Denominazione dell'insegnamento	**Numero di ore totali sull'intero ciclo**	**Distribuzione durante il ciclo di dottorato**	**Descrizione del corso**
Mathematical Optimization for Machine Learning	8	*primo anno*	*The course is aimed at providing basic Numerical Optimization tools to handle some classes of Machine Learning problems, particularly focusing on supervised classification. Optimality conditions for functions of several variables both in the constrained and the unconstrained case will be briefly recalled, along with some fundamental notions in convex analysis. The problem of separating sets in n-dimensional spaces by appropriate separation surfaces will be put in the form of an optimization problem. The Support Vector Machine (SVM) approach, where separating hyperplanes are adopted for classification purposes, will be discussed, together with possible alternative separation methods based on piecewise affine, ellipsoidal, and spherical surfaces. Multiple-Instance classification models will be discussed as well, together with the results of some applications.*
Advanced Cyber Security	8	*primo anno*	*The course aims at discussing the main methodological aspects of cybersecurity and at giving an overview of research issues that have recently received huge attention. By taking the course, the students will acquire knowledge about how security scenarios should be appropriately described and analyzed, and about interesting related research issues. The course topics are as follows. Motivations of attacks and attack vectors. Security policies. Security objectives: confidentiality, integrity, availability, authenticity, accountability. Threat models. Reference user models: network users, snooping users, co-located users. Security mechanisms. Main kinds of mechanisms: authentication, authorization, audit. Classes of attacks: eavesdropping, modification, interruption, forging. Typical issues with the design of security policies, threat models, and security mechanisms. Design principles and design rules. Security architectures. Artificial intelligence techniques for cybersecurity. Intellectual property protection, fraud detection in reviewing systems, adversarial defense of enterprise systems. Data management techniques for cybersecurity. Activity detection.*
Advanced Edge-Cloud computing systems	8	*primo anno*	*The applications used today for processing Big Data repositories are highly centralized and leverage cloud platforms to perform all major operations involving data collection, storing, processing, analysis and machine learning. However, using only the cloud can results in serious inefficiencies in terms of network traffic, latency times and optimization of energy consumption. In the latest years researchers and IT companies have proposed the adoption of the edge computing paradigm for processing data closer to where they are generated, for achieving low latency, privacy preserving and scalability. These benefits can be complemented by those provided by the cloud, which allows for aggregating large amounts of data persistently and perform compute-intensive analysis using a large amount of computing resources. This scenario defines the so-called edge-cloud compute continuum. In this course we will introduce the basic concepts of edge-cloud compute continuum and describe models, architectures, and frameworks based on this paradigm. Applications of cloud-edge computing systems in the area of Big Data analysis and machine learning will be also presented and discussed.*
Digital technologies and artificial intelligence law	8	*primo anno*	*The course focuses on the main legal aspects of digital technologies and AI. The first part of the course (modules 1-2) is dedicated to general aspects, relating to the development of a legal notion of cyberspace and the analysis of different regulatory approaches. Subsequently, having acknowledged the disciplinary inadequacy of formal legislation, the issue of non-regulatory based regulatory systems is addressed. In this sense, the need for an "interdisciplinary" approach is recognized that can lead to the definition of legal rules "modeled on the nature of things" to be regulated. Specifically, the disciplinary potential of design is analyzed, i.e. the suitability of design standards in regulating digital phenomena in a much more incisive way than the laws in a formal sense. From the examination of the advantages and criticalities of such an approach - especially with regard to the respect for fundamental rights and freedoms – we come to envisage a new model of regulation, based on the interaction between legal and technical factors, the result of which is to to arrive at the creation of a so-called norm "techno- juridical" which derives its binding character, in the light of the principle of horizontal subsidiarity. The second part of the course (modules 3-4) addresses the problem of the so-called cybersecurity, wrt both digital activities and more specifically artificial intelligence. We come to the definition - also in the light of the main European regulatory interventions - of a "proceduralized" and "multiphase" security model, based on the subsidiary interaction between legal, technical and organizational-managerial factors. Subsequently, the issue of responsibility deriving from the production and management of artificial intelligence systems is dealt with, both in terms of existing legislation and in terms of European regulatory proposals.*

			Module 5 will address some sectoral issues (e.g. copyright; personal data; smart contracts, predictive justice).
