

**ANX-PR/CL/001-01**  
**GUÍA DE APRENDIZAJE**

**ASIGNATURA**

Rigorous software development

**CURSO ACADÉMICO - SEMESTRE**

2016-17 - Primer semestre

## Datos Descriptivos

---

<b>Nombre de la Asignatura</b>	Rigorous software development
<b>Titulación</b>	10AM - Master Universitario en Ingeniería del Software
<b>Centro responsable de la titulación</b>	Escuela Técnica Superior de Ingenieros Informáticos
<b>Semestre/s de impartición</b>	Primer semestre
<b>Carácter</b>	Optativa
<b>Código UPM</b>	103000546
<b>Nombre en inglés</b>	Rigorous software development

## Datos Generales

---

<b>Créditos</b>	4	<b>Curso</b>	1
<b>Curso Académico</b>	2016-17	<b>Período de impartición</b>	Septiembre-Enero
<b>Idioma de impartición</b>	Inglés	<b>Otros idiomas de impartición</b>	

## Requisitos Previos Obligatorios

---

### Asignaturas Previas Requeridas

El plan de estudios Master Universitario en Ingeniería del Software no tiene definidas asignaturas previas superadas para esta asignatura.

### Otros Requisitos

El plan de estudios Master Universitario en Ingeniería del Software no tiene definidos otros requisitos para esta asignatura.

## Conocimientos Previos

---

### Asignaturas Previas Recomendadas

El coordinador de la asignatura no ha definido asignaturas previas recomendadas.

### Otros Conocimientos Previos Recomendados

First-order logic, formal proofs, declarative programming, reasoning about properties of algorithms.

All students willing to take this course are encouraged to get in touch with one of the instructors prior to enrollment.

## Competencias

---

CG10 - Capacidad de pensamiento creativo con el objetivo de desarrollar enfoques y métodos nuevos y originales

## Resultados de Aprendizaje

---

RA65 - RA-AV-1 - Acquaintance with design requirements and implementation requirements.

RA70 - RA-AV-5 - Effective use of rigorous software development techniques.

RA68 - RA-AV-3 - Knowledge of languages for formal specification

RA69 - RA-AV-4 - Knowledge of techniques for formally proving code correctness.

RA66 - RA-AV-2 Acquaintance with various techniques for formal software development

RA67 - RA-AV-2 - Acquaintance with various techniques for formal software development

## Profesorado

---

### Profesorado

Nombre	Despacho	e-mail	Tutorías
Carro Liñares, Manuel	D2304	manuel.carro@upm.es	Please send an e-mail to ensure an appointment before going to the instructor's office.
Mariño Carballo, Julio ( <b>Coordinador/a</b> )	D2308	julio.marino@upm.es	Please send an e-mail to ensure an appointment before going to the instructor's office.

**Nota.-** Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

## Descripción de la Asignatura

---

Software is getting more and more complex and is becoming responsible for critical tasks. Therefore, any technology aimed at ensuring the reliability and quality of software will be increasingly relevant.

There are many ways to approach these goals. The *declarative* approach relies on languages and logics with a solid mathematical foundation. This includes especificacion languages (VDM, Z, B, Event-B, OBJ, Alloy, ...), functional programming languages (Haskell, Erlang,  $\lambda$ -calculi?), logic programming languages (Prolog, CLP, ASP,?) among others.

Some basic knowledge of logic and functional and logic programming is assumed as a prerequisite.

Some goals of the course are:

- To motivate the use of technologies in software development under the correctness-by-construction paradigm.
- To study different families of languages aimed at easing the process of building correct software.
- To understand the differences between declarative and procedural languages and the impact of these aspects in software development.
- To identify the better niches for the industrial application of declarative / correctness by construction technologies.

