Thesis Seminars by Student Doctoral Year

- **1st Year**
  - **Student:** Matteo Zavatteri
    - **Adviser:** Luca Viganò
    - **Date, Time, Location:** 29/10, room 1.75 CV2
    - **Title:** Enforcing Security Policies While Executing Workflows
    - **Abstract:** Business Processes handled by Web Applications are more and more widespread. A web application is an application written in some programming language which supports current web standards and related protocols, whereas a business process consists of a set of tasks to be executed, in some order, to achieve some business goal(s). This work aims at enforcing security policies while the workflow (that is, the technological part in charge of executing the business process) is being executed. Abstracting from the specific security measures, we cannot forget to say that, in general, security goes against the usability of a system. Therefore, the first requisite to be dealt with is the flexibility of the security methods we are going to use. Moreover, time is an intrinsic aspect of each business reality and it is often neglected, or managed with ad-hoc solutions, technologically speaking. For these reason I propose to build a framework which allows to formalise a two level transition system in which one part is in charge of handling the access control part (by relying on role-based access control models and their temporal extensions), whereas the other is in charge of handling the workflow part respecting temporal constraints (relying on structured workflow modelling languages). Once this framework is ready, it will be possible to investigate how to: (i) formalise users' authentication and authorisation in web contexts, (ii) set up temporal delegations and study interesting properties such as transitivity, (iii) validate the system with model checking techniques in order to find attack traces (that is, a sequence of transitions which lead the system to a state in which some security properties do not hold anymore. Finally, as a concretisation of the scientific contributions, I propose to use TRBAC as the access control model, and TNest as the workflow control model, to build a proof of concept.

  - **Student:** Rosario Distefano
    - **Adviser:** Franco Fummi
    - **Date, Time, Location:** 4/11, 14.00, meeting room 2nd floor
    - **Title:** Modeling Biological Systems with Electronic Design Automation
    - **Abstract:** Model development and analysis of biological systems is recognized as a key requirement for integrating in-vitro and in-vivo experimental data. In-silico simulations of a biochemical model allows one to test different experimental conditions, helping in the discovery of the dynamics that regulate the system. Several characteristics and issues of biological system modeling are common to the electronics system modeling, such as concurrency, reactivity, abstraction levels, as well as state space explosion during verification. This thesis proposes a modeling and simulation framework for discrete event-based execution of biochemical systems through the use of EDA techniques. Moreover, the proposed framework uses techniques like property checking and mutation analysis in order to reach as much as possible a complete understanding of the biological system.

  - **Student:** Gabriele Tosadori
    - **Adviser:** Fausto Spoto
    - **Date, Time, Location:** 4/11, 11.30, ground floor meeting room
    - **Title:** Biological network analysis: from topological indexes to biological applications
    - **Abstract:** I will describe a Systems Biology approach that involves the topological analysis of biological networks by using some metrics called centralities. I will give some basic about graphs, that are the mathematical model used for this kind of study and then i will explain what i am going to do in order to understand how the known topological indexes (e.g. Closeness, Degree, Betweenness) could be useful in investigating the properties of a network and its nodes.

  - **Student:** Giorgio Roffo
    - **Adviser:** Marco Cristani
    - **Date, Time, Location:** 6/11, 11.30am, Sala riunioni, floor 2,
    - **Title:** statistical analysis of text chats: a novel challenge for social media
    - **Abstract:** No other technology penetrated our everyday life as quickly and ubiquitously as social media. Billions of users are using these programs every day, exploiting novel communication means. Among these, "instant messaging" is one of the most pervasive. The peculiarity of an

exchange of instant messages is that it shows aspects of literary text and spoken conversation, in which textual information delivery follows turn-taking dynamics, resembling spoken interactions. This create a hybrid way of communicating, originating novel strategies for enriching the messages (the use of the emoticon as example). This thesis aims at studying text chats under a statistical point of view, inheriting what has been done with the automatic analysis of texts and with the modeling of spoken interactions, with the goal of producing novel strategies for capturing information about the conversations themselves but also about the users, from their style of communicating until some personality traits. The presentation will present this intriguing research challenge, showing preliminary results and discussing the research direction I would like to explore in the next years.

- **Student:** Matteo Denitto
  - **Adviser:** Manuele Bicego
  - **Date, Time, Location:** 10/11, 10.30, aula riunioni al secondo piano di CV2
  - **Title:** Factor Graphs for Pattern Recognition
  - **Abstract:** Graphical representations (such as flow charts, diagrams) are key tools for machine intelligence. A notable example of graphical representations are Factor Graphs often used in pattern recognition, computer vision and coding theory. Factor graphs allow to represent a general global functions as a decomposition of local functions and they are used to perform both optimization and inference. Due to their general formulation factor graphs can be used to solve a wide range of problems, nonetheless their design and resolution are not easy tasks. My thesis aims at facing the challenges provided by these models, focusing on novel design methodology and resolution algorithms in the context of pattern recognition and bioinformatics.

