Faculty of Engineering and Architecture
Master's Degree Program in Computer Engineering, Cybersecurity and Artificial Intelligence

DEGREE PROGRAM REGULATIONS OF THE MASTER'S DEGREE

COMPUTER ENGINEERING, CYBERSECURITY AND ARTIFICIAL INTELLIGENCE (CLASS LM-32)

A.Y. 2025/26

SUMMARY

GENERAL DATA

Name of the Course of Study Studio	Computer Engineering, Cybersecurity and Artificial Intelligence
Class of belonging	Class LM-32: Class of Master's Degrees of Computer Engineering
Duration	The normal duration of the Master's Degree Course is 2 academic years and the number of credits necessary to obtain the qualification is 120.
Reference Structure	Facoltà di Ingegneria e Architettura
Reference Department	Dipartimento di Ingegneria Elettrica ed Elettronica (DIEE)
Teaching venue	Via Marengo n° 2 – Cagliari
Coordinator	Prof. Giorgio Giacinto
Web site	https://web.unica.it/cyberai
Language of teaching delivery	English
Teaching delivery methods	conventional (in person)
Access	free
Places reserved for non-EU students	40

Further general information on the Course of Study is provided on the website.

Art. 1 - Premises and purposes

These Regulations of the Master's Degree Course in Computer Engineering, Cybersecurity and Artificial Intelligence (class LM-32) are approved by the Council of the Degree Program in accordance with the Teaching Statute, respecting the freedom of teaching and respecting the rights and duties of lecturers and students, based on the Ministerial Decree. 270/2004 and subsequent amendments and additions, to the Statute, the University Teaching Regulations and the Student Academic Career Regulations and to Law 264/1999 relating to access planning.

Art. 2 - Bodies of the Degree Program

The bodies of the Degree Program, with a detailed description of functions, duties, and responsibilities, are defined in the document "The Quality Assurance System of the Degree Program," available on the course's website, in Italian.
The Council of the Degree Program may identify additional Committees tasked with analyzing and handling activities related to specific functions of the Council of the Degree Program.

Art. 3 - Specific Learning Objectives of the Degree Program and Description of the Program Structure

The computer, in its various forms, has become an essential component in different areas of social, economic, and productive life of the country, enabling accelerated development combined with greater efficiency and effectiveness thanks to the Internet connection and the ability to process large amounts of data through artificial intelligence techniques. Along with these development opportunities comes an increasing vulnerability of systems to cyberattacks aimed at compromising data confidentiality, integrity, and service continuity. Therefore, there is a growing need for professionals capable of designing and managing advanced computer systems in complex civil and industrial environments, mitigating the risks arising from potential cyberattacks.

The structure of the Master's Degree Program in Computer Engineering, Cybersecurity, and Artificial Intelligence aims to train highly specialized engineers in the design, management, and maintenance of complex and secure computer systems in industrial settings. These engineers will possess advanced skills in the fields of cybersecurity and artificial intelligence and will be capable of analyzing and proposing innovative and effective design solutions in these areas.

To achieve this goal, the specific learning objectives can be outlined according to four educational axes, identified in the areas of computer engineering, systems engineering, security science, and artificial intelligence. The overall aim is to combine a solid education in the fundamental domains of computer engineering and systems engineering with specialized training in the topics of cybersecurity and artificial intelligence.

The graduate of the Master's Degree in Computer Engineering, Cybersecurity, and Artificial Intelligence in relationship to the field of Computer Engineering:

- Has an in-depth knowledge of software development methodologies and is capable of designing, planning, developing, and managing complex and/or innovative software systems in various application contexts.
- Understands and can effectively utilize computing architectures and communication methodologies typical of industrial settings, embedded systems, distributed environments (cloud and mobile computing), and the Internet of Things.

These objectives are achieved through courses in the core area of computer engineering and related fields such as electronics and telecommunications.

In the field of Systems Engineering:

- Is knowledgeable about the methodologies and technologies for modeling, analyzing, and designing supervision and control systems, particularly those developed in industrial settings and for critical infrastructure, considering "cyber" security aspects.

These objectives are achieved through courses in the core area of automation and related fields of industrial and information engineering, aimed at providing knowledge of at least one specific application area.

In the field of Security Science:

- Understands methodologies for analyzing vulnerabilities and risks to which a computer system is exposed, as well as technologies and methodologies for their mitigation.
- Is capable of designing and devising computer systems with reduced "cyber" risk in relation to the application context, detecting and managing computer incidents in operating systems, assessing their legal and economic implications.

These objectives are achieved through courses in the core area of computer engineering and the related field of legal informatics.

