Guide pédagogique

***Module** « Modélisation et vérification de systèmes réactifs critiques »*

***Option IAIL – 9.3** (4 crédits ECTS)*

Place du module et enjeux

Quel que soit le profil visé par les étudiants de l'option Intelligence Artificielle et Ingénierie Logicielle du département 2IA, leur métier les conduira à concevoir, réaliser ou plus simplement étudier la performance de systèmes réactifs : ce sont des systèmes constitués de composants logiciels en interaction avec des systèmes de différentes natures (électroniques, mécaniques, etc.) dans un environnement les sollicitant en permanence. Ces systèmes présentent la caractéristique d'être répartis spatialement, de communiquer selon différents protocoles mettant en jeu des mécanismes de synchronisation spécifiques. Comme tout système logiciel, ils doivent répondre à des propriétés fonctionnelles, mais leur environnement d'utilisation nécessite que leurs propriétés temporelles et de sûreté soient également vérifiées. Il est donc nécessaire de connaître les processus d'Ingénierie Système permettant de concevoir de tels systèmes et d'en maîtriser les techniques et bonnes pratiques de conception et de vérification.

Ce module constitue une introduction à la conception d'ingénierie des systèmes réactifs par une approche dirigée par les modèles en montrant la complémentarité d'une approche formelle où architectures, composants et communications sont modélisés et analysés en vue de vérifier les propriétés de vivacité et de sûreté du système durant sa conception.

Responsable : Anne-Lise Courbis
Téléphone : 04 34 24 62 63
Courriel : anne-Lise.courbis@mines-ales.fr

IMT Mines Alès
École Mines-Télécom

Teaching guide and syllabus

« Modelling and Verification of Dependable Reactive Systems » module

AISE option – 9.3 *(4 ECTS credits)*

Subject matter importance and associated issues

Students of CSAI department, whatever their future work and application domains, will face problems of design, realisation or performance evaluation of embedded or distributed systems: such systems are constituted with several software components interacting with other systems of various types (electronical, mechanical, human, etc.). Several features characterized these systems: their components are spatially distributed; data or events are exchanged through specific communication protocols; synchronization mechanisms are required to run the system in a proper way. Liveness is a key feature of such systems since they have to react permanently to events coming from their environment. Like any software system, they must be compliant to their requirements and meet the expected functional properties. However, due to their features and their environment of use, it is necessary to verify their temporal and safety properties. It is thus useful for future engineers in software development to know System Engineering processes for designing such systems as well as techniques and practices of design and verification.

This module introduces main concepts of system engineering applied to reactive embedded systems. The model driven architecture approach is associated with formal methods where components, behaviours and communications are modelled and analysed in order to verify both liveness and safety properties.

Responsable : Anne-Lise Courbis
Téléphone : 04 34 24 62 63
Courriel : anne-Lise.courbis@mines-ales.fr

ENSEIGNEMENTS ACADÉMIQUES	**Volume horaire**	Détail des coefficients	Crédits
Modélisation et vérification de systèmes réactifs critiques o Architectures de systèmes réactifs o Spécification formelle et vérification en Electrum/Alloy o Spécification formelle et vérification en algèbres de processus	**50 h** 16 17 17	 1 1 1	4

Matière 1

Titre de la matière : Architectures de systèmes réactifs	
Code : 2IAiail 9.3.1	**Titre du module :** Modélisation et vérification de systèmes réactifs critiques
Semestre : S9	**Cursus de rattachement :** Département 2IA, option IAIL

Heures présentiel	Heures Total	Cours	TD	TP	Projet	Contrôles	Travail personnel	Coef /module	ECTS
16	25	12			4	0,5	9	1	1,3

Résumé	Ce cours présente les caractéristiques des architectures de systèmes réactifs et une approche permettant de les modéliser

Responsable	Anne-Lise Courbis – CERIS/IMT Mines Alès
Équipe enseignante	Anne-Lise Courbis – CERIS/IMT Mines Alès

Mots-clés	Systèmes réactifs, Modélisation à base de composants.
Prérequis	UML (Matière 2IA – S8.4.1 : Conception des logiciels)

Contexte et objectif général :
Cet enseignement introduit les bases de la conception de systèmes répartis par une approche basée sur les modèles

Programme et contenu :