## Temario

---

1. Introduction
  - 1.1. Overview, motivation, and challenges for rigorous SW development
  - 1.2. Review of background: formal logic, proofs...
2. Correctness by Construction
  - 2.1. Event-B: Theory and development methods.
  - 2.2. Event-B: the Rodin tool
3. Verification.
  - 3.1. Classical program verification
  - 3.2. The Dafny tool
  - 3.3. The Alloy tool
  - 3.4. Property-based testing
4. Specifications
  - 4.1. Algebraic specifications
  - 4.2. The Maude algebraic specification language



## Cronograma

**Horas totales:** 32 horas

**Horas presenciales:** 32 horas (30.8%)

**Peso total de actividades de evaluación continua:**  
100%

**Peso total de actividades de evaluación sólo prueba final:**  
100%

Semana	Actividad Presencial en Aula	Actividad Presencial en Laboratorio	Otra Actividad Presencial	Actividades Evaluación
Semana 1	<b>Course introduction</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral			
Semana 2	<b>Rigorous software development: a broad landscape</b> Duración: 01:45 LM: Actividad del tipo Lección Magistral			<b>Exercises, questions, and answers</b> Duración: 00:15 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial
Semana 3	<b>Event-B</b> Duración: 01:45 AC: Actividad del tipo Acciones Cooperativas			<b>Exercises, questions, and answers</b> Duración: 00:15 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial
Semana 4	<b>Event-B</b> Duración: 01:45 AC: Actividad del tipo Acciones Cooperativas			<b>Exercises, questions, and answers</b> Duración: 00:15 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial
Semana 5	<b>Event-B</b> Duración: 01:45 AC: Actividad del tipo Acciones Cooperativas			<b>Exercises, questions, and answers</b> Duración: 00:15 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial
Semana 6	<b>Event-B</b> Duración: 01:45 AC: Actividad del tipo Acciones Cooperativas			<b>Exercises, questions, and answers</b> Duración: 00:15 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial
Semana 7	<b>Event-B</b> Duración: 01:45 AC: Actividad del tipo Acciones Cooperativas			<b>Exercises, questions, and answers</b> Duración: 00:15 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial
Semana 8	<b>Program Verification</b> Duración: 01:45 LM: Actividad del tipo Lección Magistral			<b>Exercises, questions, and answers</b> Duración: 00:15 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial

Semana 9	<b>Program Verification</b> Duración: 01:45 LM: Actividad del tipo Lección Magistral			<b>Exercises, questions, and answers</b> Duración: 00:15 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial
Semana 10	<b>Program Verification</b> Duración: 01:45 LM: Actividad del tipo Lección Magistral			<b>Exercises, questions, and answers</b> Duración: 00:15 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial
Semana 11	<b>Algebraic specifications</b> Duración: 01:45 LM: Actividad del tipo Lección Magistral			<b>Exercises, questions, and answers</b> Duración: 00:15 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial
Semana 12	<b>Algebraic specifications</b> Duración: 01:45 LM: Actividad del tipo Lección Magistral			<b>Exercises, questions, and answers</b> Duración: 00:15 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial
Semana 13	<b>Algebraic specifications</b> Duración: 01:45 LM: Actividad del tipo Lección Magistral			<b>Exercises, questions, and answers</b> Duración: 00:15 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial
Semana 14	<b>Alloy</b> Duración: 01:45 PR: Actividad del tipo Clase de Problemas			<b>Exercises, questions, and answers</b> Duración: 00:15 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial
Semana 15	<b>Exercises and problems</b> Duración: 02:00 AC: Actividad del tipo Acciones Cooperativas			
Semana 16				<b>Project presentation</b> Duración: 02:00 TG: Técnica del tipo Trabajo en Grupo Evaluación continua Actividad presencial
Semana 17				<b>Project presentation/Exam</b> Duración: 02:00 OT: Otras técnicas evaluativas Evaluación sólo prueba final Actividad presencial

**Nota.-** El cronograma sigue una planificación teórica de la asignatura que puede sufrir modificaciones durante el curso.

**Nota 2.-** Para poder calcular correctamente la dedicación de un alumno, la duración de las actividades que se repiten en el tiempo (por ejemplo, subgrupos de prácticas") únicamente se indican la primera vez que se definen.