- **Student:** Alberto Lovato
  - **Adviser:** Fausto Spoto
  - **Date, Time, Location:** November 12, 9:30, lecture hall H, CV2
  - **Title:** Fact Semantics and Verification of Java's Concurrency Annotations
  - **Abstract:** Concurrency is an integral part of any computing system. It is used to increase performance of programs, when multiple threads of execution happen at the same time. Concurrency bugs are not easily detected, and so it is desirable to have automatic software to verify multithreaded correctness. There already exist tools for concurrent software verification, but they are still in their infancy and typically unsound or applicable to very restrictive classes of software (no heap management). I propose the use of code annotations for documentation as well as verification of concurrency properties of Java programs. I will start with new precise definitions of existing annotations, introduced informally with the 2006 book "Java Concurrency in Practice": @Immutable, @ThreadSafe, @NotThreadSafe and @GuardedBy. They were proposed for simple documentation, and adopted sparingly in software projects, among which the open source ones Google Guava, Bitcoinj, Parfait. Existing tools verifying these annotations are incomplete, or just incorrect, and so my work should include the development of verification procedures for related properties (e.g., immutability). My proposal is to combine user-provided annotations and verification procedures to help producing well-documented and verified concurrent software.

- **2nd Year**
  - **Student:** Mauro Zucchelli
    - **Adviser:** Gloria Menegaz
    - **Date, Time, Location:** 5/11, 13:30, aula G.
    - **Title:** Towards Brain Tissue Microstructure Characterization using Diffusion MRI
    - **Abstract:** Diffusion Magnetic Resonance Imaging (dMRI) quantifies the diffusion of the water molecules in biological tissues. From the diffusion signal it is possible to calculate the corresponding ensemble average propagator (EAP), representing the ensemble average probability density function of the population of water molecules in the physical space. Nowadays different reconstruction techniques are used to model the diffusion signal starting from complex acquisition schemes in Fourier space in order to reconstruct the propagator. Numerous metrics can be then derived from the EAP in order to extract information about brain tissues characterization, white matter fibers orientation and fibre density. The overall goal of this thesis is to improve the state-of-the-art (SOA) by facing the following issues: identification of the optimal sampling in the q-space; identification of the optimal basis for signal reconstruction; definition of new scalar indices (features) that are anatomically and biophysically plausible besides being objectively measurable in a robust, accurate and stable manner (numerical biomarkers). This will open new perspectives in both the scientific and clinical framework for the

assessment of structural properties of tissues in both healthy subjects and patients besides supporting and improving cortical connectivity models.

- **Student:** Francesco Visentin
  - **Adviser:** Paolo Fiorini
  - **Date, Time, Location:** 6/11, 14:30, Aula Verde.
  - **Title:** A first step toward distributed sensing for soft robot
  - **Abstract:** Soft robots are a new trend in the robotic community. They are made by soft, deformable materials that enable them to easily conform to unstructured environment like biological systems do. In order to control this ability, sensors that return information about their spatial configuration and feedback from the environments are needed. Current solutions consist in the use of "classical" type of sensor that are (usually) bulky and thus limit the capabilities of the deformable material. A different type of sensors have to be developed in order to exploit all the features of the material used for the robot structure. In this presentation the first step toward the development of a novel type of sensor that enables sensing capabilities without limiting the deformation property of the soft material is presented. The sensor is based on a imaging technique known as Electrical Imaging Tomography.

- **Student:** Michele Lora
  - **Adviser:** Franco Fummi
  - **Date, Time, Location:** 13/11, 11.00, Aula verde
  - **Title:** Making Homogeneous the Platform-Based Design of Heterogeneous Cyber-Physical Systems
  - **Abstract:** In the last few years the term Embedded System has been more and more replaced by the concept of Cyber-Physical System. This is due to the increasing attention given by the designers to the physical world interacting with the system. Considering the surrounding environment as a further dimension in the design of computational devices lead to a whole new level of heterogeneity that has to be handle. At the current State of the art this heterogeneity is handled exploiting model based design, sacrificing the reuse of components, often necessary to target time-to-market and cost constraints. Alternatively, reuse is supported by co-simulation techniques, usually unable to assure a correct integration. A set of methodologies capable to form a design flow to model Cyber-Physical Systems, allowing reuse of previously designed components while assuring the system integration correctness is missing. Thus, it is a crucial target of the current research in this area. This problem is addressed by the proposed thesis, developing a framework to automatically integrate heterogeneous components into homogeneous and domain-independent models. Then, a set of methodologies is defined on these homogeneous models, to efficiently simulate, manipulate and synthesize Cyber-Physical Systems.