1. Conception d'architectures
   - Définitions et standards
   - Propriétés attendues
   - Techniques de communication de systèmes répartis
   - Principes fondamentaux de conception (couplage faible, cohésion forte, abstraction et approche incrémentale)
   - Les Patterns & Styles Architecturaux
2. Ingénierie des Systèmes Réactifs par une approche MDA (Model Driven Architecture)
   - Modélisation des éléments du système
   - Formalisation de comportement par machines à états
   - Modélisation de l'architecture du système
3. Projet de réalisation d'une architecture à partir d'une spécification informelle d'un système réactif (projet en commun avec les autres cours du module)

Méthode et organisation pédagogique :
L'enseignement sera organisé en cours/TP suivi d'un projet commun avec les autres matières du module, mené en groupe. Les TP et le projet seront réalisés sur les ordinateurs personnels des élèves. Un examen écrit individuel sera organisé pour s'assurer que les élèves ont acquis les bases.
Le découpage est prévu comme suit :

- 12h de cours/TP
- 4h de projet (dont 1h réservée aux soutenances)

Acquis d'apprentissage visés :
Abstraction et Modélisation de systèmes, Vue structurelle et vue comportementale d'un système

Évaluation :
par projet (rapport + présentation orale commune avec les autres matières du module) + examen écrit de 30'

Retour sur l'évaluation fait à l'élève :
A l'issue de la présentation orale du projet + commentaires faits sur le rapport du projet (maximum 3 semaines après la date de remise) + commentaires sur copies d'examen

Support pédagogique et références :
Support du cours mis en ligne incluant une bibliographie

Matière 2

Titre de la matière : Spécification formelle et vérification en Electrum/Alloy	
Code : 2IAiail 9.3.2	**Titre du module :** Modélisation et vérification de systèmes réactifs critiques
Semestre : S9	**Cursus de rattachement :** Département 2IA, option IAIL

Heures présentiel	Heures total	Cours	TD	TP	Projet	Contrôles	Travail personnel	Coef /module	ECTS
17	25	12			4	1	9	1	1,4

Résumé	Ce cours présente le formalisme Alloy/Electrum permettant de spécifier un système réactif ainsi que les propriétés comportementales qu'il doit satisfaire. Il comporte d'une part des aspects théoriques, et d'autre part l'utilisation d'un outil de modélisation et de vérification formelle.

Responsable	Julien Brunel – ONERA, Toulouse (cours/TP)
Équipe enseignante	Julien Brunel – ONERA, Toulouse (cours/TP)

Mots-clés	Spécification formelle, Vérification Formelle, Logique, Model Checking, Alloy, Electrum
Prérequis	Concept de modélisation de systèmes, techniques de communication synchrone et asynchrone, Introduction aux spécifications formelle en Alloy (cf. enseignement 2IA S8.4.2).

Contexte et objectif général :
Ce cours permet aux futurs ingénieurs d'aborder les aspects théoriques et pratiques de modélisation et de vérification de systèmes critiques dans l'environnement Electrum.

Programme et contenu :

1. Présentation du formalisme Alloy/Electrum utilisé pour décrire le comportement des systèmes réactifs et les propriétés attendues
2. Projet de spécification et de vérification d'un système à l'aide de l'outil Electrum (projet commun avec les autres cours du module)

Méthode et organisation pédagogique :
L'enseignement sera organisé en cours/TP suivi d'un projet commun avec les autres matières du module, mené en binôme. Les TP et projet seront réalisés sur les ordinateurs personnels des élèves.
Le découpage est prévu comme suit :

- 12h de cours/TP
- 4h de projet

Acquis d'apprentissage visés :
Abstraction et modélisation formelle de systèmes, expression formelle de propriétés en logique

Évaluation : par projet (rapport + présentation orale commune avec les autres matières du module) + examen écrit de 1h

Retour sur l'évaluation fait à l'élève :
A l'issue de la présentation orale du projet + commentaires faits sur le rapport du projet (maximum 3 semaines après la date de remise) + commentaires sur copies d'examen

Support pédagogique et références :
1 jeu de planches (support papier / pdf)

Matière 3

Titre de la matière : Spécification et vérification en algèbres de processus	
Code : 2IAiail 9.3.	**Titre du module :** Modélisation et vérification de systèmes réactifs critiques
Semestre : S9	**Cursus de rattachement :** Département 2IA, option IAIL

Heures présentiel	Heures total	Cours	TD	TP	Projet	Contrôles	Travail personnel	Coef /module	ECTS
17	28	12			4	1	11	1	1,3

Résumé	Ce cours aborde des techniques formelles permettant de spécifier un système réactif ainsi que les propriétés comportementales qu'il doit satisfaire. Il comporte d'une part des aspects théoriques incluant les systèmes de transitions et la logique, et d'autre part l'utilisation d'un outil de modélisation et de vérification formelle.