In the field of Artificial Intelligence:

- Understands the underlying approaches of algorithms used for machine learning and artificial intelligence and is capable of using them to devise and design systems whose operational functionalities depend on intelligent data processing.
- Is capable of utilizing knowledge in the field of artificial intelligence to design physical and logical protection systems for the mitigation of "cyber" risk, also using cutting-edge enabling technologies (such as, for example, biometric technologies).

These objectives are achieved through courses in the core area of computer engineering.

Furthermore, the Master's degree graduate will also have acquired the skills necessary to access higher levels of education, such as doctoral programs, second-level Master’s degrees, and specialization schools focused on cybersecurity. This objective will be pursued through a combination of training activities, particularly through activities related to the final examination.

For many courses, project activities carried out in the laboratory are planned, aimed at developing and testing advanced solutions for problems of complexity comparable to those encountered in the real world.

The organization of prerequisites and the scheduling of courses in various periods will be based on the division of courses into the four reference areas, characterized by a significant degree of integration of educational content.

All courses will be taught in English, not only to promote internationalization and attractiveness to external parties but also to facilitate graduates' approach to lifelong learning through access to industry-specific information primarily available in English.

Art. 4 – Expected employment and professional activities for graduates

Role in a work context:

1. Designing, developing, managing, and testing computer systems in various sectors (manufacturing, public administrations, services) characterized by the acquisition, transmission, and processing of signals in civil, industrial, and information domains.
2. Designing, developing, and managing computer systems in all industrial sectors where 'security' and 'intelligence' are fundamental axes (for example, intelligent systems for logical and physical security).
3. Designing cyber intelligence and/or cyber security services.
4. Designing systems that utilize Artificial Intelligence and Machine Learning algorithms.
5. Supervisory and technical management activities in the aforementioned areas.
6. Fundamental, applied research, and industrial development. Support for Research and Development in companies. Support for technology transfer.

Skills associated with the role:

Ability to interact with the external world oriented towards understanding and negotiating the requirements of a secure computer system, connected to a specific application issue.

Capability to analyze and define the modules of a given computer system, identifying criticalities and implementation issues.

Skill in translating the results of the analysis of each module into detailed specifications concerning the realization (or integration) or further organization of the software systems and/or specific components of the overall system, with particular reference to securing each of them with state-of-the-art technological solutions.

Ability to specifically define the most appropriate implementation solutions, with regard to code writing, operational software modules created from scratch, integrating existing components, possibly modified or updated. (Skills 1,2,5).

Capability to identify technical solutions suitable for the characteristics of the computer system (hardware and software), organizational and managerial aspects for project realization, technological constraints, required performance, and especially related to its protection from various types of cyber-attacks. (Skills 1,2,5).

Advanced skills in the field of cyber-security in computer systems, and the realization and implementation of tools for risk mitigation. (Skills 2, 3).

Advanced skills in the fields of artificial intelligence and machine learning. (Skills 4,6).

Advanced skills for managing computer risk and designing secure computer systems also through the use of artificial intelligence methodologies. (Skills 3,4,6).

Career prospects:

Public and private organizations involved in the management and implementation of critical infrastructures, where security management is crucial.

Companies operating in the field of information systems and computer networks, with particular emphasis on those in the physical and logical security market realized through computer systems.

Industries operating in the hardware and software production sectors.

Companies operating in the fields of multimedia services, e-commerce, and internet services.

IT services for public administration and healthcare.

Industries for automation and robotics.

Companies operating in the transportation and logistics sectors.

Civil and industrial entities where automation apparatus and systems integrating computer components, measurement devices, transmission, and actuation systems are present.

Universities or research centers involved in the aforementioned application areas.

The broad and non-focused training on Sardinian industrial realities allows graduates to apply to companies or institutions located outside of Sardinia and Italy. The extensive basic training also allows for managerial roles of significant responsibility as the career progresses.

As with all second-level engineering degrees, there is the possibility of practicing the liberal profession as an "Engineer" after passing a State examination and registering with the professional association.

Art. 5 - Types of educational activities

The Degree Program is based on educational activities of six types:

1. Core activities (Type B);
2. Related or integrative activities (Type C);
3. Elective activities chosen by the student (Type D);
4. Activities related to the preparation of the final exam (Type E);
5. Additional training activities (Type F: additional language skills, computer and telematic skills, activities related to internships and training, and other skills useful for entering the job market)

For elective training activities, students are guaranteed freedom of choice among all courses offered by the University, including the acquisition of additional training credits in core disciplines, provided that the choice is consistent with the educational project.

The coherence of the proposal with the educational project is evaluated and determined by the Degree Program. The student may request recognition, in terms of credits, within the elective training activities, of experiences gained outside university curricula: these include internships, seminars, additional language skills, activities related to the Erasmus program, etc.
To acquire the respective university training credits (ECTS), passing the exam or another form of assessment of performance is required.

