



CentraleSupélec

université
PARIS-SACLAY



CentraleSupélec

ST5 - MODÉLISATION FONCTIONNELLE ET RÉGULATION

SYSTÈMES COMPLEXES ET CRITIQUES À LOGICIELS PRÉPONDÉRANTS

🎓 2A cursus Ingénieurs - 2023/2024

🏛️ CentraleSupélec - Université Paris-Saclay



Idir AIT SADOUNE

idir.aitsadoune@centralesupelec.fr



IDIR AIT SADOUNE

- **Docteur en Informatique** diplômé par l'**ENSMA** en **2010**.
 - **Thèse** sur la modélisation et la vérification des services par une approche basée sur le raffinement et sur la preuve.
- **Enseignant-chercheur** au sein du département informatique de **CentraleSupélec**.
- **Chercheur** au sein des pôles **Modèles** et **Preuve** du **LMF - Laboratoire Méthodes Formelles**.

DISCUSSION AUTOUR DES ATTENTES DES ÉLÈVES



PLAN

- La présentation de la ST
- Contexte et Enjeux
- Présentation du cours spécifique
- Enseignement d'intégration
- Validation de la ST
- Pour aller plus loin

[Retour au plan](#) - [Retour à l'accueil](#)

PLAN

- > La présentation de la ST
- > Contexte et Enjeux
- > Présentation du cours spécifique
- > Enseignement d'intégration
- > Validation de la ST
- > Pour aller plus loin

[Retour au plan](#) - [Retour à l'accueil](#)