- **Student:** Matteo Pascucci
  - **Adviser:** Andrea Masini
  - **Date, Time, Location:** 26/9
  - **Title:** Modal logics with propositional constants
  - **Abstract:** Propositional constants are propositional symbols whose interpretation is somehow fixed and their use in modal logic dates back at least to the Fifties. In some temporal logics a particular category of propositional constants, called nominals or clock-propositions, are used to "name" within the syntax the instants of a structure. My current work aims to investigate the semantics and proof theory of some of these logics. In the first part I will discuss the idea that the range of interpretations for a system whose language includes propositional constants can be defined in an accurate way in terms of general frames. The second part concerns the proposal of a deductive system for a language without any operator of realization and the third part illustrates how propositional constants can be used to obtain results of interdefinability among modal notions.

- **Student:** Tara Ghasempouri
  - **Adviser:** Graziano Pravadelli
  - **Date, Time, Location:** 12/11, 11, meeting room, second floor CV2
  - **Title:** Improving ABV by automatic generation and abstraction of PSL assertions
  - **Abstract:** Assertion-based Verification (ABV) aims at providing verification engineers with a way to formally capture the intended specifications, through the definition of logic assertions, and to formally check their compliance with the actual implementation of the intended design. Due to the huge effort required for the definition of such assertions, relevant research directions are guided by the need of simplify both assertion definition and their reuse throughout the

embedded system design flow. In this context, several approaches exist in the literature for the automatic extraction of formal assertions. Some of them, rely on static analysis of the source code, other dynamically mine specifications by analyzing simulation traces. In both cases, most of them work on techniques which are suited only for gate level or RTL HW models, or SW protocols. Moreover, they suffer of scalability problems which prevent their wide adoption for large designs. This thesis proposes a dynamic specification mining methodology that works independently from the considered abstraction level (i.e., gate-level, RTL and system level HW descriptions, as well as, embedded SW). The proposed approach aims to obtain a simple, but high-quality set of assertions and to optimize the overall execution time in comparison with existing methodologies. A technique is also described to rank the interestingness of extracted assertions and prune those that appear to be irrelevant. On the other hand, the recent works on system-level design and transaction level modeling (TLM) face with new challenges for reusing existing RTL IPs and their verification environment in TLM-based design flows. While techniques and tools to abstract RTL IPs into TLM models have begun to appear, the problem of reusing, at TLM, an assertion-based verification environment originally developed for an RTL IPs is still under explored. Some works propose techniques and frameworks to deal with ABV at TLM, with a top-down flow. But, the reuse of existing assertions in an RTL to TLM bottom-up design flow has not been analyzed yet. To fill in the gap, a new methodology is proposed in this thesis to reuse assertions originally defined for a given RTL IP, to verify the corresponding TLM model.

- **Student:** Filippo Bistaffa
  - **Adviser:** Alessandro Farinelli
  - **Date, Time, Location:** Skype conference call
  - **Title:** Combinatorial optimisation problems in large-scale multi-agent systems
  - **Abstract:** Multi-agent systems represent a powerful approach to model and solve significant problems in several application scenarios such as intelligent energy management, transportation, logistics and sensor networks. In general, multi-agent systems are characterised by complex dynamics and interactions among a large number of agents, that usually translate into hard combinatorial problems, whose solution is very demanding from the computational point of view. Hence, the study of innovative techniques which can deal with such computational complexity is fundamental and would give a strong contribution to the research in this scenarios. My thesis focuses on the design of algorithms which tackle such hard problems, in order to solve realistic challenges in large-scale multi-agent scenarios, and on the study of highly parallel computational models (e.g., GPGPUs or many-core CPUs), that can fully exploit the high degree of parallelism of modern hardware architectures hence improving the solution process. In particular, my current research focuses on forming groups of agents for two practical scenarios, i.e., collective energy purchasing and social ridesharing. In these contexts, we provide novel models and techniques to compute optimal and approximate solutions with good quality guarantees for large-scale systems.
-