Further details may be available on the Degree Programme website under the section 'Elective Activities'.
Notices concerning seminars, laboratories, or workshops that are relevant for the acquisition of type

F credits may be published under the 'Other Educational Activities' section of the Degree Programme website.

Students who have completed national civil service can request from the Council of the Degree Program the recognition of credits for the service performed. The Council, after evaluating the documents submitted by the student and the relevance between the activities carried out during civil service and the learning objectives of the Degree Program, can recognize the service performed for up to a maximum of 9 ECTS, to be allocated to the category of elective activities chosen by the student. It can also recognize additional credits, up to a maximum of 3, to be allocated to the category of "other activities".

The teaching methods adopted consist of frontal lectures and practical exercises. The educational activity is mainly organized on a semester basis. For part-time students or those simultaneously engaged in work activities, compatible with the available resources, appropriate organizational methods of educational activity may be arranged.

Art. 6 – Program Structure

Attachment 1 shows the program strcture, containing all the teaching activities foreseen by the Master's Degree Course, with the table reporting the expected learning outcomes expressed through the european Dublin Descriptors in relation to the individual training activities envisaged, as well as the reference faculty members and student mentors.

Art. 7 – Lecturers of the Degree Program

The list of lecturers of the Master's Degree Program in Computer Engineering, Cybersecurity, and Artificial Intelligence is available on the website of the Degree Program and in the Annual Faculty Course Bulletin.

Art. 8 - Admission Planning

Access to the Master's Degree Program in Computer Engineering, Cybersecurity, and Artificial Intelligence is open. Constraints are imposed by the curricular requirements and personal preparation required for admission. The sustainable intake indicated by the Ministry is 80 students.

Art. 9 - Requirements and Admission Procedures

To be admitted to the Master's Degree Program in Computer Engineering, Cybersecurity, and Artificial Intelligence, applicants must hold a bachelor's degree or another foreign qualification recognized as suitable. Enrollment in the course is also subject to meeting the curricular requirements and verifying the adequacy of the personal preparation as indicated in the following. Any necessary curricular integrations to meet the admission requirements can be acquired through enrollment in individual courses taught within the student's programs of study at the University of Cagliari.

Curricular Requirements

(a) Holding a bachelor's degree or a three-year university diploma, or another foreign qualification deemed suitable.
(b) Certification at level B2 regarding proficiency in the English language. This requirement effectively addresses the learning objectives of the class, which establish that "Graduates of the master's degree courses of the class must be able to use fluently, both in written and oral form, at least one language of the European Union in addition to Italian, also with reference to disciplinary lexicons." The presentation of the English language proficiency certification is not required if the bachelor's or three-year university diploma course, deemed suitable for admission, was mainly delivered in English.
(c) Having acquired at least 12 ECTS credits in the fields of MAT and FIS.
(d) Having acquired at least 36 university training credits in the fields of INF/01 and ING/INF, including at least 18 ECTS credits in the fields of INF/01 and ING-INF/05. A dedicated Committee, appointed by the Degree Program, is responsible for verifying the applicant's eligibility for enrollment concerning compliance with curricular requirements and personal preparation, especially in cases where these cannot be verified automatically, particularly in the case of a foreign-issued degree. The Committee, after analyzing the student's academic record, may identify a personalized program structure with a differentiation in core and related activities not exceeding 12 credits, in accordance with the Teaching Statute.

Adequacy of Personal Preparation

Following the verification of the possession of curricular requirements carried out in the manner indicated above, the adequacy of individual preparation will be determined by a Committee of the Degree Program through an examination in which knowledge of topics related to the scientific disciplinary areas for which minimum values of training credits are prescribed will be assessed.

- For mathematics: functions, differential and integral calculus in multiple variables, vectors and vector operations, matrices, systems of linear equations, eigenvalues, and eigenvectors;
- for physics: kinematics, dynamics, energy, work and power, electricity, electromagnetism;
- for computer science: programming languages and object-oriented programming, algorithms and data structures, computer architecture, databases, computer networks, operating systems.

The verification test will be conducted in accordance with the methods and times provided for by University and/or Faculty Regulations. The personal preparation of graduates who have obtained a technical-scientific bachelor's degree from the University of Cagliari or elsewhere, or obtained abroad provided it is recognized as suitable with a grade equal to or higher than 92/110 or equivalent, is considered adequate.

