Grenoble Alpes, June 2017.

[PhD2] Fabien Duchene. *Detection of web vulnerabilities via model inference assisted evolutionary fuzzing*. Thesis, Université de Grenoble, June 2014.

[PhD3] Franck de Goër de Herve. *Reverse-engineering of binaries in a single execution : a lightweight function-grained dynamic analysis*. Thesis, Université Grenoble Alpes, October 2017.

[PhD4] Karim Hossen. *Automatic model inference of Web applications and protocols for vulnerability detection*. Thesis, Université de Grenoble, December 2014.

[PhD5] Yoann Blein. *ParTraP: a language for the specification and runtime verification of parametric properties (to appear)*. Thesis, Université Grenoble Alpes, April 2019.

1.1.3 Production in conferences / congresses and research seminars

Meeting abstracts

Top 20%

Articles published in conference proceedings / congress

Top 20%

[C1] Matthias Büchler, Karim Hossen, Petru Florin Mihancea, Marius Minea, Roland Groz, and Catherine Oriat. Model Inference and Security Testing in the SPaCIoS Project. In *IEEE Working Conference on Reverse Engineering, CSMR-WCRE 2014*, pages 411–414, Antwerp, Belgium, 2014.

[C2] Alexandre Petrenko, Keqin Li, Roland Groz, Karim Hossen, and Catherine Oriat.

Inferring Approximated Models for Systems Engineering. In *15th IEEE International Symposium on High Assurance Systems Engineering (HASE 2014)*, pages 249–253, Miami, Florida, United States, 2014.

[C3] Akram Idani. Model driven secure web applications. In *ECBS*, Larnaca, Cyprus, August 2017.

[C4] Akram Idani and Yves Ledru. B for Modeling Secure Information Systems - The B4MSecure Platform (démo). In *Formal Methods and Software Engineering - 17th International Conference on Formal Engineering Methods (ICFEM 2015)*, volume 9407 of *Formal Methods and Software Engineering - 17th International Conference on Formal Engineering Methods (ICFEM 2015)*, pages 312–328, Paris, France, 2015. Springer.

[C5] Fabien Duchene, Sanjay Rawat, Jean-Luc Richier, and Roland Groz. KameleonFuzz: Evolutionary Fuzzing for Black-Box XSS Detection. In *Fourth ACM Conference on Data and Application Security and Privacy (CODASPY 2014)*, pages 37–48, Unknown, 2014. ACM.

[C6] Franck de Goër de Herve, Sanjay Rawat, Dennis Andriesse, Herbert Bos, and Roland Groz. Now You See Me: Real-time Dynamic Function Call Detection. In *ACSAC 2018: Annual Computer Security Applications Conference*, San Juan, Puerto Rico, December 2018.

[C7] Salim Chehida, Akram Idani, Yves Ledru, and Mustapha Kamel Rahmouni. Combining UML and B for the specification and validation of RBAC policies in business process activities. In *Tenth IEEE International Conference on Research Challenges in Information Science, RCIS 2016*, Grenoble, France, June 2016.

[C8] Yliès Falcone, Tom Cornebize, and Jean-Claude Fernandez. Efficient and Generalized Decentralized Monitoring of Regular Languages. In Erika Ábrahám and Catuscia Palamidessi, editors, *34th Formal Techniques for Networked and Distributed Systems (FORTE)*, volume LNCS-8461 of *Formal Techniques for Distributed Objects, Components, and Systems*, pages 66–83, Berlin, Germany, June 2014. Springer. Part 2: Monitoring and Testing.

[C9] Abderrahim Ait Wakrime, Rahma Ben Ayed, Simon Collart-Dutilleul, Yves Ledru, and Akram Idani. Formalizing Railway Signaling System ERTMS/ETCS Using UML/Event-B. In *Model and Data Engineering - 8th International Conference, (MEDI)*, pages 321–330, Marrakesh, Morocco, October 2018.

[C10] Benoit Badrignans, Vincent Danjean, Jean-Guillaume Dumas, Philippe Elbaz-Vincent, Sabine Machenaud, Jean-Baptiste Orfila, Florian Pebay-Peyroula, François Pebay-Peyroula, Marie-Laure Potet, Maxime Puys, Jean-Luc Richier, and Jean-Louis Roch. Security Architecture for Point-to-Point Splitting Protocols. In *WCICSS 2017 - IEEE World Congress on Industrial Control Systems Security*, Cambridge, United Kingdom, December 2017.