LES RESPONSABLES DE LA ST



Marc AIGUIER
marc.aiguier@centralesupelec.fr



Idir AIT SADOUNE
idir.aitsadoune@centralesupelec.fr



Paolo BALLARINI
palolo.ballarini@centralesupelec.fr

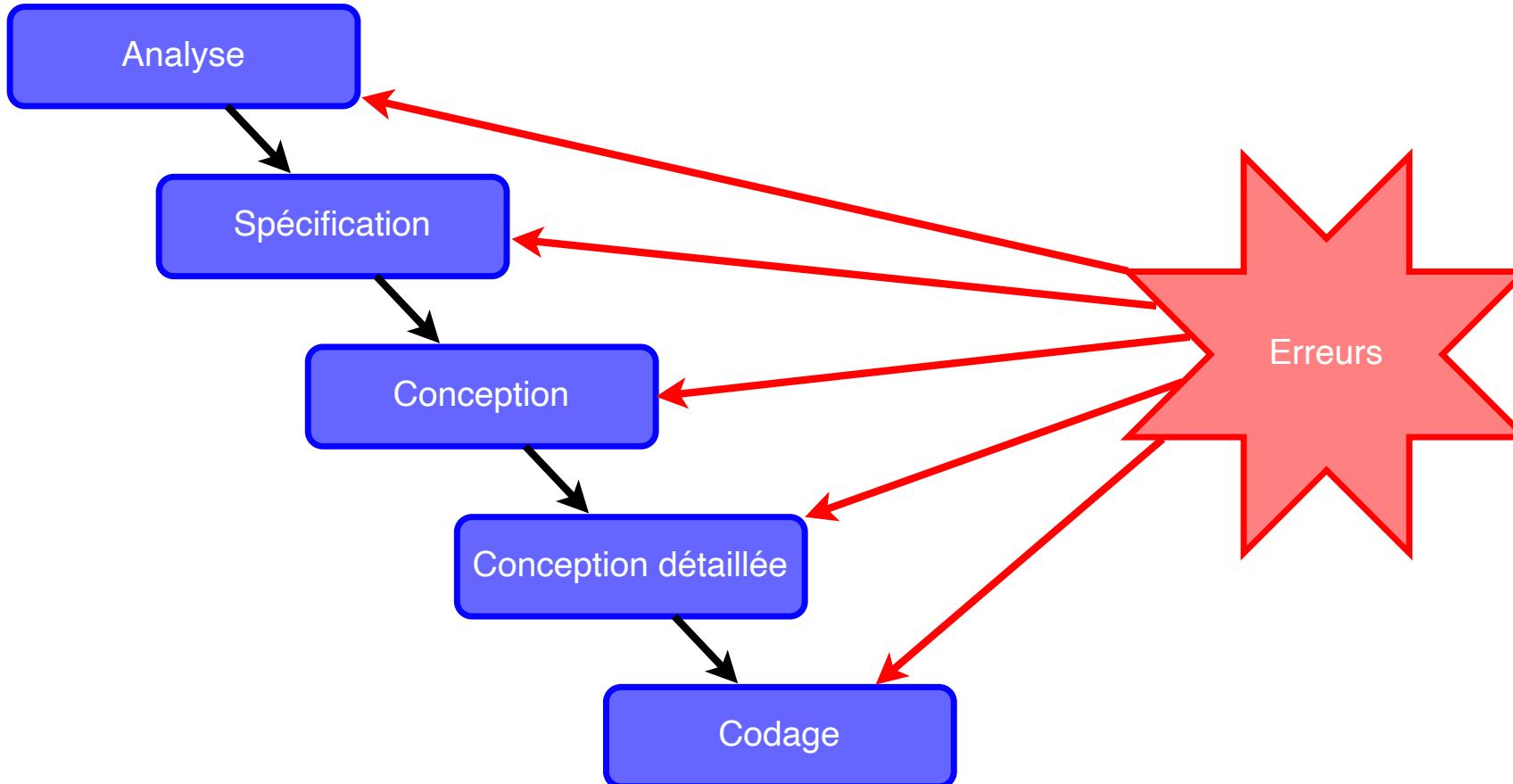


Lina YE
lina.ye@centralesupelec.fr

LE LOGICIEL INFORMATIQUE



CYCLE DE DÉVELOPPEMENT



Des **erreurs** possibles à toutes les étapes du développement.

LOGICIELS CRITIQUES

- Une défaillance dans un logiciel peut avoir des conséquences catastrophiques (humaines, financières, ...).
- Exemple du calculateur de bord d'Ariane 5
 - Vol 241/5101 du 25 janvier 2018



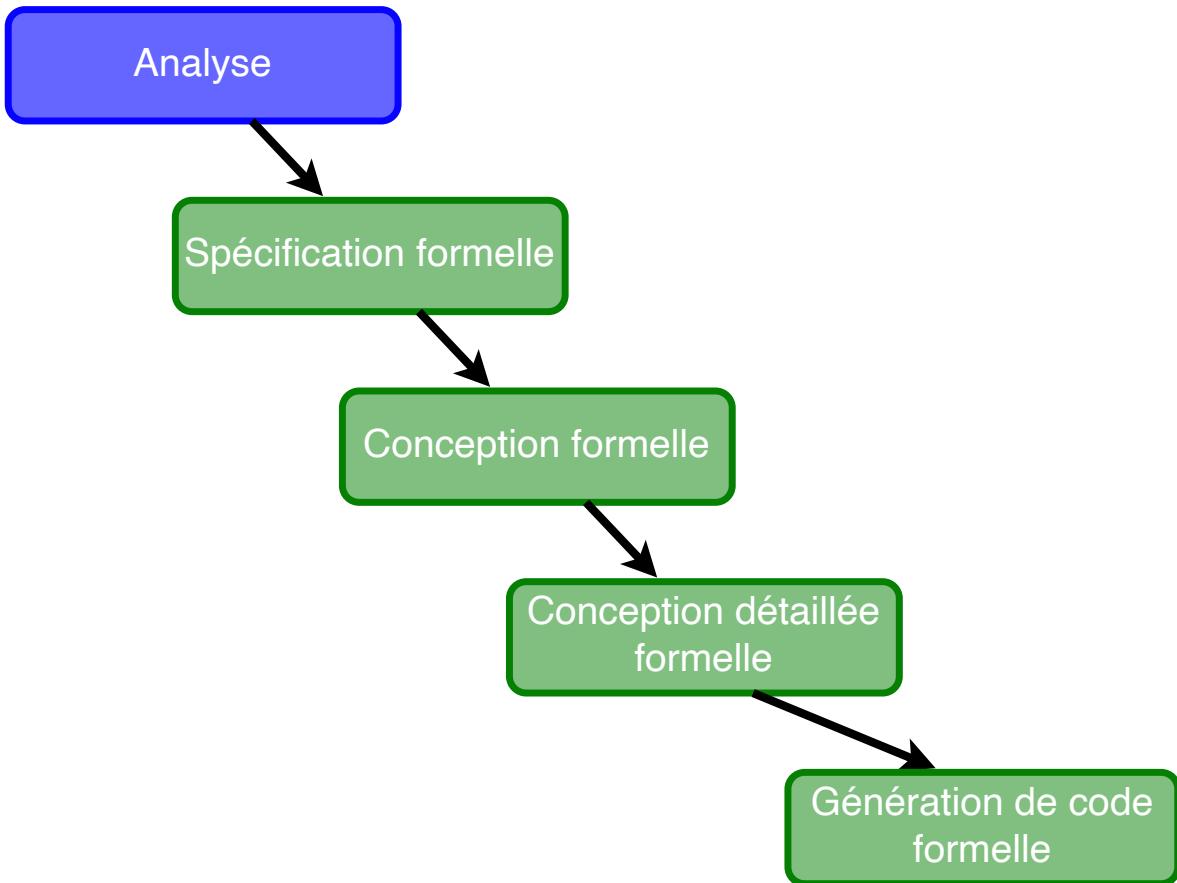
SITUATIONS À ÉVITER !!!