Aproximate Computing & digital systems	8	*primo anno*	*The design optimization of digital circuits and systems typically consists in a three-dimensional trade-off among energy dissipation, area occupancy and computational speed. In the last decade, breaking such a trade-off has become very challenging since the breakdown of Dennard's scaling, and as Moore's and Koomey's laws approaching their end. Therefore, newer devices, architectures, and design techniques have become extremely urgent, also due to the strict energy, speed and area- efficiency requirements dictated by the emerging Internet-of-Things applications. Approximate Computing (AC) is a recent design paradigm aiming to fill the gap between requirements and capabilities of current platforms. It consists in introducing a new dimension in the optimization space, accuracy, to significantly reduce the hardware complexity, energy consumption and computational time. AC can be applied in several application areas that are intrinsically resilient to computational errors, e.g., machine learning, sensor signal processing, data mining and multimedia. The degree of accuracy can span across all the vertical computing stack, starting from the algorithm level and going down to the circuit and device levels. Preferably, a cross layer interaction should be enabled to optimize the energy-area-speed-accuracy trade-off. In this course, we will describe the most recent techniques based on AC, focusing in particular on arithmetic circuits at transistor and logic level and on memory architectures. Moreover, we will present a general overview about how approximation can be leveraged at software and device levels. Finally, we will discuss about several application examples and computing platforms where AC can be applied, thus underlining the interdisciplinarity of such a design paradigm.*
A Primer on Resilient Control Methodologies for Cyber-Physical Systems	8	*primo anno*	*Recent progress on high-speed networks, wireless communication technologies and the development of novel control strategies for embedded systems gave rise to a boost in the deployment of the cyber-physical systems (CPS) paradigm within a wide range of applications.The heterogeneous nature of CPS components may give intruders the chance of launching severe attacks.Therefore, control solutions capable of ensuring CPS safety and performance under cyber-attacks are extremely important for security issues.How to keep system operations at a satisfactory level in the presence of attacks still remains an open challenge.The assumption is that the intruder is removed from the system architecture once detected.On the other hand, in most of the operating scenarios the plant must operate even if the attack is running:this poses the key question to develop a joint design for the detector and the controller in order to maintain suitable plant performance.According to these premises, the so-called resilient control problem for constrained cyber-physical systems subject to false data injections is addressed.The core of the proposed course consists in defining an ad-hoc versatile framework whose main feature consists in the ability of being geared to different classes of attacks.This is formally achieved by resorting to the receding horizon philosophy that is fully exploited for detection,countermeasures and control purposes. The set-theoretic model predictive arguments are combined with the perturbation analysis and sequential quadratic programming to reduce as much as possible the occurrence of refresh procedures on the communication network when resilient command actions are no longer available.One of its main merits consists in the dismissal of constructive assumptions existing in recent competitors.In this respect, the framework is then customized for replay and covert attacks by specifying actuation/detection phases and proving feasibility and closed-loop stability properties.*
Emerging networking paradigms for 5G/6G systems	8	*primo anno*	*Future telecommunication networks will definitely be the key enablers for emerging critical services such as autonomous driving, smart industry, AR/VR, and remote medicine, that require low latency and high reliability, along with massive connectivity and data availability. In view of this, they will have to evolve and overcome their current limits. This course aims precisely to present new network paradigms being defined for future 5G and 6G telecommunications systems. Advanced technological solutions will be presented that support the creation of: edge-device software platforms that are modular, open, and scalable, and able to meet the requirements of novel emerging services; open software frameworks for network data plane and control plane programmability; programmable access networks leveraging virtualization and flexible (re-configuration; and breakthrough algorithmic solutions for network resource orchestration. At the end of this course, students will be able to apply the theoretical knowledge acquired for solving problems related to the design, implementation, and management of 5G/6G network architectures based on the new virtualization paradigms in order to guarantee a more adequate response to user requests.*
Advanced Numerical Methods	8	*secondo anno*	*It is very well known that in practical engineering problems it is very difficult to find analytic solutions. Due to this reason, an increasing attention is devoted to numerical techniques allowing one to find approximations of the unknown desired solutions. As a result, all aspects of the floating-point arithmetic should be taken into consideration in order to provide efficient implementations of iterative algorithms. The course proposes some advance topics related to applications of numerical algorithms on computers. Deterministic and stochastic local, global, and multi-objective algorithms*

			and statistic tools will be presented and discussed. There will be taken into consideration implementations on traditional and new computers using numerical infinities and infinitesimals.