[C11] Rahma Ben Ayed, Simon Collart-Dutilleul, Philippe Bon, Akram Idani, and Yves Ledru. B Formal Validation of ERTMS/ETCS Railway Operating Rules. In *4th International ABZ Conference*, pages p124–129, France, June 2014.

[C12] Rahma Ben Ayed, Simon Collart-Dutilleul, Philippe Bon, Yves Ledru, and Akram Idani. Modélisation et validation formelle des règles d'exploitation ferroviaires.

In *Approches Formelles dans l'Assistance au Développement de Logiciels*, page 15p, France, June 2014.

[C13] Philippe Mulhem, Lydie Du Bousquet, and Sara Lakah. Quelques pas vers l'Honnêteté et l'Explicabilité de moteurs de recherche sur le Web. In *COnférence en Recherche d'Information et Applications*, Villeurbanne, France, March 2019.

[C14] Masahide Nakamura and Lydie du Bousquet. Constructing Execution and Life-Cycle Models for Smart City Services with Self-Aware IoT. In *2015 IEEE International Conference on Autonomic Computing (ICAC) and Workshop*, Grenoble, France, July 2015.

[C15] Long Niu, Sachio Saiki, Lydie Du Bousquet, and Masahide Nakamura. Recognizing ADLs Based on Non-Intrusive Environmental Sensing and BLE Beacons. In *Eighth International Conference on Indoor Positionning and Indoor Navigation (IPIN2017)*, Sapporo, Japan, September 2017.

[C16] Alexandre Petrenko, Florent Avellaneda, Roland Groz, and Catherine Oriat. From Passive to Active FSM Inference via Checking Sequence Construction. In Nina Yevtushenko, Ana Rosa Cavalli, and Hüsnü Yenigü, editors, *29th IFIP International Conference on Testing Software and Systems (ICTSS)*, volume LNCS-10533 of *Testing Software and Systems*, pages 126–141, St. Petersburg, Russia, October 2017. Springer International Publishing. Part 2: Test Derivation Methods.

[C17] Srinivas Pinisetty, Yliès Falcone, Thierry Jéron, and Hervé Marchand. Runtime Enforcement of Parametric Timed Properties with Practical Applications. In *IEEE International Workshop on Discrete Event Systems*, pages 420–427, Cachan, France, May 2014.

[C18] Srinivas Pinisetty, Yliès Falcone, Thierry Jéron, and Hervé Marchand. Runtime Enforcement of Regular Timed Properties. In *Software Verification and Testing, track of the Symposium on Applied Computing ACM-SAC 2014*, pages 1279–1286, Gyeongju, South Korea, March 2014. ACM.

[C19] Akram Idani and Nicolas Stouls. When a Formal Model Rhymes with a Graphical Notation. In *Human-Oriented Formal Methods 2014*, LNCS, Grenoble, France, September 2014. Springer. to appear.

[C20] Akram Idani, Yves Ledru, Abderrahim Ait Wakrime, Rahma Ben Ayed, and Philippe Bon. Towards a tool-based domain specific approach for railway systems modeling and validation. In *International Conference on Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification - RssRail 2019*, Lille, France, June 2019. Springer.

[C21] Amira Radhouani, Akram Idani, Yves Ledru, and Narjes Ben Rajeb. Extraction of Insider Attack Scenarios from a Formal Information System Modeling. In Véronique Cortier and Riadh Robbana, editors, *Formal Methods for Security*, volume 1158, pages 5–19, Tunis, Tunisia, June 2014. CEUR-Wrokshops.

[C22] Amira Radhouani, Akram Idani, Yves Ledru, and Narjes Ben Rajeb. GenISIS : un outil de recherche d'attaques d'initié en Systèmes d'Information (Article court). In *AFADL'16 : Approches Formelles dans l'Assistance au Développement de Logiciels*, Actes de la Conférence AFADL'16 : Approches Formelles dans l'Assistance au Développement de Logiciels, pages 19–26, Besançon, France, 2016.

[C23] Ansem Ben Cheikh, Yoann Blein, Salim Chehida, German Vega, Yves Ledru, and Lydie Du Bousquet. An Environment for the ParTraP Trace Property Language (Tool Demonstration). In *Runtime Verification - 18th International Conference, RV 2018*, pages 437–446, Limassol, Cyprus, November 2018.

[C24] Catherine Oriat, Roland Groz, and Emmanuel Perrier. SIMPA - Simpa Infers Models Pretty Automatically (Outils). In *Approches Formelles dans l'Assistance au Développement de Logiciels (AFADL'16)*, Besançon, France, June 2016.

