ANX-PR/CL/001-01

LEARNING GUIDE

SUBJECT

103000806 - Design Of Correct-by-construction Systems

DEGREE PROGRAMME

10AS - Máster Interuniversitario En Métodos Formales En Ingeniería Informática

ACADEMIC YEAR & SEMESTER

2025/26 - Semester 2

Index

Learning guide

1. Description

1.1. Subject details

Name of the subject	103000806 - Design Of Correct-By-Construction Systems
No of credits	6 ECTS
Type	Optional/elective
Academic year ot the programme	First year
Semester of tuition	Semester 2
Tuition period	February-June
Tuition languages	English
Degree programme	10AS - Máster Interuniversitario en Métodos Formales en Ingeniería Informática
Centre	10 - E.T.S. De Ingenieros Informáticos
Academic year	2025-26

2. Faculty

2.1. Faculty members with subject teaching role

Name and surname	Office/Room	Email	Tutoring hours *
Manuel Carro Liñares (Subject coordinator)		manuel.carro@upm.es	M - 13:00 - 15:00 Tu - 13:00 - 15:00 W - 13:00 - 15:00 Please get in touch with the instructor to schedule an appointment

Manuel De Hermenegildo Salinas		manuel.hermenegildo@upm.es	Sin horario. Contact the instructor to schedule an appointment.
Manuel De Hermenegildo Salinas		manuel.hermenegildo@upm.es	Sin horario. Please contact the instructor to schedule an appointment

* The tutoring schedule is indicative and subject to possible changes. Please check tutoring times with the faculty member in charge.

3. Prior knowledge recommended to take the subject

3.1. Recommended (passed) subjects

The subject - recommended (passed), are not defined.

3.2. Other recommended learning outcomes

- Declarative programming

- Programming experience (minimum 2 years)

- First-order logic

- Formal proofs

- Reasoning about properties of algorithms

- Concurrent systems and concurrent programming

4. Skills and learning outcomes *

4.1. Skills to be learned

RAC20 - Encontrar una formalización y una estrategia de validación formal adecuada para analizar propiedades de corrección en sistemas informáticos / Find the appropriate formalization and validation strategy to analyse correctness Properties in computer systems. TIPO: Competencias.

RAC22 - Comparar y decidir el modelo de concurrencia que mejor se adapte para capturar las características intrínsecas de un sistema informático concurrente / Compare and decide the concurrency model that is best suited to capture the intrinsic characteristics of a concurrent computing system. TIPO: Competencias.

RAK5 - Relacionar, señalando puntos fuertes y débiles, distintas modelizaciones de sistemas informáticos / Relate, pointing out strengths and weaknesses, different modeling of computer systems. TIPO: Conocimientos o contenidos.

RAS14 - Diseñar y valorar variaciones de un sistema informático existente para que sea posible comprobar propiedades relevantes de manera más simple / Design and evaluate variations of an existing computer system so that relevant properties can be easier to check. TIPO: Habilidades o destrezas.

RAS9 - Demostrar o desmentir formalmente propiedades de corrección de sistemas informáticos / Formally prove or disprove correctness properties of computer systems. TIPO: Habilidades o destrezas.

4.2. Learning outcomes

RA1 - All RA are defined in the previous section

* The Learning Guides should reflect the Skills and Learning Outcomes in the same way as indicated in the Degree Verification Memory. For this reason, they have not been translated into English and appear in Spanish.

5. Brief description of the subject and syllabus

5.1. Brief description of the subject

Software is becoming increasingly complex and responsible for critical tasks. Any technology aimed at ensuring the reliability and quality of software will be increasingly relevant, if not utterly necessary.

Only rigorous (e.g., mathematically sound) approaches can certify software with the highest possible assurance. These approaches include, among others, the use of specification languages, high-level programming languages (including equational, functional, and logic languages), the use of model checking and deductive verification, language-based approaches often interacting with theorem provers.

In this course we will give a hands-on introduction to rigorous software development methods that follow a *correctness-by-construction* approach. While the course is not heavy in theory, everyone is expected to have a good understanding of first-order logic and programming experience.

5.2. Syllabus

1. Introduction to Formal Methods: Proving Programs Correct

2. Fundamentals of Formal Methods: Specification, First-Order Logic, Proofs, Programs

3. Event-B Basics and the Rodin Tool

4. Sequential Systems

5. Event B: Mathematical Toolkit and Applications

6. Reactive Systems: Concurrency and Distribution

6. Schedule

6.1. Subject schedule*

Week	Type 1 activities	Type 2 activities	Distant / On-line	Assessment activities
1	**Introduction to formal methods and correctness by construction** Duration: 01:30 **Sample cases of formal development** Duration: 01:30			
2	**Event-B and related topics** Duration: 02:00 **Quizzes** Duration: 01:00			
3	**Event-B and related topics** Duration: 02:00 **Quizzes** Duration: 01:00			**Homework** Progressive assessment Not Presential Duration: 04:00
4	**Event-B and related topics** Duration: 02:00 **Quizzes** Duration: 01:00			
5	**Event-B and related topics** Duration: 02:00 **Quizzes** Duration: 01:00			
6	**Event-B and related topics** Duration: 02:00 **Quizzes** Duration: 01:00			**Homework** Progressive assessment Not Presential Duration: 04:00