Advanced Machine Learning	8	*secondo anno*	*Machine Learning (ML) is used in different fields of engineering and is proving exceptionally useful for solving problems of extraordinary complexity that until a few years ago could only be addressed by human beings. The translation of texts from one language to another, autonomous driving, image analysis are just some of the problems that can be solved by Deep Learning (DL) models with performances comparable or superior to those of human operators. The topic of this course will be the presentation of two advanced Machine Learning models: Graph Neural Networks (GNNs) and Deep Reinforcement Learning (DRL). GNNs are DL models used when the input data does not have a sequential or matrix structure but can be modeled with a graph. The GNNs allow to associate to each node a data structure that summarizes its properties (embedding) and which is calculated by aggregating and processing the information of the node with that of the neighboring nodes that are at most a certain number of hops away from the node itself. This process can be performed with a message-passing mechanism which is very similar to how Convolutional Neural Networks (CNNs) extract features from images. The embeddings provide an easy way to do node-level, edge-level, and graph-level prediction tasks. GNNs are very powerful tools and are successfully applied in many different domains such as drug research, fraud detection, route planning and network optimization. DRL models combine the Reinforcement Learning (RL) paradigm with DL.RL requires an agent to operate in an environment by performing actions that change the state of the environment.The agent receives rewards and penalties and has the goal of maximizing his earnings.The agent's decisions are returned by a DL model that is trained to learn the most convenient actions. DRL models have achieved super-human performance; as an example, they excel in robotic tasks and can beat human players in competitive games (e.g., Atari, StarCraft, Dota, and Go).*
Large Language Models: from BERT to GPT with reinforcement learning	8	*secondo anno*	*Research in artificial intelligence for natural language processing (NLP) has a long timeline, spanning over 60 years and characterized by several milestones, peaking with the recent pre-trained deep contextualized language models based on Transformers. Such models have gained tremendous success, bringing significant performance boosts in a wide range of tasks and benchmarks in NLP. Also, the principles underlying Transformers and their deep-learning architectural traits are used in the current state-of-the-art of Computer Vision and Speech Processing. In this context, the proposed course aims to provide an analysis of the key concepts and neural architectures that characterize the Transformer-based language models, with particular emphasis on the BERT models and on the generative Transformers, namely the GPT and InstructGPT family, which include the very recent and revolutionary ChatGPT. The course also offers a glimpse into future perspectives and new opportunities of artificial intelligence for supporting various application fields, possibly of high societal impact, such as law and healthcare.*
Knowledge Organization and Representation	8	*secondo anno*	*This course aims to teach ways of formally representing knowledge using structured knowledge organization systems and, above all, ontologies, to enable the students to understand and effectively apply principles and techniques of representation and organization of knowledge currently used to index, classify and provide access to information resources.* *Lectures will be focused on both theory and methodology in the modelling of specialized domains, and in the use of representations for automatic classification and handling of information, and automated reasoning. During the course, emphasis will be placed on concepts and on the main features of ontologies, with appropriate attention to their application.*
Data Analysis & Signal Processing for Electrical Engineering Applications	8	*secondo anno*	*The course introduces some data analysis and signal processing tools electrical engineering applications which all rely on the least-squares theory.* *By starting with solving the linear regression problem with noisy data, the least-squares theory will be introduced and its relationship with the pseudo-inverse matrix illustrated.* *The pseudo-inverse approach will be then used to solve generic polynomial fitting, regression, and non-linear fitting through iterative algorithms.* *The basic principles of inverse theory and deconvolution will be suddenly introduced and then the course will focus on signal processing applications, all developed for dealing with optimal deconvolution and linear system characterization in noisy environment.* *Numerical exercises and experimental demonstrations will be done during the course.*
Networking Issues and Perspective for Future Generation of IoT systems	8	*secondo anno*	*The recent advances in micro-electronics and in the computational capabilities of micro-devices opened new perspective in the design of intelligent systems where small things can work together to perform also complex tasks. The new era of Internet of Things (IoT) is already arrived and new networks and protocols design issues are arising in this evolving context. The classical protocol stack and network design criteria need to be changed to meet new network and application requirements and novel issues and threats need to be considered. The following course will present the main difference existing between a classical TCP/IP network and the emerging IoT*

			technologies focusing on QoS issues and security threats that can be observed in these novel systems. Moreover, some references to novel application domains that can benefit by the IoT application will be illustrated to offer novel perspective in the IoT design and in the IoT market development.