[C25] Emmanuel Perrier. Inférence et analyse de propriétés dans les protocoles contrôle-commande. In *Approches Formelles dans l'Assistance au Développement de Logiciels (AFADL'16)*, Besançon, France, June 2016.

[C26] Franck de Goër, Christopher Ferreira, and Laurent Mounier. scat: Learning from a Single Execution of a Binary. In *IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, Klagenfurt, Austria, 2017.

[C27] Franck de Goër, Roland Groz, and Laurent Mounier. Lightweight heuristics to retrieve parameter associations from binaries. In *Proceedings of the 5th Program Protection and Reverse Engineering Workshop, PPREW@ACSAC*, Los Angeles, CA, United States, December 2015.

[C28] Franck de Goër, Roland Groz, and Laurent Mounier. Metrics for runtime detection of allocators in binaries. In *10th USENIX Workshop on Cyber Security Experimentation and Test, CSET 2017*, Vancouver, BC, Canada, August 2017.

[C29] Karim Hossen, Catherine Oriat, Roland Groz, and Jean-Luc Richier. Automatic Model Inference of Web Applications for Security Testing. In *Position Statement at SecTest2014, co-located with ICST2014*, Cleveland, Ohio, United States, 2014.

[C30] Lydie Du Bousquet, Mickaël Delahaye, and Catherine Oriat. Applying a Pairwise Coverage Criterion to Scenario-Based Testing. In *Fifth International Workshop on Combinatorial Testing (IWCT 2016)*, Chicago, United States, April 2016.

[C31] Lydie du Bousquet and Masahide Nakamura. Improving Testability of Software Systems that Include a Learning Feature. In *The Tenth International Conference on Advances in System Testing and Validation (VALID)*, Nice, France, October 2018.

[C32] Roland Groz, Adenilso Simao, Alexandre Petrenko, and Catherine Oriat. Inferring Finite State Machines Without Reset Using State Identification Sequences. In Khaled El-Fakih, Gerassimos Barlas, and Nina Yevtushenko, editors, *27th IFIP International Conference on Testing Software and Systems (ICTSS)*, volume LNCS-9447 of *Testing Software and Systems*, pages 161–177, Sharjah and Dubai, United Arab Emirates, November 2015. Part 4: Model and System Testing.

[C33] Roland Groz, Adenilso Simao, and Catherine Oriat. Adaptive Localizer Based on Splitting Trees. In Nina Yevtushenko, Ana Rosa Cavalli, and Hüsnü Yenigü, editors, *29th IFIP International Conference on Testing Software and Systems (ICTSS)*, volume LNCS-10533 of *Testing Software and Systems*, pages 326–332, St. Petersburg, Russia, October 2017. Springer International Publishing. Part 6: Short Contributions.

[C34] Roland Groz, Adenilso Simao, Nicolas Bremond, and Catherine Oriat. Revisiting AI and testing methods to infer FSM models of black-box systems. In *Proceedings of the 13th International Workshop on Automation of Software Test, AST@ICSE 2018, Gothenburg, Sweden, May 28-29, 2018*, pages 16–19. ACM Press, May 2018.

[C35] Roland Groz, Catherine Oriat, and Nicolas Bremond. Inferring Non-resettable Mealy Machines with n States. In *International Conference on Grammatical Inference 2016 (ICGI'16)*, Delft, Netherlands, October 2016.

[C36] Roland Groz, Nicolas Bremond, and Adenilso Simao. Using Adaptive Sequences for Learning Non-Resettable FSMs. In *ICGI: International Conference on Grammatical Inference*, Wroclaw, Poland, September 2018.

[C37] Salim Chehida, Akram Idani, Yves Ledru, and Mustapha Kamel Rahmouni. Extensions du diagramme d'activité pour contrôler l'accès au SI. In *INFORSID 2015*, pages 151–165, Biarritz, France, 2015.

[C38] Yoann Blein. Identification de propriétés pour la validation d'un système cyber-physique médical. In *Approches Formelles dans l'Assistance au Développement de Logiciels (AFADL'16)*, Besançon, France, June 2016.

[C39] Yoann Blein, Arnaud Clere, Fabrice Bertrand, Yves Ledru, Roland Groz, and Lydie Du Bousquet. Improving Trace Generation and Analysis for Medical Devices. In *IEEE International Conference on Software Quality, Reliability and Security Companion, QRS-C 2017*, pages 599–600, Prague, Czech Republic, July 2017.