SOLUTIONS

- Les **règles et les techniques** de programmation.
- Les **méthodologies de conception** et de développement.
- Le **support** des langages de programmation.
- Le **test**.
- Les **méthodes formelles**.

LA PLACE DES MÉTHODES FORMELLES



Utiliser les **méthodes formelles** dans **toutes les étapes**.

LES MÉTHODES FORMELLES ET LA VÉRIFICATION

- **Les méthodes formelles**
 - ➡ Une **méthode d'ingénierie** pour le développement de systèmes basée sur des **concepts logiques et mathématiques rigoureux**.
(déterminer ce que le logiciel est censé faire)
- L'activité de **vérification**
 - ➡ **Vérifier** qu'un système **répond aux exigences** identifiées dans sa **spécification** en utilisant **une méthode formelle**.
(prouver que le logiciel fait ce qu'il est censé faire)
- **Spécification formelle/Vérification formelle/Synthèse formelle**

CONCLUSION

Une **analyse** utilisant les **méthodes formelles** peut fournir la **preuve** que le système est complet et **correct vis à vis de ses exigences**.

QUI RECOMMANDÉ LES MÉTHODES FORMELLES ?

- **Norme européenne**

L'utilisation de spécifications formelles seule rend les exigences non ambiguës.

- **Norme aéronautique**

L'utilisation de méthodes formelles a pour but d'éliminer les erreurs de spécification, de conception et de codage lors du développement.

- **Norme ferroviaire**

Pour les spécifications, des méthodes formelles sont recommandées car le modèle formel fournit précision, non ambiguïté et cohérence.

EXEMPLES DE NORMES

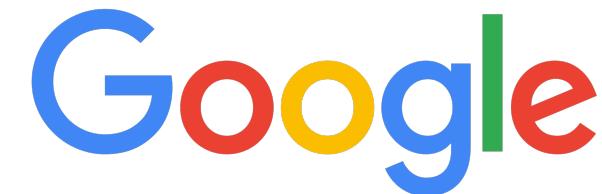
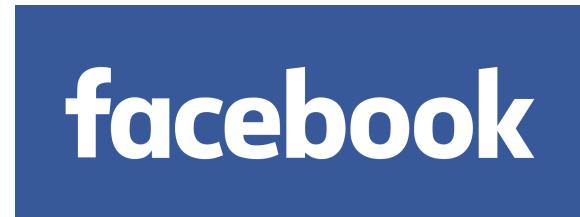
- Les normes européennes EN 50126, EN 50128, EN 50129
 - ➡ des standards utilisés dans le domaine ferroviaire.
 - ➡ requises pour les fournisseurs d'équipements de contrôle-commande.



LES MÉTHODES FORMELLES RECOMMANDÉES

- Quelques **méthodes formelles** recommandées par les **normes** :
 - ➡ "CSP, HOL, LOTOS, **Temporal Logic**, **B Method**, **Model Checking** ..."
 - ➡ **page 103** de la norme **EN 50128**

QUI UTILISE LES MÉTHODES FORMELLES?