For non-EU students residing abroad who have not obtained a qualifying degree in Italy, the Committee may conduct an evaluation based on the submitted documentation. Specifically, the Committee will analyze the previous academic record by evaluating:

a) First-level Degree (or equivalent qualification) program:

- Type, class, and title of the degree
    - Composition of the credits required for admission, with reference to the subjects of the assessment test for the adequacy of personal preparation;

    - Possible need for a personalized program structure.
- Average grades obtained in individual courses and the student's ranking within their cohort (if available).
- National or international ranking of the university that awarded the degree

b) Knowledge of the English language

c) Evaluation of the overall activity and other qualifications ascertained from the curriculum and any additional documents submitted by the student.

If the submitted documentation is insufficient to determine the level of personal preparation, an interview, which can also be conducted telematically, may be arranged.
Students who are not yet graduates but wish to enroll conditionally according to the Student Academic Career Regulations document must meet the curricular requirements and adequacy of personal preparation at the time of obtaining their degree and thus the lifting of the reservation. All students intending to enroll in the Master's Degree in Computer Engineering, Cybersecurity, and Artificial Intelligence must submit an application for the personal preparation adequacy assessment test within the deadlines set by the General Manifesto of Studies. The Committee may exempt candidates who meet the above-mentioned personal preparation adequacy requirements from the test

Art. 10 - Enrollment in the Degree Program

All those who intend to enroll in the Master's Degree Course in Computer Engineering, Cybersecurity, and Artificial Intelligence must register for the test on adequacy of the personal preparation by submitting an online application at www.unica.it > Access > Esse3 – Students and Faculty, within the deadlines indicated by the General Manifesto of Studies.
Candidates must attach a self-certification of their degree with the exams passed during their academic career and, if requested by the Council of the Degree Program, the related syllabi. In the case of a degree obtained abroad, refer to specific ministerial circulars.
Since activities already recognized for the allocation of academic credits within the bachelor's degree courses cannot be recognized again as academic credits in the Master's Degree, the Course of Study, based on the exams passed in the bachelor's program, may define an individual study plan different from the official one that must be followed by the student to obtain the degree, in compliance with the Teaching Statute.

The operational procedures for online enrollment in the Course of Study can be found on the university's website, on the webpage "Enroll > Access to Master's Degree Courses" webpage.

Art. 11 - Enrollment in Subsequent Years, Transfers, and Transitions

A student enrolled in the Master's Degree in Computer Engineering, Cybersecurity, and Artificial Intelligence is considered enrolled in subsequent years, for the academic year of reference, upon payment of the first installment, as indicated in the Student Contribution Regulations, within the deadline and in compliance with the other modalities specified annually in the General Manifesto of Studies.

Transfers and Transition Procedures from Other Degree Programs

The transfers and transitions to the Master's Degree in Computer Engineering, Cybersecurity, and Artificial Intelligence are subject to the possession of curricular requirements and the verification of the personal preparation required for admission.
Students transferring from another Master's Degree Course or from another university who wish to be admitted to the Master's Degree in Computer Engineering, Cybersecurity, and Artificial Intelligence must submit a request for validation of the university exams already passed and recognition of the corresponding credits simultaneously with the enrollment application, attaching a self-certification of the completed educational activities and, if required by the Degree Program, the corresponding syllabi.
The Council of the Degree Program, after verifying the required admission criteria, will evaluate, also based on the syllabi, the possible equivalencies or partial correspondences with the subjects provided in the study plan and will validate the exams, recognizing the maximum number of credits possible based on the programs of the exams successfully passed. This evaluation may include interviews to verify the actual knowledge possessed, justifying any failure to recognize previously acquired credits. Specifically, in the case of transfers from Master's degree courses in the same class, and if conducted through accredited distance learning methods according to current regulations, at least 50% of the credits earned in each scientific-disciplinary sector will be recognized.
The year of the course to which the student is admitted will be determined by the Council of the Degree Program based on the validated disciplines and credits.

Art. 12 – Internships

The Degree Program in Computer Engineering, Cybersecurity, and Artificial Intelligence promotes and encourages training activities aimed at acquiring skills useful for entering the job market and facilitating professional choices through direct knowledge of the working sectors of Information Engineering. It supports the implementation of internships and training stages at companies, institutions, and public administrations. The management of these activities is carried out by the Faculty of Engineering and Architecture and, at the departmental level within the Department of Electrical and Electronic Engineering, through a special commission (CRLM - Commission for Relations with Labour Market), which includes representatives from all degree programs promoted by the department itself.
For this purpose, based on the proposal of a faculty member of the Degree Program who serves as the internal tutor, the Council defines specific training projects for each interested student, based on agreements with the host entities, in which an employee of the host entity acts as the external tutor. Internal internships may also be activated under the responsibility of a university faculty member. The corresponding credits are recognized by a resolution of the Council of the Degree Program, based on the documentation presented.
The activation, management, and monitoring of curricular internships are carried out through a specific CINECA application called TSP. On the 'Internship' page of the Degree Program's website, you can find operational guidelines, instructions, and procedures for starting the internships