## Actividades de Evaluación

Semana	Descripción	Duración	Tipo evaluación	Técnica evaluativa	Presencial	Peso	Nota mínima	Competencias evaluadas
2	Exercises, questions, and answers	00:15	Evaluación continua	OT: Otras técnicas evaluativas	Sí	3.85%		CG10
3	Exercises, questions, and answers	00:15	Evaluación continua	OT: Otras técnicas evaluativas	Sí	3.85%		CG10
4	Exercises, questions, and answers	00:15	Evaluación continua	OT: Otras técnicas evaluativas	Sí	3.85%		CG10
5	Exercises, questions, and answers	00:15	Evaluación continua	OT: Otras técnicas evaluativas	Sí	3.85%		CG10
6	Exercises, questions, and answers	00:15	Evaluación continua	OT: Otras técnicas evaluativas	Sí	3.85%		CG10
7	Exercises, questions, and answers	00:15	Evaluación continua	OT: Otras técnicas evaluativas	Sí	3.85%		CG10
8	Exercises, questions, and answers	00:15	Evaluación continua	OT: Otras técnicas evaluativas	Sí	3.85%		CG10
9	Exercises, questions, and answers	00:15	Evaluación continua	OT: Otras técnicas evaluativas	Sí	3.85%		CG10
10	Exercises, questions, and answers	00:15	Evaluación continua	OT: Otras técnicas evaluativas	Sí	3.85%		CG10
11	Exercises, questions, and answers	00:15	Evaluación continua	OT: Otras técnicas evaluativas	Sí	3.85%		CG10
12	Exercises, questions, and answers	00:15	Evaluación continua	OT: Otras técnicas evaluativas	Sí	3.85%		CG10
13	Exercises, questions, and answers	00:15	Evaluación continua	OT: Otras técnicas evaluativas	Sí	3.85%		CG10
14	Exercises, questions, and answers	00:15	Evaluación continua	OT: Otras técnicas evaluativas	Sí	3.8%		CG10
16	Project presentation	02:00	Evaluación continua	TG: Técnica del tipo Trabajo en Grupo	Sí	50%		CG10
17	Project presentation/Exam	02:00	Evaluación sólo prueba final	OT: Otras técnicas evaluativas	Sí	100%		CG10

## Criterios de Evaluación

Depending of the number of students, the final grade will be obtained either from:

- A suite of short, individual practical exercises periodically proposed which will be worth 50% of the final grade. The remaining 50% will come from short presentations.
- Individual practical exercises, if the number of students is too high to allow for the extra sessions needed for the presentations.

Exercises for each unit will have the same relative weight for the overall grade, although individual exercises in a given unit can have different weights.

## Recursos Didácticos

Descripción	Tipo	Observaciones
Event B development environment	Otros	
Dafny	Otros	
Maude	Otros	
Alloy	Otros	
Modeling in Event-B: System and Software Engineering. Jean-Raymond Abrial. Cambridge University Press.	Bibliografía	
<a href="http://wiki.event-b.org/">http://wiki.event-b.org/</a>	Bibliografía	
The Dafny web page at Microsoft RiSE: <a href="http://www.rise4fun.com/Dafny">http://www.rise4fun.com/Dafny</a>	Recursos web	
All About Maude -- A High Performance Logical Framework. Clavel, M., Durán, F., Eker, S., Lincoln, P., Martí-Oliet, N., Meseguer, J., Talcott, C. Lecture Notes in Computer Science, vol. 4350.	Bibliografía	
Alloy: A Lightweight Object Modelling Notation. Daniel Jackson. ACM Transactions on Software Engineering and Methodology (TOSEM'02), volume 11, issue 2, pages 256-290.	Bibliografía	
Seven Myths of Formal Methods. Anthony Hall. IEEE Software, September 1990	Bibliografía	
Seven More Myths of Formal Methods. Jonathan P. Bowen, Michael G. Hinchey. IEEE Software, July 1995.	Bibliografía	
First Steps in the Verified Software Grand Challenge. Cliff Jones, Peter O'Hearn, Jim Woodcock. IEEE Computer, April 2006.	Bibliografía	

## Otra Información

All students willing to take this course are encouraged to get in touch with one of the instructors prior to enrollment, in order to verify their background.