Responsable	Thomas Lambolais – CERIS/IMT Mines Alès
Équipe enseignante	Thomas Lambolais – CERIS/IMT Mines Alès

Mots-clés	Spécification formelle, Vérification Formelle, Model Checking, CCS, LTS
Prérequis	Concept de modélisation et d'Architecture de systèmes, techniques de communication synchrone et asynchrone

Contexte et objectif général :
Ce cours propose de sensibiliser les futurs ingénieurs aux approches formelles de spécification et de vérification de systèmes réactifs en vue de d'analyser leur comportement.

Programme et contenu :

1. Présentation des formalismes utilisés pour décrire le comportement des systèmes réactifs :
   - CCS (Calculus of Communicating Systems) avec l'outil CAAL, ou LOTOS avec l'outil CADP.
   - LTS (Labelled Transition Systems), systèmes de transition,
   - traces d'exécution,
   - relations de comparaison : bisimulations, conformité, ,..
2. Présentation du langage formel HML (Henessy Milner Logics) permettant de décrire des propriétés
3. Expérimentations à l'aide de l'approche outillée

Méthode et organisation pédagogique :
L'enseignement sera organisé en cours/TP suivi d'un projet commun avec les deux autres matières du module, mené en groupe. Les TP et projet seront réalisés sur les ordinateurs personnels des élèves.
Le découpage est prévu comme suit :

- 12h de cours/TP
- 4h de projet

Acquis d'apprentissage visés :
Abstraction et Modélisation formelle de systèmes, Expression formelle de propriétés en logique

Évaluation : par projet (rapport + présentation orale commune avec les autres matières du module) + examen écrit de 1h

Retour sur l'évaluation fait à l'élève :
A l'issue de la présentation orale du projet + notation du rapport du projet (maximum 3 semaines après la date de remise).+ commentaires sur copies d'examen

Support pédagogique et références :
1 jeu de planches (support papier / pdf)

Méthode et organisation pédagogique

Il s'agit d'un enseignement classique avec une partie réalisée en cours interactifs et une partie appliquée au travers de TD/TP et d'un projet. Des outils de modélisation et d'analyse seront utilisés. Les élèves devront les télécharger (gratuitement) et les installer sur leur ordinateur personnel.

Modalité d'évaluation

Le niveau d'acquisition des compétences sera évalué selon les exigences suivantes :

N° indicateur	Indicateur
1	Connaître les savoirs formels et pratiques du socle des fondamentaux
2	Exploiter les savoirs théoriques et pratiques
3	Analyser, interpréter, modéliser, émettre des hypothèses, et résoudre

Répartition

Matière	**Contrôle**	**Coefficients**	**Type de notation**	**Indicateurs évalués**	**Chapitres**
Architectures de systèmes réactifs	Projet commun aux trois matières	1	En groupe	1, 2, 3	Tous
Spécification formelle et vérification en Electrum/Alloy					
Spécification et vérification en algèbres de processus					
Architectures de systèmes réactifs	Examen écrit	1/3	individuel	1,2	Tous
Spécification formelle et vérification en Electrum/Alloy	Examen écrit	1/3	individuel	1,2	Tous
Spécification et vérification en algèbres de processus	Examen écrit	1/3	Individuel	1,2	Tous

Dans chacune des matières du module, une évaluation non prévue à l'emploi du temps (contrôles surprise) peut advenir.

Engagement de l'étudiant, éthique et professionnalisme

La démarche éthique est définie dans le règlement intérieur de l'établissement. Chaque étudiant s'engage à en prendre connaissance et à la respecter.

Obligation des cours : Présence obligatoire pour tous à chaque séance

Nombre d'heures estimées de travail personnel *:* pour acquérir les compétences demandées, il est nécessaire que l'étudiant consacre minimum 45 min de travail personnel de compréhension et d'approfondissement par séance de cours.
30h de travail personnel sont estimées, principalement dédiées à la définition et réalisation du projet.

Nombre d'heures estimées de préparation aux travaux dirigés (TD) *:* 45 minutes

Pénalité pour retard :

Tout travail remis en retard sans motif valable peut être pénalisé de 1 point par jour de retard (notation sur 20 points).