- **3rd Year**
  - **Student:** Pietro Lovato
    - **Adviser:** Manuele Bicego
    - **Date, Time, Location:** 27/10/2014, 10:30, sala verde
    - **Title:** Bag of words approaches for bioinformatics
    - **Abstract:** In recent years, several Pattern Recognition and Computer Vision problems have been successfully faced by techniques based on the "bag of words" representation - a representation which characterizes an object with a vector of counts of basic elements constituting the object. Even if largely applied to several scientific fields (with increasingly sophisticated approaches such as topic models), techniques based on this representation have not been completely exploited in Bioinformatics, due to the methodological and applicative challenges derived from the peculiar scenario. Nevertheless, in this context the bag of words paradigm is ubiquitous: many tasks can be described as counting basic repeating elements, and highly interpretable solutions (a stringent need in nowadays bioinformatics research) can be effectively derived. The aim of the talk is to illustrate the problems related to the creation of bag of words models and representations for some specific bioinformatics problems, such as the microarray expression analysis, the classification of proteins sequences, or the analysis of self-immune diseases. In each case, the suitability of the bag of words representation will be highlighted, and possible solutions - developed during the three years of my PhD studentship - will be presented.
  - **Student:** Michele Peroli

        - **Adviser:** Luca Viganò
        - **Date, Time, Location:** 30/10
        - **Title:** A Model-Based Testing Approach for Web Applications
        - **Abstract:** Penetration testing is the most common approach for testing the security of web applications, but model-based testing has been steadily maturing into a viable alternative/complementary approach. Penetration testing is very efficient but the experience of the security analyst is crucial; model-based testing relies on formal methods but the security analyst has to first create a suitable model of the application under test. In my thesis, I propose a formal and flexible model-based security testing framework that contributes to filling the gap between these two security testing approaches. This is possible through the use of a database of actions and their low-level definition that ties concrete actions, performed through a web browser, to high-level actions present in the model.

    - **Student:** Vincenzo Bonnici
        - **Adviser:** Vincenzo Manca
        - **Date, Time, Location:** 6/11 at 9:30 am in Sala Riunioni Secondo Piano
        - **Title:** Unconventional Genomes and Biological Network Analysis
        - **Abstract:** The research works of my Ph.D. thesis concern the informational and relational analysis of biological data. Informational analysis aims to provide a systematic approach to analyze genomic sequences. The studies extend an existing project, called InfoGenomics, where well-characterized dictionary-based genomic features are presented. Part of the new contribution is focused on genomic distributions, such as those regarding occurrence and recurrence of k-mers, in real and synthetic genomes. A natural development is the definition of algorithms able to localize regions where some distributional patterns occur, in order to yield informational genome annotation useful in the recognition of biological functions. Genomic functional elements and the other biological entities are linked together in biological networks to describe complex biological systems. Part of the new contribution regards the extraction and integration of biological entity relations from scientific sources. The subgraph isomorphism (SubGI) problem plays and important role in some network-based applications. Algorithms for its efficient resolution on biological data are presented. They include a new SubGI algorithm for the one-to-one case, winner at the ICPR Biograph2014 contest, and its parallelization, as well as the parallelized version of a methodology for searching in databases of graphs.

- **4th Year**
    - **Student:** Alberto Calvi
        - **Adviser:** Luca Viganò
        - **Date, Time, Location:** 27/10/2014, 10:30, sala verde
        - **Title:** Model-Based Security Testing: Automated Generation of Vulnerability-driven Test Cases
        - **Abstract:** When it comes to security testing, the skills and experience the tester has acquired during his activity are the key factors that will determine the accuracy and efficiency of the testing process. Model-Based Testing (MBT) is a research field that has been growing and developing for years and it has been lately applied also to test the security of web services. MBT consists in exploiting a formal model of the System Under Test (SUT) and model-checking tools to cast the test generation problem as a model-checking problem. This reduction allows for the generation of a set of Abstract Test Cases (ATC). The objective of my Ph.D. thesis is the definition and implementation of formal techniques to test the security of web applications and communication protocols. To achieve this goal I have developed and applied Mutation Testing techniques, assuming the presence of a secure model of the SUT, to generate ATC that, after a concretization step, can be executed on the SUT's implementation. I have also designed and developed a more general MBT approach based on the idea of Chained Attacks, a sequence of exploits allowing an intruder to attack the security of a web application, and the formalization of the web intruder. This new MBT approach also provide means for the semi-automatic generation of a SUT's model that is usually a task preventing the application of MBT techniques in the industrial field.

    - **Student:** Marco Rocchetto
        - **Adiser:** Luca Viganò
        - **Date, Time, Location:** 27/10/2014
        - **Title:** Automated reasoning for the verification of security protocols and web applications
        - **Abstract:** Interpolation has been successfully applied in formal methods for model checking and test-case generation for sequential programs. Security protocols, however, exhibit such idiosyncrasies that make them unsuitable to the direct application of interpolation.

I address this problem and present an interpolation-based method for security protocol verification. My method starts from a protocol specification and combines Craig interpolation, symbolic execution and the standard Dolev-Yao intruder model to search for possible attacks on the protocol. Interpolants are generated as a response to search failure in order to prune possible useless traces and speed up the exploration. I illustrate my method by means of concrete examples and discuss the results obtained by using a prototype implementation.