Art. 13 – University Credits (ECTS)

The overall learning commitment of a full-time student in one year is conventionally set at 60 ECTS (CFU), with each credit corresponding to 25 hours of work. In the European Credit Transfer Systems 1 CFU equals 1 ECTS.
The portion of this commitment reserved for individual study or other individual training activities cannot be less than 50%. Each credit corresponds to no more than 10 hours of lectures or equivalent teaching activities, including exercises and equivalent assisted activities, with the remaining hours dedicated to individual study.
In the case of training activities with a high experimental or practical content, one credit corresponds to a minimum of 8 and a maximum of 16 hours of assisted activity in the classroom and/or laboratory, with the remaining hours up to the total 25 hours intended for study and personal elaboration, and/or individual practice in the laboratory and in the field.
Finally, for individual study activities, exclusively laboratory activities, and internships, each credit corresponds to 25 hours of the student's actual commitment.

Art. 14 - Prerequisites

There are no official prerequisites; however, students are required to follow the program structure, respecting the sequence of courses and their respective exams, as indicated in Attachment 1.

Art. 15 - Attendance Requirements

Attendance at training activities is generally mandatory. Verification of attendance will be carried out according to the methods and criteria established by the Council of the Degree Program. Students who submit a request with justified and documented reasons may be exempted from the attendance requirement for courses.

Art. 16 – Assessment of Academic Performance

The annual number of exam sessions and their distribution throughout the year are established in accordance with the University's and Faculty's Regulations.
Exams for the assessment of academic performance consist of a final test evaluating the student's knowledge of the course's official syllabus. This test may be oral, written, or a combination of both. The exam may include the discussion of papers, projects, and experiences conducted by the candidate under the direction of the professors, and may also consider any intermediate tests taken by the student during the semester.
The methods for verifying the learning objectives for each course are described on their respective pages, available through the Council of the Degree Program and Lecturer's website.
The final grade is expressed in thirtieths, and a minimum score of 18/30 is required to pass the exam. Passing an exam allows the student to earn the corresponding credits.
For integrated courses consisting of two or more teaching modules, the overall assessment cannot be divided into separate evaluations for the individual courses or modules. The final evaluation will be given jointly by the professors responsible for the courses. The related credits will therefore be awarded only after the comprehensive assessment of all modules, even if they are distributed over two semesters.
Examination committees are composed of at least two members, appointed according to the procedures outlined in the University Teaching Regulations document.

Art. 17 – Rules for submission of Individual Study Plans

Students may submit an individual study plan in accordance with DM 270/2004, as supplemented by DM 96/2023 and the University Teaching Regulations, which must be approved by the Council of the Degree Program, in compliance with the current Teaching Statute. The submission of individual study plans must take place by October 31, or by March 15 for students who regularize their enrollment by February 28, unless otherwise decided by the Council.
However, students are required to indicate the independently chosen educational activities as provided for in Art. 10, paragraph 5, letter a) of DM 270/04. For this purpose, students are assured the freedom to choose from all courses offered by the University, including the acquisition of additional educational credits in the core disciplines, provided that the choice is consistent with the educational project.

Art. 18 – National Mobility (Erasmus in Italy)

The Degree Program Council may allow participation in the Italian Erasmus, a project aimed at promoting student mobility among Italian universities, based on agreements established between the universities. The project is intended to support the development of innovative study programs that encourage interdisciplinarity and flexibility in educational offerings, strengthening integration and complementarity among the participating universities. The call for applications for national mobility will be available on the Degree Program website.

Art. 19 – International mobility

The Degree Program in Computer Engineering, Cybersecurity, and Artificial Intelligence promotes and encourages educational activities abroad. To this end, specific agreements are established with foreign universities offering courses in Computer Engineering or related fields. The program recognizes credits earned during periods of study abroad, subject to examination of the curricula of the courses taken and their consistency with the learning objectives of the Master's Degree program in Computer Engineering, Cybersecurity, and Artificial Intelligence.

Art. 20 - Recognition of ECTS for Extracurricular Activities

According to article 5, paragraph 7 of D.M. 270/04, the Council of the Degree Program may recognize academic credits derived from individually certified professional knowledge and skills in accordance with the current regulations, as well as other knowledge and skills acquired through second-level university training activities in which the university has participated in the design and implementation. The maximum number of recognizable university credits is 24; in all cases the total number of recognized ECTS, including those from both I and II level degree programs, cannot exceed 48. Recognition will be carried out solely based on the skills demonstrated by each student. Forms of collective recognition of credits are excluded.