Équipe enseignante

Nom	Domaine d'expertise	Courriel/Téléphone
Julien Brunel, ONERA, Toulouse	Spécification et Vérification Formelles en Alloy, Logique, Model Checking Analyses de Sûreté de Fonctionnement	julien.brunel@onera.fr
Anne-Lise Courbis, CERIS, IMT Mines Alès	Ingénierie Dirigée par les Modèles, Modélisation de systèmes embarqués, Simulation, Vérification formelle	anne-lise.courbis@mines-ales.fr 04 34 24 62 63
Thomas Lambolais, CERIS, IMT Mines Alès	Génie logiciel, spécification formelle validation	thomas.lambolais@mines-ales.fr 04 34 24 62 60

ACADEMIC TEACHING	**Teaching hours**	Coefficients	Credits
Modelling and Verification of Dependable Reactive Systems	**50 h**		
○ Reactive System Architecture	16	1	4
○ Formal Specification and Verification in Electrum/Alloy	17	1	
○ Formal Specification and Verification in Process Algebra	17	1	

Class 1

ClassTitle : Reactive System Architectures	
Code : 2IAiail 9.3.1	**Module title :** Modelling and Verification of Dependable Reactive Systems
Semester : S9	**Classification :** CSAI department, AISE option

Hours of presence	Total hours	Lectures	Workshop	Labs	Project	Testing	Personal work	Coef /module	ECTS
16	25	12			4	0,5	9	1	1,3

Summary	This course presents main concepts of reactive system architecture as well as methods and tools for their design

Head	Anne-Lise Courbis – CERIS/IMT Mines Alès
Teaching team	Anne-Lise Courbis – CERIS/IMT Mines Alès

Key words	Embedded System, Reactive Systems, Component Modelling
Prerequisites	UML (module 2IA-8.4.1: software conception)

Context and general objective:
This course deals with main concepts of embedded systems design based on a Model Driven Engineering approach.

Programme and contents:

1. Software Architecture Design
   - Definitions and standards
   - Expected properties,
   - Communication and Synchronization of embedded systems
   - Design Principles (loose coupling, high cohesion, abstraction and incrementality)
   - Architectural Patterns & Styles
2. Reactive System Engineering though a MDA (Model Driven Architecture) approach
   - Behavioral Modelling by UML state machines
   - Architectural modelling using UML composite component diagrams
3. Experimentation with a framework to design a software architecture starting from an informal specification

Method and pedagogic organisation:
The class is organised in lectures / lab sessions, followed by a project shared with the other classes of the modules, and carried out by small group of students. Student personal computers are required for the lab sessions and project development. The course is organised as follows:

- 12 h course/lab
- 4h project

Targeted skills or knowledge:
Abstraction & System Modelling, System Architecture, System Behaviour, System Analyses

Evaluation :
Project report and oral presentation + individual exam (30')

Feedback made to the student:
During the oral presentation + commentaries on the project report (max. 3 weeks after the end of project) + commentaries on the exam copies

Teaching material and references:
Slides including a bibliography

Class 2

Class title: Formal Specification and Verification in Electrum/Alloy	
Code : 2IAiail 9.3.2	**Module title :** Modelling and Verification of Dependable Reactive Systems
Semester: S9	**Classification :** CSAI Department, AISE option

Hours of presence	Total hours	Lectures	Workshop	Labs	Project	Testing	Personal work	Coef /module	ECTS
17	25	12			4	1	9	1	1,4

Summary	This class deals with Alloy/Electrum for the specification of a reactive system and of the behavioural and structural properties it must fulfil. The class includes theoretical aspects on the one hand, and some experimentation with a formal modelling and verification software

Head	Julien Brunel – ONERA, Toulouse
Teaching team	Julien Brunel – ONERA, Toulouse

Key words	Formal specification, reactive system verification, Alloy
Prerequisites	System Architecture Design, synchronous and asynchronous communication, Formal Specification introduction with Alloy (class 2IA 8.4.2)

Context and general objective:
The goal of this class is to provide insight into the formal specification and verification of reactive systems in Alloy: how to model a system in a formal way and how to express the properties that the system must satisfy.

Programme and contents:
1. Presentation ofAlloy/Electrum formalism used to specify the system behavior and the expected properties
2. Experimentations with the tool Electrum

Method and pedagogic organisation:
The class is organised in lectures / lab sessions, followed by a project shared with the other classes of the module carried out by small groups of students.

Targeted skills or knowledge :
To be able to model an abstract view of a system behaviour, to be able to specify properties using logic.