Thesis Seminars by Academic Adviser

- **Manuele Bicego**
  - **Student:** Matteo Denitto
    - **Year:** 1st
    - **Date, Time, Location:** 10/11, 10.30, aula riunioni al secondo piano di CV2
    - **Title:** Factor Graphs for Pattern Recognition
    - **Abstract:** Graphical representations (such as flow charts, diagrams) are key tools for machine intelligence. A notable example of graphical representations are Factor Graphs often used in pattern recognition, computer vision and coding theory. Factor graphs allow to represent a general global functions as a decomposition of local functions and they are used to perform both optimization and inference. Due to their general formulation factor graphs can be used to solve a wide range of problems, nonetheless their design and resolution are not easy tasks. My thesis aims at facing the challenges provided by these models, focusing on novel design methodology and resolution algorithms in the context of pattern recognition and bioinformatics.
  - **Student:** Pietro Lovato
    - **Year:** 3rd
    - **Date, Time, Location:** 27/10/2014, 10:30, sala verde
    - **Title:** Bag of words approaches for bioinformatics
    - **Abstract:** In recent years, several Pattern Recognition and Computer Vision problems have been successfully faced by techniques based on the "bag of words" representation - a representation which characterizes an object with a vector of counts of basic elements constituting the object. Even if largely applied to several scientific fields (with increasingly sophisticated approaches such as topic models), techniques based on this representation have not been completely exploited in Bioinformatics, due to the methodological and applicative challenges derived from the peculiar scenario. Nevertheless, in this context the bag of words paradigm is ubiquitous: many tasks can be described as counting basic repeating elements, and highly interpretable solutions (a stringent need in nowadays bioinformatics research) can be effectively derived. The aim of the talk is to illustrate the problems related to the creation of bag of words models and representations for some specific bioinformatics problems, such as the microarray expression analysis, the classification of proteins sequences, or the analysis of self-immune diseases. In each case, the suitability of the bag of words representation will be highlighted, and possible solutions - developed during the three years of my PhD studentship - will be presented.

- **Marco Cristani**
  - **Student:** Giorgio Roffo
    - **Year:** 1st
    - **Date, Time, Location:** 6/11, 11.30am, Sala riunioni, floor 2,
    - **Title:** statistical analysis of text chats: a novel challenge for social media
    - **Abstract:** No other technology penetrated our everyday life as quickly and ubiquitously as social media. Billions of users are using these programs every day, exploiting novel communication means. Among these, "instant messaging" is one of the most pervasive. The peculiarity of an exchange of instant messages is that it shows aspects of literary text and spoken conversation, in which textual information delivery follows turn-taking dynamics, resembling spoken interactions. This create a hybrid way of communicating, originating novel strategies for enriching the messages (the use of the emoticon as example). This thesis aims at studying text chats under a statistical point of view, inheriting what has been done with the automatic analysis of texts and with the modeling of spoken interactions, with the goal of producing novel strategies for capturing information about the conversations themselves but also about the users, from their style of communicating until some personality traits. The presentation will present this intriguing research challenge, showing preliminary results and discussing the research direction I would like to explore in the next years.

- **Alessandro Farinelli**
  - **Student:** Filippo Bistaffa
    - **Year:** 2nd
    - **Date, Time, Location:** Skype conference call
    - **Title:** Combinatorial optimisation problems in large-scale multi-agent systems
    - **Abstract:** Multi-agent systems represent a powerful approach to model and solve significant problems in several application scenarios such as intelligent energy management, transportation, logistics and sensor networks. In general, multi-agent systems are characterised by complex dynamics and interactions among a large number of agents, that usually translate into hard combinatorial problems, whose solution is very demanding from the computational point of view. Hence, the study of innovative techniques which can deal with such computational complexity is fundamental and would give a strong contribution to the research in this scenarios. My thesis focuses on the design of algorithms which tackle such hard problems, in order to solve realistic challenges in large-scale multi-agent scenarios, and on the study of highly parallel computational models (e.g., GPGPUs or many-core CPUs), that can fully exploit the high degree of parallelism of modern hardware architectures hence improving the solution process. In particular, my current research focuses on forming groups of agents for two practical scenarios, i.e., collective energy purchasing and social ridesharing. In these contexts, we provide novel models and techniques to compute optimal and approximate solutions with good quality guarantees for large-scale systems.