[C40] Yoann Blein, Yves Ledru, Lydie du-Bousquet, and Roland Groz. Extending specification patterns for verification of parametric traces. In *the 6th Conference on Formal Methods in Software Engineering (FormaliSE'18)*, pages 10–19, Gothenburg, Sweden, June 2018. ACM Press.

[C41] Yves Ledru, Akram Idani, Rahma Ben Ayed, Abderrahim Ait Wakrime, and Philippe Bon. A separation of concerns approach for the verified modelling of railway signalling rules. In *International Conference on Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification - RssRail 2019*, Lille, France, June 2019.

[C42] Yves Ledru, Akram Idani, and Jean-Luc Richier. Validation of a security policy by the test of its formal B specification - a case study. In *Third FME Workshop on Formal Methods in Software Engineering (Formalise'15)*, Third FME Workshop on Formal Methods in Software Engineering (Formalise'15), pages 6–12, Firenze, Italy, 2015. IEEE.

[C43] Yves Ledru, Yoann Blein, Lydie Du Bousquet, Roland Groz, Arnaud Clere, and Fabrice Bertrand. Requirements for a Trace Property Language for Medical Devices. In *the International Workshop on Software Engineering in Healthcare Systems, SEHS@ICSE 2018*, Gothenburg, Sweden, May 2018. ACM Press.

Other products presented in symposia / congress and research seminars

Top 20%

1.1.4 Tools and products

Software

For each software we use the self-assessment criteria of INRIA. [1]

- A stands for Audience (1 to 5),
- SO stands for Software Originality (1 to 4),
- SM stands for Software Maturity (1 to 5),
- EM stands for Evolution and Maintenance (1 to 4),
- and SDL stands for Software Distribution and Licensing (1 to 5).

The following software have seen significant developments in the last five years.

- SIMPA: SIMPA Infers Models Pretty Automatically. It implements a number of active inference algorithms, as well as driver generators to connect to web systems (and other drivers for other types of systems). git@gricad-gitlab.univ-grenoble-alpes.fr:vasco/SIMPA.git
  Self-assessment: *A-2*, *SO-4*, *SM-2*, *EM-2*, *SDL-4*
- ParTraP, a language for the specification of properties on parametric traces is supported by an IDE and an example generator. It is distributed as an Eclipse plug-in at http://vasco.imag.fr/tools/partrap/. The tool is distributed under the LGPL v3 licence.
  Self-assessment: *A-3*, *SO-3*, *SM-2.5*, *EM-2*, *SDL-4*
- B4MSecure, which integrates SecureUML and B, is distributed as an Eclipse plug-in from http://vasco.imag.fr/tools/b4msecure/. The tool is distributed under the LGPL v3 licence. Written and video documentation are also provided.
  Self-assessment: *A-3*, *SO-3*, *SM-3*, *EM-2*, *SDL-4*
- Meeduse (http://vasco.imag.fr/tools/meeduse/), a tool to mix the formal B method with Domain Specific Languages (DSLs) done in EMF-based platforms like Sirius, GMF and XText. Demonstration videos are provided and the tool distribution is currently done by e-mail on demand.
  Self-assessment: *A-2*, *SO-3*, *SM-1*, *EM-2*, *SDL-2*
- `scat`: analysis of binary code to retrieve function parameters and their types, as well as functions that are strongly coupled, such as file open/close, or memory allocators. https://github.com/Frky/scat
  Self-assessment: *A-2*, *SO-3*, *SM-2*, *EM-2*, *SDL-4*

The following software was available at the start of the 2014-19 period. Although they were not involved in our recent research, these tools are still maintained and distributed.

- The Tobias combinatorial generator is available as a service through a web page http://tobias.liglab.fr/. Written and video documentation are provided and the service has been experimented during master's courses.
  Self-assessment: *A-3*, *SO-3*, *SM-3*, *EM-2*, *SDL-4*
- RoZ, a tool to integrate UML and Z, is currently rearchitectured to share components with B4MSecure. It will be distributed under the LGPL v3 licence at http://vasco.imag.fr/RoZ/. The previous version of the software is used by MIAGE master's students as part of their curriculum.
  Self-assessment: *A-2*, *SO-3*, *SM-3*, *EM-2*, *SDL-2*

[1] https://www.inria.fr/medias/recrutement-metiers/pdf/criteria-for-software-self-assessment

1.1.5 Instruments and methodology

Nothing to report.

1.1.6 Other products

Nothing to report.

1.1.7 Editorial activities

Nothing to report.