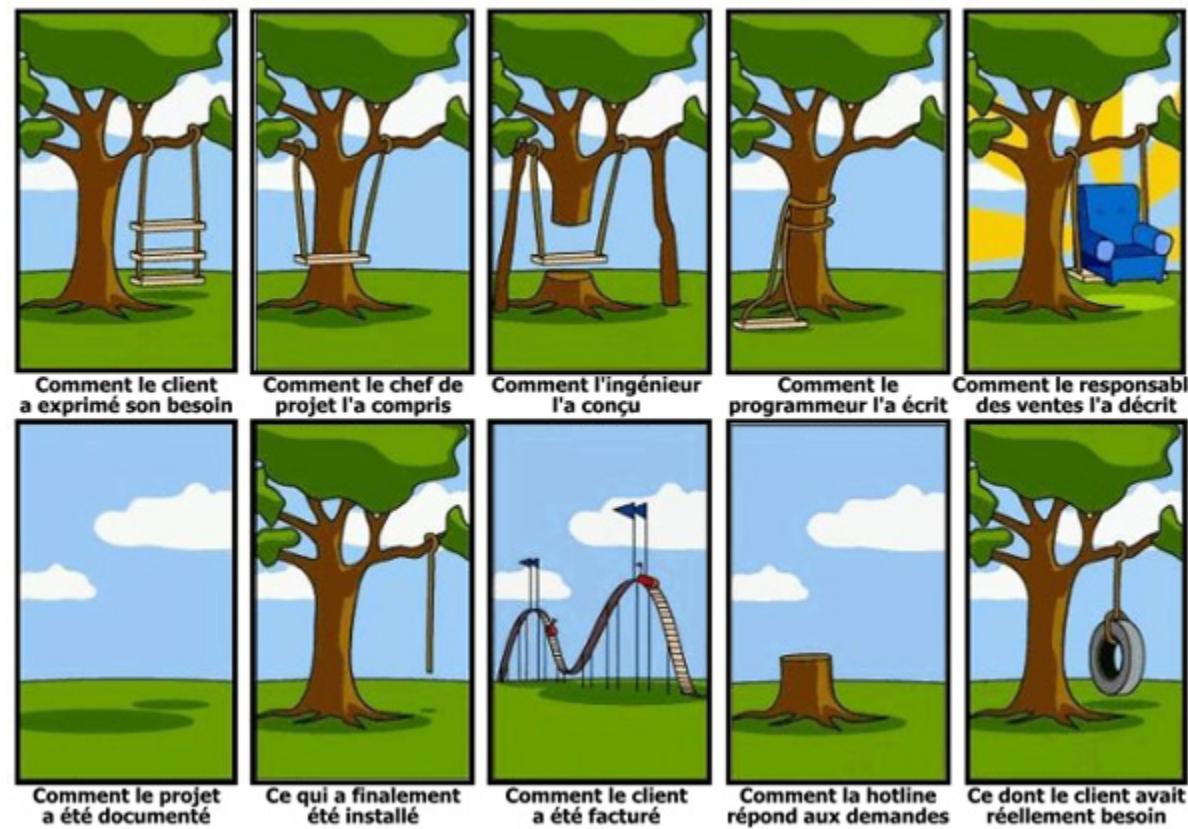


EVALUATION ASSURANCE LEVEL (EAL)

- **7 niveaux d'assurance** d'évaluation selon les critères communs
 - **EAL1** : testé fonctionnellement
 - **EAL2** : testé structurellement
 - **EAL3** : testé et vérifié méthodiquement
 - **EAL4** : conçu, testé et vérifié méthodiquement
 - **EAL5** : conçu de façon semi-formelle et testé
 - **EAL6** : conception vérifiée de façon semi-formelle et système testé
 - **EAL7** : conception vérifiée de façon formelle et système testé
- **Les applications civiles** : les EAL sont généralement de 1 à 4 (4+).
- **Les applications militaires** : les EAL sont de 5 à 7.