Art. 21 - Guidance and Tutoring

The Study Program promotes the active and fruitful participation of students in university life and works to prevent dropouts and delays in studies through various guidance and tutoring services. Details of these services are available on the Degree Program's website, under the "Guidance" section.

Art. 22 – Final Exam

To be admitted to the final exam, students must have passed the exams of the courses and completed the other training activities provided for in their study plan, in accordance with the procedures established by these regulations, including those related to the preparation of the final exam, earning the corresponding credits.
The final exam consists of discussing a report (thesis) on an individual project carried out by the student under the supervision of at least one professor from the Faculty of Engineering and Architecture at the University of Cagliari, addressing technical and/or scientific aspects relevant to the field of information engineering, particularly information security or artificial intelligence.
The project may involve a critical analysis of the state of the art, the drafting of at least a preliminary design, the development of methodologies and techniques with a certain degree of originality, or the transfer of methodologies and techniques from different fields into the information engineering sector.
The thesis must be written in English.

The activities related to the preparation of the final exam may be carried out:

- at one of the research groups of the Department of Electrical and Electronic Engineering (DIEE) that provide teaching for the Degree Program;
- at a research group that collaborates with the groups mentioned in the previous point;
- abroad, within the framework of one of the various international programs offered by the university (Erasmus Plus, Erasmus Placement, Globus Placement, etc.) or as a Free Mover;
- at a company located regionally, nationally, or abroad, provided that this activity does not coincide with the activity performed during an internship for which specific academic credits have been awarded, unless these credits have been recognized only for a fraction of the total work performed.

The thesis is discussed before a committee consisting of 5 professors from the Degree Program, potentially supplemented by professors who teach in the Degree Programs of the Department of Electrical and Electronic Engineering and generally chaired by the coordinator. During the discussion, the student may use graphical and computer aids.
The presentation must cover the context of the work performed, an adequate overview of the problems addressed and the state of the art, a description of the materials and/or methods used, the results obtained, and the future prospects of the work. The presentation aims to verify the graduate's ability to communicate professionally and discuss the chosen topic clearly and competently. At the end of the presentation, a question session takes place with the committee members (thesis defense).
The committee evaluates the final exam by expressing a judgment which, together with the evaluation of the study program, contributes to determining the final grade, which will be with mark expressed out of 110.

Criteria for Awarding the Graduation Grade

The graduation grade is awarded based on the academic record, the thesis, and the discussion in front of the committee. The thesis is evaluated based on the completeness of the examination of the state of the art, the adequacy of the materials and methods used, the accuracy and

comprehensiveness of the results obtained, the depth of problem analysis, and the degree of innovation in the proposed solutions. The presentation is assessed based on the candidate's ability to translate the work into an effective, complete, and clear set of slides and their ability to respond competently and professionally to questions.

A student takes a number n of exams. To each i-th exam with i=1,…,n, a possibly different number of ECTS credits are associated. Then, the formula for the graduation grade is:

Graduation grade = thesis mark + $\frac{\sum_{i=1}^{n} (mark\ of\ exam_i) \times (CFU\ of\ exam_i)}{\sum_{i=1}^{n} (CFU\ of\ exam_i)} \times \frac{110}{30}$.

The thesis mark ranges from 0 to 9 points.
As a guideline for awarding the Thesis mark, the following classification of the type of work carried out by the student is used:

- Compilation Thesis: up to 4 points;
- Project Thesis: up to 6 points;
- Research Thesis: up to 9 points.

Honors can be awarded unanimously by the committee only if the sum of the Thesis mark and the exam average is equal to or greater than 112.

Art. 23 - Collection of student feedback

The Degree Program promotes the systematic collection of students' opinions regarding the courses, the degree program itself, the services offered, and the exams passed. The results are periodically monitored and analyzed with the aim of identifying and implementing actions aimed at the continuous improvement of the Degree Program. Anonymized analytical reports and summary tables of students' opinions are available on the University and Degree Program websites.

Art. 24 – Quality assurance

The Master's Degree Program in Computer Engineering, Cybersecurity, and Artificial Intelligence promotes a policy of planning and managing activities aimed at continuous improvement, in accordance with the regulations on Quality Assurance of the university educational processes and both national and international best practices. Documents related to the Quality Assurance System of the Degree Program are available on the "Quality and Improvement" page.

Art. 25 - Transparency – Methods of Information Transmission to Students

The Study Program website is the preferred tool for transmitting information to students. Through the website, the following can be accessed:

- regulations governing the operation of the Master's Degree Program;
- the Teaching Statute of the Master's Degree Program;
- the program structure of the Master's Degree Program;
- calendars and schedules of teaching activities;
- calendars and schedules of exam and graduation sessions;
- information about professors and courses.