- **Paolo Fiorini**
  - **Student:** Francesco Visentin
    - **Year:** 2nd
    - **Date, Time, Location:** 6/11, 14:30, Aula Verde.
    - **Title:** A first step toward distributed sensing for soft robot
    - **Abstract:** Soft robots are a new trend in the robotic community. They are made by soft, deformable materials that enable them to easily conform to unstructured environment like biological systems do. In order to control this ability, sensors that return information about their spatial configuration and feedback from the environments are needed. Current solutions consist in the use of "classical" type of sensor that are (usually) bulky and thus limit the capabilities of the deformable material. A different type of sensors have to be developed in order to exploit all the features of the material used for the robot structure. In this presentation the first step toward the development of a novel type of sensor that enables sensing capabilities without limiting the deformation property of the soft material is presented. The sensor is based on a imaging technique known as Electrical Imaging Tomography.

- **Franco Fummi**
  - **Student:** Rosario Distefano
    - **Year:** 1st
    - **Date, Time, Location:** 4/11, 14.00, meeting room 2nd floor
    - **Title:** Modeling Biological Systems with Electronic Design Automation
    - **Abstract:** Model development and analysis of biological systems is recognized as a key requirement for integrating in-vitro and in-vivo experimental data. In-silico simulations of a biochemical model allows one to test different experimental conditions, helping in the discovery of the dynamics that regulate the system. Several characteristics and issues of biological system modeling are common to the electronics system modeling, such as concurrency, reactivity, abstraction levels, as well as state space explosion during verification. This thesis proposes a modeling and simulation framework for discrete event-based execution of biochemical systems through the use of EDA techniques. Moreover, the proposed framework uses techniques like property checking and mutation analysis in order to reach as much as possible a complete understanding of the biological system.

  - **Student:** Michele Lora
    - **Year:** 2nd
    - **Date, Time, Location:** 13/11, 11.00, Aula verde
    - **Title:** Making Homogeneous the Platform-Based Design of Heterogeneous Cyber-Physical Systems
    - **Abstract:** In the last few years the term Embedded System has been more and more replaced by the concept of Cyber-Physical System. This is due to the increasing attention given by the designers to the physical world interacting with the system. Considering the surrounding

environment as a further dimension in the design of computational devices lead to a whole new level of heterogeneity that has to be handle. At the current State of the art this heterogeneity is handled exploiting model based design, sacrificing the reuse of components, often necessary to target time-to-market and cost constraints. Alternatively, reuse is supported by co-simulation techniques, usually unable to assure a correct integration. A set of methodologies capable to form a design flow to model Cyber-Physical Systems, allowing reuse of previously designed components while assuring the system integration correctness is missing. Thus, it is a crucial target of the current research in this area. This problem is addressed by the proposed thesis, developing a framework to automatically integrate heterogeneous components into homogeneous and domain-independent models. Then, a set of methodologies is defined on these homogeneous models, to efficiently simulate, manipulate and synthesize Cyber-Physical Systems.

- **Vincenzo Manca**
  - **Student:** Vincenzo Bonnici
    - **Year:** 3rd
    - **Date, Time, Location:** 6/11 at 9:30 am in Sala Riunioni Secondo Piano
    - **Title:** Unconventional Genomes and Biological Network Analysis
    - **Abstract:** The research works of my Ph.D. thesis concern the informational and relational analysis of biological data. Informational analysis aims to provide a systematic approach to analyze genomic sequences. The studies extend an existing project, called InfoGenomics, where well-characterized dictionary-based genomic features are presented. Part of the new contribution is focused on genomic distributions, such as those regarding occurrence and recurrence of k-mers, in real and synthetic genomes. A natural development is the definition of algorithms able to localize regions where some distributional patterns occur, in order to yield informational genome annotation useful in the recognition of biological functions. Genomic functional elements and the other biological entities are linked together in biological networks to describe complex biological systems. Part of the new contribution regards the extraction and integration of biological entity relations from scientific sources. The subgraph isomorphism (SubGI) problem plays and important role in some network-based applications. Algorithms for its efficient resolution on biological data are presented. They include a new SubGI algorithm for the one-to-one case, winner at the ICPR Biograph2014 contest, and its parallelization, as well as the parallelized version of a methodology for searching in databases of graphs.

- **Andrea Masini**
  - **Student:** Matteo Pascucci
    - **Year:** 2nd
    - **Date, Time, Location:** 26/9
    - **Title:** Modal logics with propositional constants
    - **Abstract:** Propositional constants are propositional symbols whose interpretation is somehow fixed and their use in modal logic dates back at least to the Fifties. In some temporal logics a particular category of propositional constants, called nominals or clock-propositions, are used to "name" within the syntax the instants of a structure. My current work aims to investigate the semantics and proof theory of some of these logics. In the first part I will discuss the idea that the range of interpretations for a system whose language includes propositional constants can be defined in an accurate way in terms of general frames. The second part concerns the proposal of a deductive system for a language without any operator of realization and the third part illustrates how propositional constants can be used to obtain results of interdefinability among modal notions.