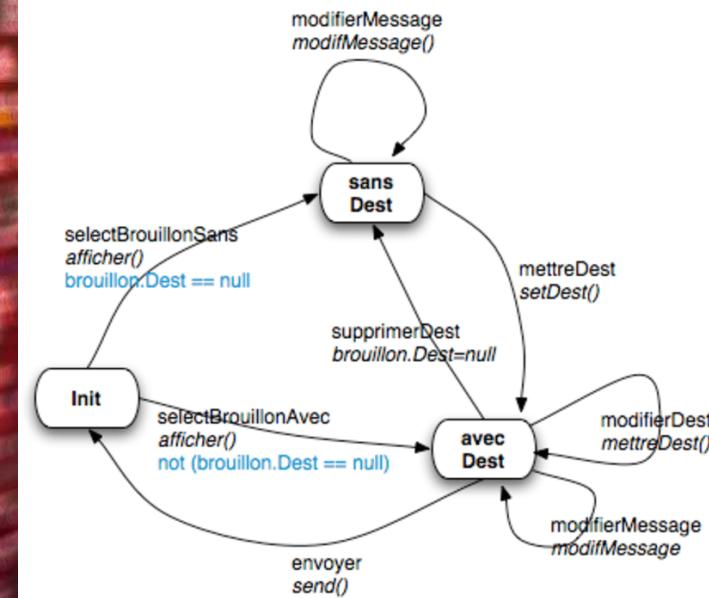
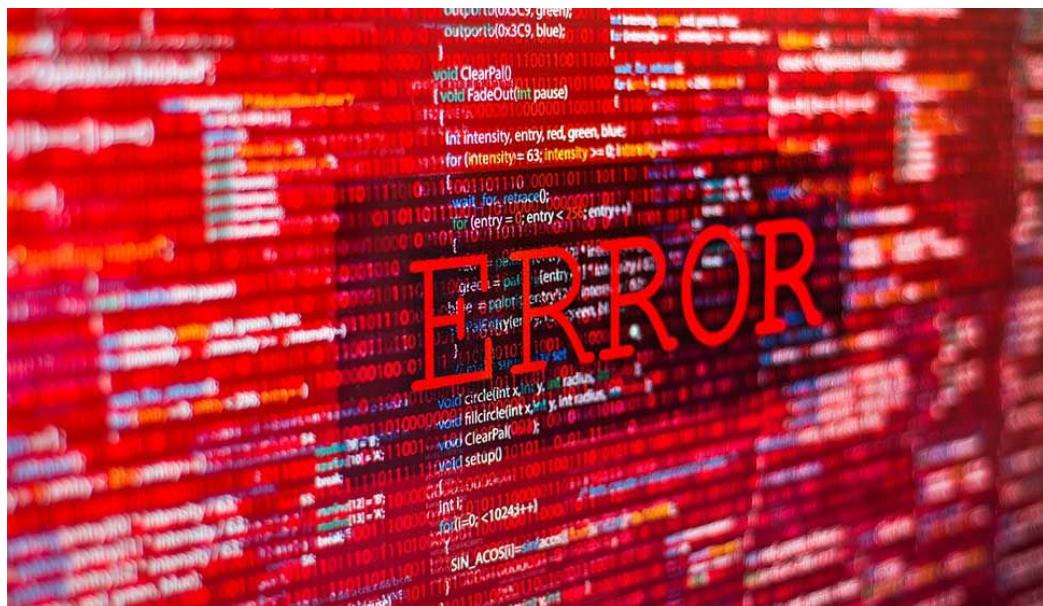
QUELQUES MYTHES

- L'utilisation des méthodes formelles **produit un logiciel parfait ?**
 - ➡ non-sens, une spécification formelle est un modèle du monde réel
 - ➡ peut inclure des erreurs, des omissions et des malentendus



QUELQUES MYTHES

- Utiliser les méthodes formelles \approx faire de la preuve de programme ?
 - ➡ la modélisation d'un système est valable sans vérification de programmes
 - ➡ la spécification formelle force à une analyse détaillée du système



QUELQUES MYTHES

- Les méthodes formelles que pour **les systèmes critiques** ?
 - ➡ l'expérience industrielle montre que les coûts de développement sont réduits pour tous les types de systèmes.
(IHM multimodales, microservices, validation de données, ...)



QUELQUES MYTHES

- Les méthodes formelles sont uniquement pour **les mathématiciens** ?
➡ non-sens, les mathématiques employées sont élémentaires.

$$\begin{aligned} \text{tg } \alpha \text{ ctg } \alpha &= 1 \\ \frac{a}{\sin \alpha} &= \frac{b}{\sin \beta} = \frac{c}{\sin \gamma} = 2R \\ (-a) \text{ tg}(\alpha - \beta) &= \frac{\text{tg } \alpha - \text{tg } \beta}{\log_b c} \end{aligned}$$

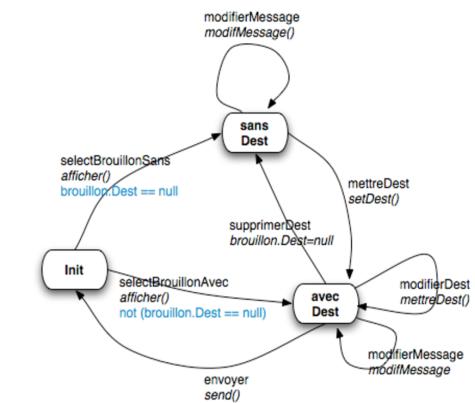
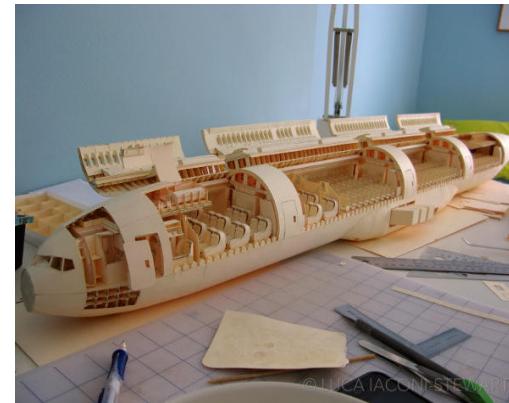
QUELQUES MYTHES

- Les méthodes formelles **augmentent les coûts de développement ?**
➡ non-prouv , il y a un d placement des coûts vers les premières t ches.