1.1.8 Reviewing activities

Reviewing of articles

Altogether, the members of the VASCO team reviewed 215 articles in journals and conferences.

- Yves Ledru was reviewer for the following journals :
  International journals: IEEE Trans. on Software Engineering (IEEE Computer Society Press), Formal Aspects of Computing (Springer), Real-Time Systems (Springer), IEEE Transactions on Reliability (IEEE Computer Society Press), ACM Trans. on Software Engineering Methodology (ACM), Journal of Software : Evolution and Process (Wiley), Computer Journal (Oxford University Press), Logic Journal of the IGPL (Oxford University Press), Frontiers of Information Technology & Electronic Engineering (Springer), Journal of Information Security and Applications (Elsevier).
  French-speaking journals: Technique et Science Informatiques (TSI) and Ingénierie des Systèmes d'Information (ISI).

- Yves Ledru was member of the programme committee of the following conferences:
  International conferences: FHIES/SEHC 2014, FM '14, '15, '16 et '18, FormaliSE '14, '15, '16 and '17 , MEDI '14, '15, '16, '17, '18 and '19, ERTS2 '14, SAC/SVT Track '17 and '18, SecureMDE '18, WETICE/FVSBS '15, '16 and '19, WISSE '14, '15, and '16.
  French-speaking conferences: AFADL '14, '15, '16, '17, '18 and '19, CAL '15 and '16, CIEL '17, INFORSID '16, JLDP '14.

- Jean-Luc Richier was reviewer for the following international journals :
  Int. Journal of Space Based and Situated Computing (IJSSC), Elsevier Information and Software Technology, Journal of Computer Networks and Communications.

- Roland Groz was reviewer for the following journals :
  Software Testing, Verification and Reliability (Wiley), International Journal on Software and Systems Modeling (Springer), Empirical Software Engineering (Springer), Software Quality Journal (Springer), Journal of Systems and Software (Elsevier).

- Roland Groz was member of the programme committee of the following conferences:
  SECTEST 2015, ICGI 2016, Int. Conference on Testing Software and Systems ICTSS'17, '15.

- Akram Idani was reviewer for the following international journals:
  Journal of Intelligent Information and Database Systems (Interscience) – 2015
  Software and Systems Modeling (Springer), Journal of Object Technology, Logic Journal of the IGPL (Oxford University Press), IEEE Software (IEEE), Journal of Critical Computer-Based Systems (Inderscience), Journal of Systems and Software (Elsevier).

- Akram Idani was member of the programme committee of:
  Int. Symposium on Symbolic Computation in Software Science (2016)
  Int. Conference on Model and Data Engineering MEDI'16, '15, '14
  Int. Workshop on Verification of Model Transformations VOLT'15, '14
  Int. Workshop on Information Systems Security Engineering WISSE'16, '15
  Conférence francophone AFADL'18, '17, '16, '15, '14
  34ème Congrès INFORSID 2017

- Lydie du Bousquet was reviewer for the following international journals:
  Computing Surveys Review (ACM), Transactions on Reliability (IEEE), Transactions on Software Engineering (IEEE), Journal of Computer Science and Technology (Springer), Journal of Systems and Software (Elsevier)

- Lydie du Bousquet was member of the programme committee of:
  IEEE/ACIS Int. Conference on Computer and Information Science - ICIS'19, '18, '17, '16
  Automated Software Testing - A-TEST'19)
  IEEE Int. Conference on Software Testing, Verification, and Validation - ICST'14
  Int. Conference on Quality Software QRS'14
  Int. Conference on Software Engineering Advances - ICSEA'18, '17, '16, '15, '14)
  Int. Conference on Advances in System Testing and Validation - Valid'18, '17, '16, '15, '14
  Int. Workshop on Mutation Analysis - Mutation'16, '15, '14
  Int. Workshop on User Interface Test Automation INTUITEST'17, '16 and Int. Workshop on User Interface Test Automation and TESting Techniques for event BasED Software '19, '18
  Conférence francophone AFADL'19, '18, '17, '16, '15.

Grant evaluation (public or charities)

- Yves Ledru:
  - Expert reviews for the MEI (Mission Expertise Internationale) of MEST (DGRI) which evaluates international programmes such as PHC (1 project in 2014, 4 in 2015, 1 in 2016, 1 in 2018).
  - Reviewer in 2015 for a project submitted to the generic call of ANR.
  - Mid-term Expert for the ANR GEMOC project (2014).
  - Reviewer for Université de Namur (Belgique) in 2018, for the CIMI Labex (Toulouse, 2017) and the Hauts de France region (2017).