- **Gloria Menegaz**
  - **Student:** Mauro Zucchelli
    - **Year:** 2nd
    - **Date, Time, Location:** 5/11, 13:30, aula G.
    - **Title:** Towards Brain Tissue Microstructure Characterization using Diffusion MRI
    - **Abstract:** Diffusion Magnetic Resonance Imaging (dMRI) quantifies the diffusion of the water molecules in biological tissues. From the diffusion signal it is possible to calculate the corresponding ensemble average propagator (EAP), representing the ensemble average probability density function of the population of water molecules in the physical space. Nowadays different reconstruction techniques are used to model the diffusion signal starting from complex acquisition schemes in Fourier space in order to reconstruct the propagator. Numerous metrics can be then derived from the EAP in order to extract information about brain tissues

characterization, white matter fibers orientation and fibre density. The overall goal of this thesis is to improve the state-of-the-art (SOA) by facing the following issues: identification of the optimal sampling in the q-space; identification of the optimal basis for signal reconstruction; definition of new scalar indices (features) that are anatomically and biophysically plausible besides being objectively measurable in a robust, accurate and stable manner (numerical biomarkers). This will open new perspectives in both the scientific and clinical framework for the assessment of structural properties of tissues in both healthy subjects and patients besides supporting and improving cortical connectivity models.

- **Graziano Pravadelli**
  - **Student:** Tara Ghasempouri
    - **Year:** 2nd
    - **Date, Time, Location:** 12/11, 11, meeting room, second floor CV2
    - **Title:** Improving ABV by automatic generation and abstraction of PSL assertions
    - **Abstract:** Assertion-based Verification (ABV) aims at providing verification engineers with a way to formally capture the intended specifications, through the definition of logic assertions, and to formally check their compliance with the actual implementation of the intended design. Due to the huge effort required for the definition of such assertions, relevant research directions are guided by the need of simplify both assertion definition and their reuse throughout the embedded system design flow. In this context, several approaches exist in the literature for the automatic extraction of formal assertions. Some of them, rely on static analysis of the source code, other dynamically mine specifications by analyzing simulation traces. In both cases, most of them work on techniques which are suited only for gate level or RTL HW models, or SW protocols. Moreover, they suffer of scalability problems which prevent their wide adoption for large designs. This thesis proposes a dynamic specification mining methodology that works independently from the considered abstraction level (i.e., gate-level, RTL and system level HW descriptions, as well as, embedded SW). The proposed approach aims to obtain a simple, but high-quality set of assertions and to optimize the overall execution time in comparison with existing methodologies. A technique is also described to rank the interestingness of extracted assertions and prune those that appear to be irrelevant. On the other hand, the recent works on system-level design and transaction level modeling (TLM) face with new challenges for reusing existing RTL IPs and their verification environment in TLM-based design flows. While techniques and tools to abstract RTL IPs into TLM models have begun to appear, the problem of reusing, at TLM, an assertion-based verification environment originally developed for an RTL IPs is still under explored. Some works propose techniques and frameworks to deal with ABV at TLM, with a top-down flow. But, the reuse of existing assertions in an RTL to TLM bottom-up design flow has not been analyzed yet. To fill in the gap, a new methodology is proposed in this thesis to reuse assertions originally defined for a given RTL IP, to verify the corresponding TLM model.

- **Fausto Spoto**
  - **Student:** Gabriele Tosadori
    - **Year:** 1st
    - **Date, Time, Location:** 4/11, 11.30, ground floor meeting room
    - **Title:** Biological network analysis: from topological indexes to biological applications
    - **Abstract:** I will describe a Systems Biology approach that involves the topological analysis of biological networks by using some metrics called centralities. I will give some basic about graphs, that are the mathematical model used for this kind of study and then i will explain what i am going to do in order to understand how the known topological indexes (e.g. Closeness, Degree, Betweenness) could be useful in investigating the properties of a network and its nodes.

  - **Student:** Alberto Lovato
    - **Year:** 1st
    - **Date, Time, Location:** November 12, 9:30, lecture hall H, CV2
    - **Title:** Fact Semantics and Verification of Java's Concurrency Annotations
    - **Abstract:** Concurrency is an integral part of any computing system. It is used to increase performance of programs, when multiple threads of execution happen at the same time. Concurrency bugs are not easily detected, and so it is desirable to have automatic software to verify multithreaded correctness. There already exist tools for concurrent software verification, but they are still in their infancy and typically unsound or applicable to very restrictive classes of software (no heap management). I propose the use of code annotations for documentation as well

as verification of concurrency properties of Java programs. I will start with new precise definitions of existing annotations, introduced informally with the 2006 book "Java Concurrency in Practice": @Immutable, @ThreadSafe, @NotThreadSafe and @GuardedBy. They were proposed for simple documentation, and adopted sparingly in software projects, among which the open source ones Google Guava, Bitcoinj, Parfait. Existing tools verifying these annotations are incomplete, or just incorrect, and so my work should include the development of verification procedures for related properties (e.g., immutability). My proposal is to combine user-provided annotations and verification procedures to help producing well-documented and verified concurrent software.