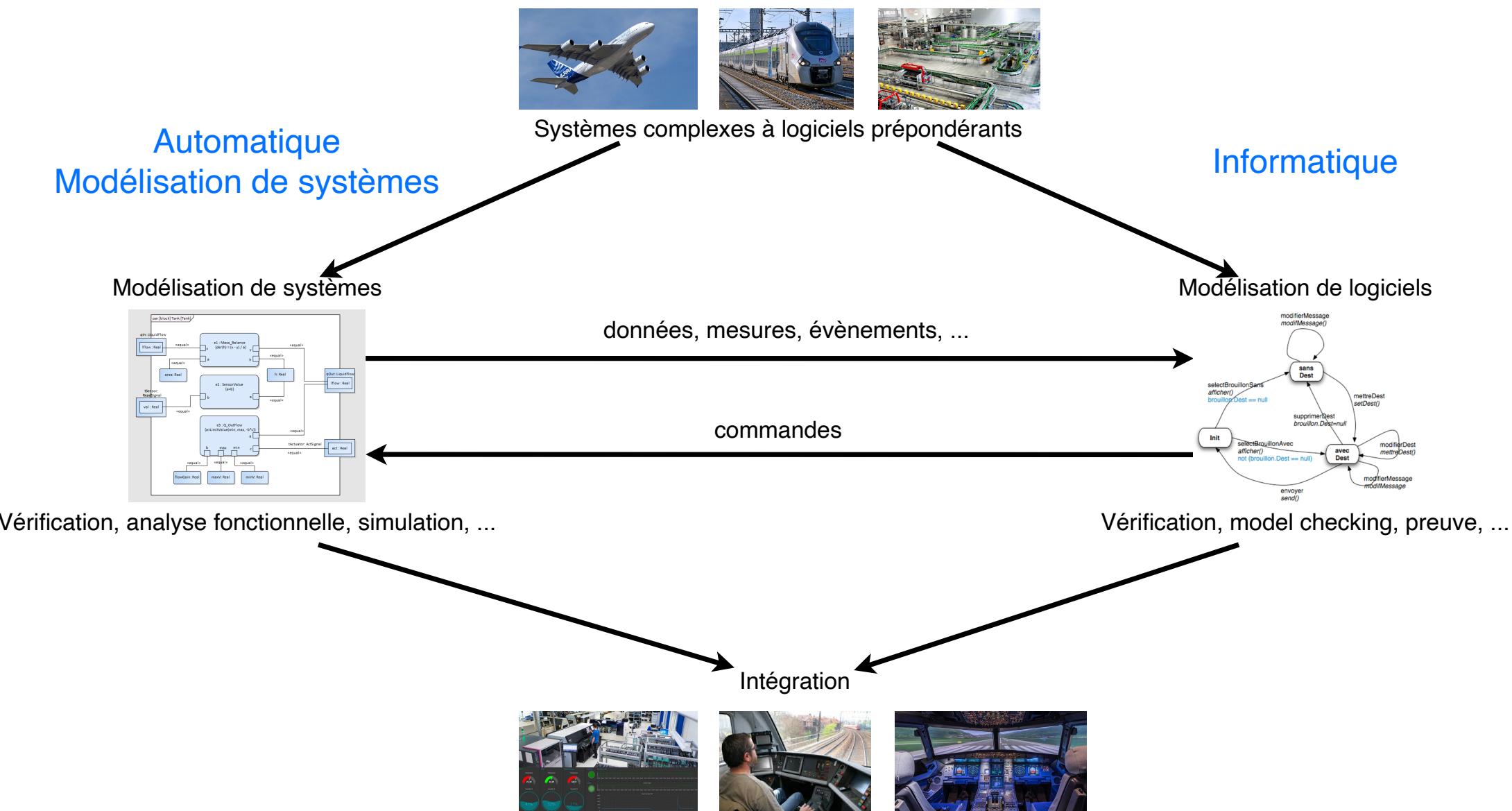


QUELQUES MYTHES

- Les clients **ne peuvent pas comprendre** les spécifications formelles.
➡ il faut les paraphraser en langage naturel, ou utiliser le prototypage.