Additionally, the websites of the Degree Program and the Faculty of Engineering and Architecture may publish:

- general information;

- announcements;
- forms;
- other useful information.

Art. 26 - Diploma supplement

In accordance with current regulations, the University issues, upon request, a certificate supplement to the Master's Degree in Computer Engineering, Cybersecurity, and Artificial Intelligence. This certificate provides, also in English and according to models consistent with those adopted by European countries, the main details related to the specific curriculum followed by the student to obtain the degree.

Art. 27 - Simultaneous Enrollment in Two Degree Programs

In accordance with Ministerial Decree No. 930 of July 29, 2022, implementing Law No. 33 of April 12, 2022, entitled "Provisions on simultaneous enrollment in two higher education courses", while maintaining the obligation to possess the necessary academic qualifications for access to different levels of university education, the possibility of simultaneously enrolling in two higher education courses within the same University or belonging to Universities, schools, or specialized higher education institutions, including foreign ones, is provided.
In the case of simultaneous enrollment in two degree programs, if the student has already earned academic credits in the first program, the Council of the Degree Program proceeds with the recognition of the completed educational activities; in the case of transferred educational activities, recognition is granted automatically.
In the event of partial recognition of completed educational activities in one degree program, the Council of the Degree Program facilitates the student's participation in additional educational activities to ensure full recognition of the completed educational activities.
Failure to recognize credits must be adequately justified.

Art. 28 - Final and Transitional Provisions

For matters not expressly stated in this regulation, reference is made to the current legislation.

Attachment 1 – Degree Programme

1st year

Sem	Course	SSD	TAF	ECTS	Hours
1	Industrial Software Development	ING-INF/05	B	7	70
1	Cybersecurity Technologies and Risk Management	ING-INF/05	B	8	80
1	Supervisory control and monitoring	ING-INF/04	B	9	90
	Integrated Course: Network and Web Security				
1	- Module: Network Security	ING-INF/03	C	4	40
2	- Module: Web security	ING-INF/05	B	5	50
	Integrated Course: Intelligent Systems				
1	- Module: Artificial Intelligence	ING-INF/05	B	6	60
2	- Module: Machine Learning	ING-INF/05	B	7	70
2	Computer Vision Technologies and Biometrics	ING-INF/05	B	6	60
2	Fault diagnosis and estimation in dynamical systems	ING-INF/04	B	5	50

2nd year

Sem	Course	SSD	TAF	ECTS	Hours
	Integrated Course: Embedded Systems				
1	- Module: Advanced Embedded Systems	ING-INF/01	C	8	80
1	- Module: Internet of Things and Digital Twins	ING-INF/03	C	6	60
	Integrated Course: Digital Forensics				
1	- Module: Digital Forensics Techniques	ING-INF/05	B	5	50
2	- Module: Digital Forensics Law	IUS/20	C	5	50
	One choice among:				
1	Machine Learning Security	ING-INF/05	B	5	50
2	Control, Learning and Security in Network Systems	ING-INF/04	B	5	50
2	Stochastic Models	ING-INF/04	B	5	50

Additional credits to acquire

Sem	Educational activity	SSD*	TAF*	ECTS	Hours
	1 course from table 1		C	6	
	Other activities		F	3	
	Elective activities[1]		D	10	
	Final Examination		E	15	

TOTAL CREDITS 120

(1) The selection of the corresponding credits must be consistent with the student's program structure and must have the binding approval of the Council of the Degree Program.

Table 1. List of courses of type C (1 choice among those proposed)

Sem	Course	SSD	TAF	ECTS	hours
	1st year				
2	Integrated Course: Smart Grid and Critical Infrastructures - Module: Industrial Informatics for energy storage systems	ING-IND/32	C	2	20
2	- Module: Critical infrastructures for innovative power distribution	ING-IND/33	C	2	20
2	- Module: Measurements and Cybersecurity for Smart Grid	ING-INF/07	C	2	20
2	Data driven models for system engineering	ING-IND/31	C	6	60
	2nd year				
1	Physical-layer techniques for Wireless communication security	ING-INF/02	C	6	60

The semester could change; check in Course bulletin of the academic year.