7	**Event-B and related topics** Duration: 02:00 **Quizzes** Duration: 01:00			
8	**Event-B and related topics** Duration: 02:00 **Quizzes** Duration: 01:00			
9	**Event-B and related topics** Duration: 02:00 **Quizzes** Duration: 01:00			**Homework** Progressive assessment Not Presential Duration: 08:00
10	**Quizzes** Duration: 01:00 **Event-B and related topics** Duration: 02:00			
11	**Presentation of term project** Duration: 01:00 **Event-B and related topics** Duration: 02:00			**Term project** Progressive assessment Not Presential Duration: 20:00
12	**Event-B and related topics** Duration: 02:00 **Quizzes** Duration: 01:00			
13	**Event-B and related topics** Duration: 02:00 **Quizzes** Duration: 01:00			
14	**Event-B and related topics** Duration: 02:00 **Quizzes** Duration: 01:00			

15	**Presentaciones de trabajo en grupo** Duration: 03:00			**Presentation and defense of group projects** Progressive assessment Presential Duration: 03:00
16				
17				**Final regular exam** Global examination Presential Duration: 03:00

Depending on the programme study plan, total values will be calculated according to the ECTS credit unit as 26/27 hours of student face-to-face contact and independent study time.

7. Activities and assessment criteria

7.1. Assessment activities

7.1.1. Assessment

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
3	Homework		No Presential	04:00	20%	2 / 10	RAS9
6	Homework		No Presential	04:00	20%	2 / 10	RAC20
9	Homework		No Presential	08:00	20%	2 / 10	RAK5 RAS14 RAC22
11	Term project		No Presential	20:00	%	4 / 10	RAK5 RAS14 RAC22
15	Presentation and defense of group projects		Face-to-face	03:00	40%	4 / 10	RAK5 RAS9 RAS14 RAC20 RAC22

7.1.2. Global examination

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
17	Final regular exam		Face-to-face	03:00	100%	5 / 10	RAK5 RAS9 RAS14 RAC20 RAC22

7.1.3. Referred (re-sit) examination

Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills

Extra final exam		Face-to-face	03:00	100%	5 / 10	RAK5 RAS9 RAS14 RAC20 RAC22

7.2. Assessment criteria

- No mandatory activities are necessary to pass via the final exams
- The minimum grade to pass the course is 5 over 10 (either when it is calculated as the weighted sum of individual homework or when it is the grade of a single comprehensive exam).
- The topics covered in the different homework assignments cannot be tested separately in the final exam, as they are deeply intertwined and are not isolated units of knowledge.
- The global exams, both the regular and the extraordinary ones, will be in person.

- Copying from any source (either textbooks, the Internet, another student, or any other source) with or without the permission of the author of the source, as well as other types of academic fraud, can lead to a 'fail' grade in the course and / or being reported to the academic authorities, who will decide whether to take additional authoritative measures. In particular, in case of non-ethical or fraudulent behavior, the Law 3/2022 of February 24th will be applied, as well as the corresponding UPM regulations. Article 12 and 14 of Law 3/2022 states that a serious fault may mean, among other outcomes, failing the corresponding sitting.
- There are no learning blocks whose earned grades can be carried over to future academic courses.
- Failure to deliver a homework assignment at the time and in the form stated by the instructor(s) may result in a failure for that exercise.
- For progressive evaluation: if for any reason it is not possible to prepare / hand out some homework assignment, its weight in the final grade will be split among the rest of the homework exercises in such a way that the relative weight of the rest of the assignments, when compared with each other, will be the same they had before removing the homework that could not be handed out.

8. Teaching resources

8.1. Teaching resources for the subject

Name	Type	Notes
Lawrence Paulson's class notes	Bibliography	Lawrence Paulson?s Logic and Proof are the course notes of the author for a Logic course in Cambridge. Highly recommended, as they are both rigorous and very concise. They provide very good background material for both parts of the course.
Logic in Computer Science (Huth and Ryan)	Bibliography	A very good book on the use of logic in computer science is Logic in Computer Science, by Huth and Ryan. The Computer Science School should have several copies. There may be electronic copies on the Internet, if possible of the second edition.
http://wiki.event-b.org/	Web resource	Central Event-B site
Modeling in Event-B: System and Software Engineering, by Jean-Raymond Abrial.	Bibliography	The reference book for Event B, with plenty of worked examples.

9. Other information

9.1. Other information about the subject

This course will be given in English. Please note that in case Spanish appears as the course language in the general description, that would be a clerical mistake.