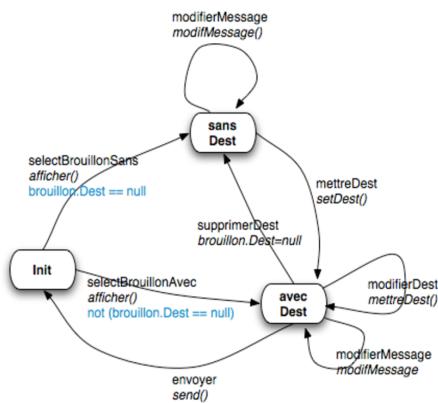


LE CADRE DE LA ST



L'OBJECTIF DE LA ST

Comment exprimer (modéliser) et vérifier les propriétés comportementales des systèmes critiques?



Cette ST va vous aider à répondre à cette question !!!

PLAN

- La présentation de la ST
- Contexte et Enjeux
- Présentation du cours spécifique
- Enseignement d'intégration
- Validation de la ST
- Pour aller plus loin

[Retour au plan](#) - [Retour à l'accueil](#)

PLANNING

Lundi 18 septembre 2023 - Amphi II, Eiffel

08h15 - 09h45 Présentation de la séquence thématique

Idir AIT-SADOUNE (CentraleSupélec)

10h00 - 11h30 Séminaire

Guillaume GIRAUD (RTE)

PLANNING

Lundi 25 septembre 2023 - Amphi II, Eiffel

08h15 - 09h45 Séminaire

Lucien PEREZ (IKOS Consulting)

10h00 - 11h30 Présentation des EI

Idir AIT-SADOUNE (CentraleSupélec)

PLANNING

Mardi 26 septembre 2023 - Amphi II, Eiffel

08h15 - 09h45 Séminaire

Michel BATTEUX (Systemic Intelligence)

10h00 - 11h30 Séminaire

Thierry LECOMTE (ClearSy)

NOTE DE SYNTHÈSE

- Rédaction d'une **note de prise de recul individuelle** qui sera évaluée selon un processus **d'évaluation par les pairs**.
- Longueur de **pages maximum** rédigée en **français/anglais** et portant sur les aspects suivants :
 - Description et compréhension de la thématique
 - Enjeux/défis économiques, sociaux, industriels, actuels et futurs
 - Verrous scientifiques et technologiques majeurs
 - Domaines clés d'innovation pour l'ingénieur
- Une attention particulière sera portée à la clarté de cette note.

CONTENU D'UNE NOTE

Vous pourrez apporter, en développant les points précédents, des éléments de réponse aux interrogations suivantes :

- Quels sont **les points des modules contexte et enjeux qui m'ont le plus marqué**, quels messages ressortent du lot, pourquoi ?
- Ai-je pris conscience **des besoins de développement sur des compétences importantes** pour l'ingénieur ?
- Quel est mon ressenti par rapport à **mes attentes** en sélectionnant cette Séquence Thématique ?
- Quelles **innovations pour le futur** ?
- Pourquoi et comment pourrais-je les aborder ?

ÉVALUATION PAR LES PAIRS

Processus d'évaluation

- **Une note** de prise de recul **rédigée par chacun**
- **3 notes** de prise de recul **notées par chacun**
- **Une note** de prise de recul sera **notée par 3 étudiants**
- **Note finale:** moyenne des notes reçues par une note.

Dates importantes (délai strict)

- **Dépôt du travail:** au plus tard le **vendredi 20/10/2023 à 23h59.**
- **Évaluation par les pairs :** entre le **23 et le 27/10/2023 à 23h59.**

PLAN

- La présentation de la ST
- Contexte et Enjeux
- Présentation du cours spécifique
- Enseignement d'intégration
- Validation de la ST
- Pour aller plus loin

[Retour au plan](#) - [Retour à l'accueil](#)

LE PROGRAMME

CONCEPTION ET VÉRIFICATION DE SYSTÈMES CRITIQUES

Les logiques temporelles

2 CMs, 2 TDs (4 × 1h30)

Marc AIGUIER (CentraleSupélec)

Le Model Checking

1 CMs, 3 TDs (4 × 1h30)

Paolo BALLARINI (CentraleSupélec)

Les automates temporisés

2 CMs, 4 TDs, 1 TP (6 × 1h30)

Lina YE (CentraleSupélec)

Les modèles stochastiques

2 CMs, 3 TDs, 1 TP (5 × 1h30)

Paolo BALLARINI (CentraleSupélec)

ORGANISATION DU COURS

- **Date de début** : lundi 18/09/2023 à 15h15 / **Amphi II, Eiffel.**
 - **Cours** : en présentiel
 - **TD** : en présentiel
 - **TP** : devoir maison
- Polycopie, slides, énoncés des TD/TP, corrections des TD/TP **en versions PDF** disponibles sur **Edunao**.
- Polycopie **en version papier** disponible
- Le polycopie contient plus d'informations que ce qui sera vu en cours.