Reviewing of research institutes

Yves Ledru:

- Member of the evaluation committee of ONERA/DTIM in 2014.
- For Hcéres (Haut conseil de l'évaluation de la recherche et de l'enseignement supérieur) : member of the evaluation committee of the CRIStAL laboratory (Lille, 2019).

Participation in institutional committees and juries (CNRS, Inserm, etc.)

- Lydie du Bousquet was member of the CE25 ANR evaluation committee in 2018.
- Yves Ledru chaired the selection process of ARC6 for grant evaluations.
- Yves Ledru was member from 2007 till 2018 of the scientific committee of the IMAGINOVE competitive cluster.

1.1.9 Academic research grants

European (ERC, H2020, etc.) and international (NSF, JSPS, NIH, World Bank, FAO, etc.) grants - partnership

SPACIOS project: "Secure Provision and Consumption in the Internet of Services", EC FP7/STREP, started on October 1st 2010, ended on January 30th 2014.
Local Partner: Grenoble INP, local responsible: Roland Groz
Partners: U. di Verona (lead), U. di Genova, ETH Zürich, IeAT, T.U. München, SAP, Siemens
Description: Methods and tools to detect vulnerabilities in deployable services over the Internet.

National public grants (ANR, PHRC, FUI, INCA, etc.) - coordination

Safe PICS: "Intelligent d'accord, mais aussi sûr et sécurisé", financed by CNRS, started on January 1st 2015 and ended on December 31st 2017
Coordinator : Lydie du Bousquet
Local partner : CNRS Alpes
Partners: Kobe University
Description: validation of smart systems, i.e. which learn from their environment.

National public grants (ANR, PHRC, FUI, INCA, etc.) - partnership

MODMED project: "MODel and verify MEDical Cyber-Physical Systems with execution Trace Properties", financed by ANR, started on October 1st 2015, ended on March 31st 2019
Local Partner: UGA, local responsible: Yves Ledru
Partners: MinMaxMedical, Blue Ortho
Description: This project designs a language and tools to produce traces of medical devices, and then specify and evaluate properties on these traces. LIG defined the ParTraP language to express these properties, and several tools to support this language.

SACADE project: "Scénarios d'Attaque Contre Automates avec Distribution et Encapsulation", financed by the ASTRID programme of ANR, started on October 1st 2016 and ended on April 30th 2019
Local Partner: Grenoble INP, local responsible: Roland Groz
Partners: GIPSA-lab and Vérimag (two Grenoble laboratories)
Description: The goal of the project is to propose a methodology to detect vulnerabilities and attacks against a SCADA system. It adopts a Model-Based Testing approach where a model of the target architecture is exploited. The project involves two teams of the LIG: Drakkar and VASCO.

PHILAE project: "From Model-Based Testing to Cognitive Test Automation", financed by ANR, started on October 1st 2018, ended on March 31st 2022
Local Partner: Grenoble INP, local responsible: Roland Groz
Partners: Université Bourgogne Franche-Comté, Orange Labs Service, Smartesting, Simula Labs (Norway), University of the Sunshine Coast (Australia)
Description: The goal of the project is to automate the production of models in a Model-Based Testing approach by exploiting traces of the system and building models using model inference.

InS3PECT PEPS: "Ingénierie Système de Services Sécurisés Pour ObjEts ConnecTés", financed by CNRS, started on January 1st 2017 and ended on December 31st 2017
Local Partner: CNRS, local responsible: Yves Ledru
Partners: Nice University, LabSTICC
Description: security for IoT.

Local grants (collectivités territoriales) - coordination

ARC6, Academic Research Community, "Technologies de l'Information et de la Communication et Usages Informatiques Innovants"; financed by Auvergne-Rhône-Alpes region 2014-2018 Coordinator : Yves Ledru
Local partner : UGA,
Partners: 42 laboratories in the Auvergne-Rhône-Alpes region
Description: These projects correspond to the scientific responsibility for regional research networks in the fields of ICT. Budget was dedicated to support scientific animations organized by the network.

Kouno-Tori: "systèmes cyber-physiques pour un monde plus intelligent"; financed by Auvergne-Rhône-Alpes region 2018-2019
Coordinator : Lydie du Bousquet
Local partner : UGA,
Partners: University of Kobe (Japan)
Description: This project supports an international collaboration with the University of Kobe (Japan) on the theme of the validation of smart applications. It mainly supports visits to our japanese partner.