Abbreviations

SSD	Scientific Disciplinary Sector
TAF	Type of Educational Activity

Expected learning outcomes, expressed through the European Qualifications Framework descriptor

EUROPEAN DESCRIPTORS **Form compiled with reference to the Degree Program in Computer Engineering, Cybersecurity and Artificial Intelligence** **(classe LM-32)**	**EDUCATIONAL ACTIVITIES**																						
	Industrial Software Development	Supervisory control and monitoring	Cybersecurity Technologies and Risk Management	Fault diagnosis and estimation in dynamical systems	Computer Vision Technologies and Biometrics	Network and Web Security - CI - Network Security	Network and Web Security - CI - Web security	Intelligent Systems - CI- Artificial Intelligence	Intelligent Systems - CI- Machine Learning	Digital Forensics - CI - Digital Forensics Techniques	Digital Forensics - CI - Digital Forensics Law	Embedded Systems - CI- Advanced Embedded Systems	Embedded Systems - CI- Internet of Things and Digital Twins	Smart Grid and Critical Infrastructures - CI - Industrial Informatics for energy storage systems	Smart Grid and Critical Infrastructures - CI - Critical infrastructures for innovative power distribution	Smart Grid and Critical Infrastructures - CI - Measurements and Cybersecurity for Smart Grid	Data driven models for system engineering	Physical-layer techniques for Wireless communication security	Machine Learning Security	Control, Learning, and Security in Network Systems	Reverse Engineering and Malware Analysis	Stochastic Models	Final examination
A – Knowledge and Understanding																							
1) Know and understand software development methodologies in various business environments, particularly in distributed systems. Know and understand the fundamentals of methodologies for secure software development.	x		x	x		x	x					x	x						x			x
2) Know and understand computing architectures and communication methodologies characteristic of embedded systems and the Internet of Things.				x								x	x					x	x			x
3) Know and understand methodologies for the modeling of complex systems and the technologies for their governance, with particular reference to aspects related to cybersecurity.	x	x	x	x										x	x	x	x		x	x	x	x
4) Know and understand aspects related to the logical and physical security of networks and complex systems, IT technologies, and organizational and managerial methodologies for designing secure software and for risk mitigation and system analysis in the event of a breach.	x	x	x	x	x	x	x			x					x	x		x	x	x		x
5) Know and understand the economic and legal aspects related to cybersecurity.	x	x	x							x	x				x							x
6) Know and understand the approaches underlying algorithms used in machine learning and artificial intelligence, and their application in the implementation of physical and logical protection mechanisms.			x		x			x	x								x		x			x
B – Ability to Apply Knowledge and Understanding																							
1) Ability to apply knowledge related to the design, development, and verification of software in complex environments, including in relation to secure software development.	x		x	x		x	x					x	x						x			x
2) Ability to apply knowledge of embedded systems and Internet of Things architectures aimed at software development in distributed environments and the security analysis from the perspective of risk arising from cyberattacks.	x		x	x								x	x					x	x			x

3) Ability to apply knowledge relating to the modeling and management of complex systems, with particular attention to security and risk management aspects.	x	x	x	x				x						x	x	x	x			x	x	x	x
4) Ability to formulate and apply cutting-edge solutions for risk mitigation in the field of cybersecurity, both in the design phase and during operation, in various application contexts, and for system management in the presence of a breach.	x	x	x	x	x	x	x	x	x	x	x				x	x		x	x	x			x
5) Ability to implement original and appropriate algorithmic solutions derived from knowledge of artificial intelligence methodologies, including applications to physical and logical system security.			x		x	x	x	x	x								x		x				x
C – Autonomy of Judgment																							
1) Ability to form one's own evaluation and/or judgment based on the interpretation of available data and abstract models.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2) Ability to identify methods, including original and innovative ones, for collecting any additional data necessary to achieve greater certainty regarding complex topics in information engineering, with particular emphasis on cybersecurity aspects.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3) Ability to effectively communicate information and ideas, as well as discuss problems and solutions. Know how to choose the appropriate form and medium of communication for both specialist and non-specialist audiences.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
D – Communication Skills																							
1) Ability to effectively communicate information and ideas, as well as discuss problems and solutions. Know how to choose the appropriate form and medium of communication for both specialist and non-specialist audiences.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E – Learning Ability																							
1) Have the self-learning skills necessary for an engineer to continuously update themselves in line with the evolution of science and technology in the field of information engineering.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2) Have the ability to draw from various bibliographic sources in order to acquire new skills.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3) Have the self-learning abilities needed to pursue further studies, such as second-level Master's degrees and PhDs in the field of information engineering—and cybersecurity in particular—as well as to begin professional activities at research and advanced design centers.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Reference faculty members and Mentors available to the students

Reference faculty members	**Mentors**
Biggio Battista	Biggio Battista
Franceschelli Mauro	Franceschelli Mauro
Giacinto Giorgio	Giacinto Giorgio
Maiorca Davide	Davide Maiorca
Seatzu Carla	Seatzu Carla
Sotgiu Angelo	