Advanced methods to design hardware accelerators	8	*secondo anno*	*Modern applications, like Computer Vision (CV), Internet of Things (IoT), Deep Learning (DL) oriented to image classification, object detection and segmentation tasks, intelligent autonomous vehicles, smart manufacturing, and many others, demand high computational speed, significant energy efficiency and flexibility. For this reason, designing hardware accelerators currently receives a great deal of attention. This course overviews the main advanced methodologies to design both Application Specific Integrated Circuits (ASICs) and Field-Programmable-Gate-Array (FPGA)-based hardware accelerators suitable to support the above cited applications. In particular, design and algorithmic strategies exploitable to reduce the computational complexity of deep learning models without compromising the achievable accuracy are examined. Moreover, several design techniques oriented to edge computing systems are explored. The course also provides an overview on techniques currently used to efficiently implement CNN inference on low-power edge devices through data-level approximations, such as quantization and pruning. Some noteworthy state-of-the-art FPGA and ASIC implementations will be also presented. At the end of this course, students will have a comprehensive knowledge of the main design techniques applicable at circuit-, architecture- and system-level to hardware accelerate computationally intensive elaborations. They also will get an understating of methodologies and tools that can be used in several artificial intelligence applications also related to their research topics.*
Advanced Big Data	8	*terzo anno*	*The course provides an introduction to big data and their processing with MapReduce. First, foundations of big data and NoSQL databases are provided. Here, big data characteristics and real-life applications are described, along with NoSQL databases and the reference Cloud Computing computational framework. Then, the course focuses the attention on the MapReduce processing model and its application to several big-data-processing-related application scenarios, such as database management. Case studies and examples, as well as state-of-the-art systems and tools, are provided and discussed in details.*
Deep Generative Models	8	*terzo anno*	*The course is aimed at reviewing the foundational aspects as well the recent advances in generative probabilistic models, which learn distributions from data aimed at generating new data instances from the learned distribution. In recent years, these models have been parameterized using deep neural network and combined with advanced stochastic optimization methods. This has enabled their widespread and adoption to modeling of complex data (images, text, audio) in several application areas, including computer vision, speech and natural language processing, social media analytics.* *The course will focus on the mathematical foundations of generative modeling techniques. We will cover some key concepts from the recent literature, including variational auto-encoders, normalizing flows, generative adversarial networks, as well recent models based on neural differential equations and physics guided machine learning.*
Computational issues in game theory	8	*terzo anno*	*The course will touch several facets of modern computational game theory and its applications which include Strategic games, coalitional games, TU and NTU games, integer games, games over mathematical structures, pure and mixed Nash equilibria, cooperative solution concepts (vNM-solutions, core, bargaining set, kernel, Shapley value, nucleolus), fair allocation and fair division problems. Within the described formal context, focus will be on computational issues, namely, the complexity of reasoning with games and practical computation methods.*
Sensor-based Wearable Computing Systems	8	*terzo anno*	*Wearable computing is a relatively new area of research and development that aims at supporting people in different application domains: health-care (monitoring assisted livings), fitness (monitoring athletes), social interactions (enabling multi-user activity recognition, e.g. handshake), videogames (enabling joystick-less interactions), factory (monitoring employees in their activity), etc. Wearable computing systems (WCS) are based on tiny sensorized computing devices (e.g. to measure heart rate, temperature, blood oxygen, etc), common wearable accessories (e.g. watch, belt, etc) augmented with , and even smart clothes. Wearable computing has been recently boosted by the introduction of body sensor networks (BSNs), i.e. networks of wireless wearable sensor nodes coordinated by more capable coordinators (smartphones, tablets, PCs).* *In this course, we will introduce programming approaches and methods to develop (i.e. model, implement and deploy) efficient WCS systems/applications. From a practical viewpoint, the course introduces TinyOS/nesC- based programming of Shimmer wearable sensors to collect and transmit bio-signals (e.g. ECG and body motion) and provide students with hardware/software tools for the development of simple full-fledged wearable computing systems. The main research outcomes of the open-source SPINE Body-of-Knowledge (SPINE-BoK https://spine-bok.dimes.unical.it/) will be also briefly overviewed.*