PIA (labex, equipex etc.) grants - partnership

ARAMIS project: "Architecture Robuste pour les Automates et Matériels des Infrastructures Sensibles". PIA "Technologie coeur de filière: Sécurité numérique", started on October 2014, ended on September 2017.
Local Partner: UGA, local responsible: Jean-Luc Richier
Partners: ATOS Worldgrid, CEA Leti, Seclab, UGA (4 laboratories: LIG with 3 teams (Drakkar, MOAIS, VASCO), Institut Fourier, LJK, Verimag)
Description: This project developed a industrial prototype providing a secure communication channel for insdustrial protocols such as SCADA, including filtering mechanisms.

Grants from foundations and charities (ARC, FMR, FRM, etc.) - partnership

NeXTRegio, "ERTMS Régional: Méthodologie innovante pour la spécification de l'ERTMS Régional sous contrainte de sécurité", financed by Institut de Recherche Technologique (IRT) Railenium, started November 1st 2016, and ended on May 20th 2019
Local Partners: UGA and Grenoble INP, local responsible: Yves Ledru
Partners: IRT Railenium
Description: This project aims at performing a system level analysis of a railway signalling system. It is supported by the B4MSecure tool which makes a separation of concerns between a physical model where accidents may happen, and permissions which rule the behaviour of agents and prevent accidents.

1.1.10 Visiting senior scientists and post-doc

Post-docs (total number)

2 post-docs.

Name	*Status*	*Date*
CHEHIDA Salim	Post-Doc	01/03/2018 - 31/03/2019
WANG Lingxiao	Post-Doc	01/06/2016 - 30/04/2017

Foreign post-docs

2 (Algeria and China)

Visiting scientists (total number)

6 visiting scientists.

Foreign visiting scientists

Name	*Status*	Country	*Date*
CHEHIDA Salim	PhD Student	Algeria	01/10/14 - 31/03/16
JABER Mohamad	Assistant Professor, American Univ. of Beirut	Lebanon	01/06/14 - 30/06/14
NACEUR Maha	PhD Student	Tunisia	13/12/14 - 31/03/15
NAKAMURA Masahide	Associate Professor, Univ. of Kobe	Japan	03/02/15 - 30/10/15 21/03/19 - 25/03/19
PETRENKO Alexandre	Professor, CRIM, Montréal	Canada	05/05/14 - 02/06/14 10/10/16 - 15/10/16
SIMAO Adenilso	Professor, Univ. Sao Paulo	Brasil	08/09/14 - 19/09/14 10/11/17 - 22/11/17

1.1.11 Scientific recognition

Prizes and/or distinctions

- In 2016, the ITEA-2 project Diamonds (October 2010 - June 2013) was awarded "EUREKA Innovation Award 2015/2016" in the category 'Added Value' during the "EUREKA Week Innovation 2016 - Smart Cities - Sustainable & Gravitational Communities" .
- In 2015, Amira Radhouani, PhD Student in the VASCO team was runner-up at the Grenoble Final of "Ma thèse en 180 secondes".
- In 2015, the paper "Lightweight heuristics to retrieve parameter associations from binaries" [C27] won the best paper award at the 5th Program Protection and Reverse Engineering Workshop, PPREW@ACSAC, Los Angeles.
- In 2019, the paper "Quelques pas vers l'Honnêteté et l'Explicabilité de moteurs de recherche sur le Web" [C13] won the best paper award at the COnférence en Recherche d'Information et Applications, CORIA'19, Villeurbanne, France.

Invitations to meetings and symposia

- Yves Ledru was invited to the workshop "JML : Advancing Specification Language Methodologies", March 23-27 2015, at the Lorentz center, Leiden, Netherlands. (Lorentz Center organizes one week workshops similar to the ones of Schloss Dagstuhl).
- Roland Groz was invited to the workshop "Systematic Analysis of Security Protocol Implementations", June 11-15, 2018 at the Lorentz center, Leiden, Netherlands. (Lorentz Center organizes one week workshops similar to the ones of Schloss Dagstuhl).
- Roland Groz was invited to the workshop "Machine Learning for Dynamic Software Analysis: Potentials and Limits", April 24-27, 2016 at Schloss Dagstuhl, Germany.
- Yves Ledru was invited to the pannels of the National days of GDR GPL "Génie de la programmation et du logiciel et Agilité : un mariage heureux ?" (Bordeaux 2015) and "Ingénierie des exigences : de l'enseignement à la pratique" (Grenoble 2018).