- **Luca Viganò**
  - **Student:** Matteo Zavatteri
    - **Year:** 1st
    - **Date, Time, Location:** 29/10, room 1.75 CV2
    - **Title:** Enforcing Security Policies While Executing Workflows
    - **Abstract:** Business Processes handled by Web Applications are more and more widespread. A web application is an application written in some programming language which supports current web standards and related protocols, whereas a business process consists of a set of tasks to be executed, in some order, to achieve some business goal(s). This work aims at enforcing security policies while the workflow (that is, the technological part in charge of executing the business process) is being executed. Abstracting from the specific security measures, we cannot forget to say that, in general, security goes against the usability of a system. Therefore, the first requisite to be dealt with is the flexibility of the security methods we are going to use. Moreover, time is an intrinsic aspect of each business reality and it is often neglected, or managed with ad-hoc solutions, technologically speaking. For these reason I propose to build a framework which allows to formalise a two level transition system in which one part is in charge of handling the access control part (by relying on role-based access control models and their temporal extensions), whereas the other is in charge of handling the workflow part respecting temporal constraints (relying on structured workflow modelling languages). Once this framework is ready, it will be possible to investigate how to: (i) formalise users' authentication and authorisation in web contexts, (ii) set up temporal delegations and study interesting properties such as transitivity, (iii) validate the system with model checking techniques in order to find attack traces (that is, a sequence of transitions which lead the system to a state in which some security properties do not hold anymore. Finally, as a concretisation of the scientific contributions, I propose to use TRBAC as the access control model, and TNest as the workflow control model, to build a proof of concept.

  - **Student:** Michele Peroli
    - **Year:** 3rd
    - **Date, Time, Location:** 30/10
    - **Title:** A Model-Based Testing Approach for Web Applications
    - **Abstract:** Penetration testing is the most common approach for testing the security of web applications, but model-based testing has been steadily maturing into a viable alternative/complementary approach. Penetration testing is very efficient but the experience of the security analyst is crucial; model-based testing relies on formal methods but the security analyst has to first create a suitable model of the application under test. In my thesis, I propose a formal and flexible model-based security testing framework that contributes to filling the gap between these two security testing approaches. This is possible through the use of a database of actions and their low-level definition that ties concrete actions, performed through a web browser, to high-level actions present in the model.

  - **Student:** Alberto Calvi
    - **Year:** 4th
    - **Date, Time, Location:** 27/10/2014, 10:30, sala verde
    - **Title:** Model-Based Security Testing: Automated Generation of Vulnerability-driven Test Cases
    - **Abstract:** When it comes to security testing, the skills and experience the tester has acquired during his activity are the key factors that will determine the accuracy and efficiency of the testing process. Model-Based Testing (MBT) is a research field that has been growing and developing for years and it has been lately applied also to test the security of web services. MBT consists in exploiting a formal model of the System Under Test (SUT) and model-checking tools to cast the test generation problem as a model-checking problem. This reduction allows for the

generation of a set of Abstract Test Cases (ATC). The objective of my Ph.D. thesis is the definition and implementation of formal techniques to test the security of web applications and communication protocols. To achieve this goal I have developed and applied Mutation Testing techniques, assuming the presence of a secure model of the SUT, to generate ATC that, after a concretization step, can be executed on the SUT's implementation. I have also designed and developed a more general MBT approach based on the idea of Chained Attacks, a sequence of exploits allowing an intruder to attack the security of a web application, and the formalization of the web intruder. This new MBT approach also provide means for the semi-automatic generation of a SUT's model that is usually a task preventing the application of MBT techniques in the industrial field.

- **Student:** Marco Rocchetto
  - **Year:** 4th
  - **Date, Time, Location:** 27/10/2014,
  - **Title:** Automated reasoning for the verification of security protocols and web applications
  - **Abstract:** Interpolation has been successfully applied in formal methods for model checking and test-case generation for sequential programs. Security protocols, however, exhibit such idiosyncrasies that make them unsuitable to the direct application of interpolation. I address this problem and present an interpolation-based method for security protocol verification. My method starts from a protocol specification and combines Craig interpolation, symbolic execution and the standard Dolev-Yao intruder model to search for possible attacks on the protocol. Interpolants are generated as a response to search failure in order to prune possible useless traces and speed up the exploration. I illustrate my method by means of concrete examples and discuss the results obtained by using a prototype implementation.