Evaluation :
Project report and oral presentation + individual exam (1h)

Feedback made to the student :
During the oral presentation + commentaries on the project report (max. 3 weeks after the end of project) + commentaries on the exam copies

Teaching material and references :
Slides

Class 3

Class Title: Specification and Verification in Process Algebra	
Code: 2IAiail 9.3.	**Module Title :** Modelling and Verification of Dependable Reactive Systems
Semester: S9	**Classification:** CSAI Department, AISE option

Hours of presence	Total hours	Lectures	Worshop	Labs	Project	Testing	Personal work	Coef /module	ECTS
17	28	12			4	1	11	1	1,3

Summary	This course presents formal techniques for specifying reactive systems and their expected behavioral properties. Theoretical aspects are introduced through transition system formalism and logic reasoning. Practical aspects are covered through a modelling and formal verification tool.

Head	Thomas Lambolais – CERIS/IMT Mines Alès
Teaching Team	Thomas Lambolais – CERIS/IMT Mines Alès

Key words	Formal Specification, Formal Verification, Model Checking, CCS, LTS
Prerequisites	System architecture modelling, synchronous and asynchronous communication

Contexte and general objective:
This course aims to sensitize future engineers to formal approaches to specifying and verifying reactive systems in order to analyze their behavior.

Programme and contents:

1. Presentation of the formalisms used to describe the behaviour of reactive systems:
   - CCS (Calculus of Communicating Systems) with the CAAL tool, or LOTOS with CADP tool.
   - LTS (Labelled transition systems), transition systems.
   - Traces analysis,
   - relations: bisimulations, conformance, ,..
2. Understanding Formal Languages for Describing Expected Properties :
   - HML (Henessy Milner Logics)
3. Experimentations with the tools CAAL or CADP

Method and pedagogic organisation:
The class is organised in lectures / lab sessions, followed by a project shared with the other classes of the module carried out by small groups of students.

- 12h of lectures
- 4h of project

Target skills or knowledge:
Abstraction and Formal Modelling, Formal definition of properties using logic formalism

Evaluation : Project report and oral presentation + individual exam (1h)

Feeback made to students:
During the oral presentation + commentaries on the project report (max. 3 weeks after the end of project) + commentaries on the exam copies

Teaching matieral and references:
Slides

Method and teaching organisation

This is a classical course containing a theoretical part with standard courses and a practical one through lab sessions and a project.

Testing procedures

The student's level of knowledge acquisition will be evaluated according to the following points:

N° Indicator	Indicator
1	To know the formal and practical knowledge constituting the foundation of a given field
2	Exploit theoretical and practical knowledge
3	Analyse, interpret, model, hypothesize and solve problems

Grading scheme

Class	**Exam**	**Coefficients**	**Administration Mode**	**Evaluated Indicators**	**Chapters**
Reactive System Architectures	Common project	1	Small group	1, 2, 3	all
Formal Specification and Verification in Electrum/ Alloy					
Formal Specification and Verification in processus algebra					
Reactive System Architectures	Exam	1/3	individual	1,2	all
Formal Specification and Verification in Electrum/ Alloy	Exam	1/3	individual	1,2	all
Formal Specification and Verification in processus algebra	Exam	1/3	individual	1,2	all

In each course of this module, an unscheduled assessment may occur.

Student commitments, ethics and professionalism

Expectations concerning ethics are defined in the establishment's code of conduct. Each student is expected to know and respect the code of conduct.

Obligatory presence in classes : Students must attend all courses, seminars and labs.

Estimated hours of personal study*:* in order to acquire the required learning level, the student is expected (must) to spend a minimum of 45min of personal study time per hour spent in class. 30h of personal work for the project.

Estimated hours of preparation required for labs/Work Shop*:* 45 minutes

Late penalties*:* Late works are subject to penalties as follows: 1 point per day (ratings between 0 and 20).

Teaching team

Name	Field of expertise	Email/Phone
Anne-Lise COURBIS	Model Based System Engineering Embedded System Modelling Formal Verification	anne-lise.courbis@mines-ales.fr 04 34 24 62 63
Julien Brunel	Formal Specification and Verification Logic Safety Validation	ONERA, Toulouse julien.brunel@onera.fr 05 62 25 26 81
Thomas LAMBOLAIS	Software Engineering, Formal specification and validation	thomas.lambolais@mines-ales.fr 04 34 24 62 60

Approbation

Ce guide pédagogique entré en vigueur à compter du 7 janvier 2019 a été mis à jour en juillet 2022.

Il est porté à la connaissance des élèves par une publication sur le site de l'école.

Rédaction	Vérification	Validation
L'enseignant responsable du module : Anne-Lise COURBIS	Le responsable d'UE / de département : Sylvie RANWEZ	Le directeur de l'école, Pour le directeur et par délégation, Le directeur de la DFA / de la DE : Michel FERLUT