Members' long-term visits abroad

- Lydie du Bousquet visited University of Kobe three times: 18/7/2016 – 15/8/2016, 18/7/2017 – 15/8/2017, and 18/7/2018 – 15/8/2018.
- Roland Groz visited Univ. of Sao Paulo (23/9/2016 – 29/9/2016).
- Amira Radhouani visited the University of Dusseldorf (december 2016)

1.1.12 Scientific animation

Organisations of meetings and symposia

All members of the VASCO team were involved in the organisation of the national days of GDR GPL (Génie de la programmation et du logiciel) in Grenoble June 12-15, 2018 and co-located events: french speaking conferences AFADL, CAL and CIEL.

As scientific leader of the ARC6 regional network "Technologies de l'Information et de la Communication et Usages Informatiques Innovants", Yves Ledru organized:

- an annual scientific day for the ARC6 community from 2014 until 2018, alternating between Lyon and Grenoble,
- industrial day in 2016 (Lyon), 2014 and 2017 (Grenoble).

Scientific and steering committees

- From 2014-2018, Yves Ledru was scientific leader of the ARC6 regional network "Technologies de l'Information et de la Communication et Usages Informatiques Innovants", which grouped 42 laboratories from the Auvergne Rhône Alpes Region.
- Yves Ledru is member of the board of the GDR GPL, acting as responsible for the web site and the mailing lists (2014-2019)
- Akram Idani is co-responsible of the MFDL working group of GDR GPL (2014-2019).
- In 2014, Lydie du Bousquet was co-responsible of the MTV2 working group of GDR GPL.

1.2 Interaction of the unit with the non-academic world, impacts on economy, society, culture or health

1.2.1 Socio-economic interactions / Patents

Nothing to report.

1.2.2 Socio-economic interactions

Nothing to report.

1.2.3 Expertise

Nothing to report.

1.2.4 Public outreach

Journal articles, interviews, book edition, videos, other popularization outputs, debates on science and society, etc.

Lydie du Bousquet published a video in the series "L'objet de mes recherches" on the Youtube channel of Université Joseph Fourier in january 2015.

1.3 Involvement of the unit and of each team in training through research

1.3.1 Educational outputs

Nothing to report.

1.3.2 Scientific productions (articles, books, etc.) from theses

Scientific productions (articles, books, etc.) from theses

PhD Student	Journals	Conferences since 2014	Conferences before 2014
BLEIN Yoann		[C23] [C38] [C39] [C40] [C43]	
DE GOER DE HERVE Franck		[C6] [C26] [C27] [C28]	
DUCHENE Fabien		[C5]	3
HOSSEN Karim		[C1][C2] [C29]	2
NGUYEN Manh Dung			
PERRIER Emmanuel		[C24] [C25]	
RADHOUANI Amira	[OA1] [J4]	[C21] [C22]	
REY Alexis			

Mean number of publications per student (Biology & Science and technology only)

The mean number of publications for students who defended is 4.4 publications/student.

1.3.3 Training

Habilitated (HDR) scientists

3 HDR : Lydie du Bousquet, Roland Groz, Yves Ledru

HDR obtained during the period

0

PhD students (total number)

8 PhD students were affiliated to VASCO during the period 2014-19.

Name	*Dates of contract*	*date of defense*	*Duration*
BLEIN Yoann	01/10/15 - 30/09/19	15/04/19	42,5 months
DE GOER DE HERVE Franck	01/10/14 - 20/10/17	20/10/17	36,5 months
DUCHENE Fabien	17/01/11 - 02/06/14	02/06/14	40,5 months
HOSSEN Karim	01/12/10 - 31/12/14	15/12/14	48,5 months
NGUYEN Manh Dung	27/11/17 27/11/20		
PERRIER Emmanuel	01/10/14 - 11/05/17	thesis stopped	
RADHOUANI Amira	01/10/13 - 23/06/17	23/06/17	45 months
REY Alexis	20/10/2017 - 31/12/20		

Defended PhDs

5

Mean PhD duration

42,6 months

Internships (M1, M2)

56 internships at master's level.

People in charge for a mention or a master's degree course (total number)

- Lydie du Bousquet is in charge of the M1 Informatique at UGA.
- Akram Idani is co-responsible of specialization AISSE of the M2 MoSIG.
- All members (6) of the VASCO team teach at Master's level in degrees featured by UGA or Grenoble INP.

People in charge for a mention or a master's degree course with international certification (Erasmus mundus)

Lydie du Bousquet is preparing an International Erasmus Mundus Master's degree linking the Universities of Barcelona (Spain), Bochum (Germany), Tsukuba (Japan) with UGA.