Advanced Measurement and Data Acquisition Systems	8	*terzo anno*	*The course, held substantially in presence in the laboratory-classroom, aims to provide students the basic skills to learn using modern instrumentation for data acquisition by programmable and reconfigurable virtual systems, ac-cording to user requirements for different applications. Methods to process and analyse statistically large data sets, and transmit and save them, will also be discussed.* *The course includes, in addition to the traditional classroom lectures, tutorials and project workshops (not manda-tory) where students will study in deep specific topics, addressing different issues.* *The main contents are:* *- Introduction to measurement instrumentation. The analog-to-digital conversion; resolution and accuracy limits for numeric values; effective number of bits of the A/D converter. Description of the Data AcQuisition systems (DAQ) performances and limits; acquisition channels and generation of control signals.* *- Virtual instrumentation. The measuring instruments available on the market. The LabVIEW graphical environment. The front panel. The block diagram. Control palette and function palette, constants, indicators and controls. How to display data. Nodes and lines. Loop structures, case, sequence. Array and cluster. SubVI. Logic functions. Development of example programs. Debugging. Waveform Data. File management. Storing and recalling data in-to/from a file.* *- Elements of hardware and software. Data acquisition cards. Specifications. Acquisitions with buffering. Practical examples and their implementation.* *- Design and implementation of Virtual Instruments (VIs). Development of some practical applications.* *- Instrumentation programming. Communication interfaces (USB, GPIB). The driver for stand-alone instrumentation: SCPI, VISA. Communication with oscilloscopes and function generators via various communication interfaces.*
Microwaves for Sensing: Circuits and Methods for Biomedical Data Analysis	8	*terzo anno*	*The course is devoted to illustrate the basic principles of sensing procedures adopting microwaves and millimeter-waves. In the first part, the sensors/circuits architectures to be adopted for sensing applications are studied, while in the second part a set of super-resolution signal processing techniques are illustrated, which are able to estimate relevant biomedical parameters from a limited set of data acquired with microwave sensors. In particular, a spectral estimation approach with a specific statistical analysis is presented to guarantee the accurate identification of the biomedical parameter of interest, with high robustness against noise. Numerical applications on selected biomedical contexts will be considered.*
Modelling, Simulation and AI in advanced Separation Processes	8	*terzo anno*	*Accurate and reliable mathematical models play a key role in membrane system design. Process simulators have been proven to be successful in modelling, simulate, and optimize various industrial processes. Most of the commercial simulators can be used to solve mathematical models based on membrane applications. The present course is discussing the various advanced process simulators with relevance to the membrane-based processes and system design. The benefits of these tools, for rigorous modelling, simulation, and optimization, will be discussed. State-of-the-art simulation for, membrane filtration, membrane reactors, and membrane-based gas separations with a special focus on new incorporation of AI will also be discussed. Innovation and approaches based on ML and AI will not only help developing commercially feasible applications, along with challenges and prospects but also in a more sustainable way. At the end detailed the role of simulators in the process synthesis-intensification framework to develop sustainable membrane-based processes with case studies will be presented. In this course, following topics will be covered:* *1. Basic membrane process and structure* *2. Simulation, Modelling, and their advantage on Chemical Processes* *3. Membrane application focusing on liquid separation* *4. ML-AI in advanced separation process industries*