PLAN

- La présentation de la ST
- Contexte et Enjeux
- Présentation du cours spécifique
- Enseignement d'intégration**
- Validation de la ST
- Pour aller plus loin

[Retour au plan](#) - [Retour à l'accueil](#)

LES ENSEIGNEMENTS D'INTÉGRATION

Présentation des sujets et des détails de l'organisation des Els
le **lundi 25/09/2023 à 10h00.**

PLAN

- La présentation de la ST
- Contexte et Enjeux
- Présentation du cours spécifique
- Enseignement d'intégration
- Validation de la ST
- Pour aller plus loin

[Retour au plan](#) - [Retour à l'accueil](#)

VALIDATION DE LA ST

- La ST5 valide une Unité d'Enseignement (UE) Séquence Thématique dédiée à la modélisation fonctionnelle et la régulation.
- L'évaluation est constituée des activités suivantes :
 - modules contexte et enjeux : 0.2 ECTS,
 - cours automatique et contrôle : 2.5 ECTS,
 - cours modélisation système : 2 ECTS,
 - cours spécifique : 2.5 ECTS,
 - enseignement d'intégration (EI) : 1.8 ECTS.
- Pour valider une UE, un élève doit obtenir une note $\geq 10/20$ à chacune des activités constituant l'UE.
- L'EI est un cas particulier et doit être validé par une note $\geq 12/20$.

EVALUATIONS

- **Module contexte et enjeux**
 - évaluation de la note de prise de recul.
- **Cours spécifique**
 - l'examen aura lieu le **Mercredi 08/11/2023**.
 - les sujets d'examens seront en français et en anglais. Les élèves peuvent composer dans la langue de leur choix (**français/anglais**).
 - le contrôle final aura une durée de **1h30**.
- **Enseignement d'Intégration**
 - la note sera détaillée lors de la présentation des Els.

ORGANISATION DES RATTRAPAGES

- **Module contexte et enjeux**
 - si la note de synthèse n'est pas rendue : la note = 0.
 - si la note $\in [0..7]$: un oral de 15 minutes est organisé.
- **Cours spécifique**
 - si la note ≤ 7 : un rattrapage est programmé.
 - examen écrit de même durée que l'examen initial.
- **Enseignement d'Intégration**
 - si la note < 12 : un rattrapage est programmé.

L'ÉVALUATION DES COMPÉTENCES

La **ST5** évalue les compétences **C1, C2, C4, C6** et **C7**.

- **Module contexte et enjeux**
 - **C2** → développer une compétence approfondie dans un domaine d'ingénieur et dans une famille de métiers
- **Cours spécifique**
 - **C1.2** → l'**examen** : utiliser et développer les modèles adaptés, choisir la bonne échelle de modélisation et les hypothèses pertinentes
 - **C1.4** → le **TP** : spécifier, réaliser et valider un système complexe

L'ÉVALUATION DES COMPÉTENCES

La **ST5** évalue les compétences **C1, C2, C4, C6 et C7**.

- **Enseignement d'Intégration**

- **C4** : Avoir le sens de la création de valeur pour son entreprise et ses clients.
- **C6** : Être opérationnel, responsable et innovant dans le monde numérique
- **C7** : Savoir convaincre

Chaque responsable d'EI va détailler les C_{ij} ciblées dans son projet.

PLAN

- La présentation de la ST
- Contexte et Enjeux
- Présentation du cours spécifique
- Enseignement d'intégration
- Validation de la ST
- Pour aller plus loin

[Retour au plan](#) - [Retour à l'accueil](#)

DOMINANTE INFORMATIQUE ET NUMÉRIQUE EN 3A

Mention : **Science du Logiciel**

<https://wdi.centralesupelec.fr/infocs/Public/Scilog>

Responsable : Frédéric BOULANGER

frederic.boulanger@centralesupelec.fr

MERCI

[Retour à l'accueil](#) - [Retour au plan](#)